CISSP.exam.715q

Number: CISSP
Passing Score: 800
Time Limit: 120 min

CISSP

Certified Information Systems Security Professional

Sections

1. Asset Security
2. Security Engineering
3. Communication and Network Security
4. Identity and Access Management
5. Security Assessment and Testing

6. Security Operations
7. Software Development Security

Exam A

QUESTION 1

The owner of a system should have the confidence that the system will behave according to its specifications. This is termed as:

A. Integrity
B. Accountability
C. Assurance
D. Availability

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:

In a trusted system, all protection mechanisms work together to process sensitive data for many types of uses, and will provide the necessary level of protection per classification level. Assurance looks at the same issues but in more depth and detail. Systems that provide higher levels of assurance have been tested extensively and have had their designs thoroughly inspected, their development stages reviewed, and their technical specifications and test plans evaluated.

In the Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the Orange Book, the lower assurance level ratings look at a system's protection mechanisms and testing results to produce an assurance rating, but the higher assurance level ratings look more at the system design, specifications, development procedures, supporting documentation, and testing results. The protection mechanisms in the higher assurance level systems may not necessarily be much different from those in the lower assurance level systems, but the way they were designed and built is under much more scrutiny. With this extra scrutiny comes higher levels of assurance of the trust that can be put into a system.

Incorrect Answers:

A: Integrity ensures that data is unaltered. This is not what is described in the question.

B: Accountability is a security principle indicating that individuals must be identifiable and must be held responsible for their actions. This is not what is described in the question.
D: Availability ensures reliability and timely access to data and resources to authorized individuals.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 390-391

QUESTION 2
The US department of Health, Education and Welfare developed a list of fair information practices focused on privacy of individually, personal identifiable information. Which one of the following is incorrect?

A. There must be a way for a person to find out what information about them exists and how it is used.
B. There must be a personal data record-keeping system whose very existence shall be kept secret.
C. There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used or made available for another purpose without their consent.
D. Any organization creating, maintaining, using, or disseminating records of personal identifiable information must ensure reliability of the data for their intended use and must make precautions to prevent misuses of that data.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Fair Information Practice was first developed in the United States in the 1970s by the Department for Health, Education and Welfare (HEW). T Fair Information Practice does not state that there the personal data record-keeping system must be secret.

Incorrect Answers:
A: HEW Fair Information Practices include that there should be mechanisms for individuals to review data about them, to ensure accuracy.
C: HEW Fair Information Practices include
- For all data collected there should be a stated purpose
- Information collected by an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual

D: HEW Fair Information Practices include
- Records kept on an individual should be accurate and up to date
- Data should be deleted when it is no longer needed for the stated purpose

References:
https://en.wikipedia.org/wiki/Information_privacy_law

QUESTION 3
The typical computer fraudsters are usually persons with which of the following characteristics?

A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
It is easy for people who are placed in position of trust to commit fraud, as they are considered to be trustworthy.

Incorrect Answers:
A: A fraudster might very well have a clean legal record. This in conjunction with a position of trust make him/her hard to detect.
B: It is most typical that a fraudster conspires with other persons as the fraudster usually acts alone.
D: A fraudster can very well follow the accepted norms of society, and this makes him/her harder to detect.

References: http://www.justice4you.org/fraud-fraudster.php

QUESTION 4
The US-EU Safe Harbor process has been created to address which of the following?

A. Integrity of data transferred between U.S. and European companies
B. Confidentiality of data transferred between U.S and European companies
C. Protection of personal data transferred between U.S and European companies
D. Confidentiality of data transferred between European and international companies

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

US-EU Safe Harbor process relates to privacy, that is protection of personal data. The Safe Harbor is a construct that outlines how U.S.-based companies can comply with the EU privacy. The Safe Harbor Privacy Principles states that if a non-European organization wants to do business with a European entity, it will need to adhere to the Safe Harbor requirements if certain types of data will be passed back and forth during business processes

Incorrect Answers:
A: The US-EU Safe Harbor process does not relate to the integrity of the data. It concerns the privacy of the data.
B: The US-EU Safe Harbor process does not relate to the Confidentiality of the data. It concerns the privacy of the data.
D: The US-EU Safe Harbor process does not relate to the Confidentiality of the data. It concerns the privacy of the data.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 992

QUESTION 5
What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

A. Level 1/Class 1 B.
Level 2/Class 2 C.
Level 3/Class 3
D. Level 4/Class 4

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Users can obtain certificates with various levels of assurance.
Level 1/Class 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.

Class 2/Level 2 verify a user's name, address, social security number, and other information against a credit bureau database.

Class 3/Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the other items of information provided by a level 2 certificate.

Incorrect Answers:
A: Level 1/Class 1 certificates verify electronic mail addresses. They do not verify a user's name, address, social security number, and other information against a credit bureau database.

C: Level 3/Class 3 certificates provide photo identification to accompany the other items of information provided by a level 2 certificate. They do not verify a user's name, address, social security number, and other information against a credit bureau database.
D: Level 4/Class 4 certificates do not verify a user's name, address, social security number, and other information against a credit bureau database.

QUESTION 6
According to Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) there is a requirement to "protect stored cardholder data." Which of the following items cannot be stored by the merchant?

A. Primary Account Number
B. Cardholder Name
C. Expiration Date
D. The Card Validation Code (CVV2)

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use.
Requirement 3 applies only if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves.
For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only council certified PIN entry devices and payment applications may be used.
PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS Requirement 3
It details technical guidelines for protecting stored cardholder data. Merchants should develop a data retention and storage policy that strictly limits storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.
Sensitive authentication data must never be stored after authorization – even if this data is encrypted.
- Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data). If required for business purposes, the cardholder's name, PAN, expiration date, and service code may be stored as long as they are protected in accordance with PCI DSS requirements.
- Never store the card-validation code (CVV) or value (three- or four-digit number printed on the front or back of a payment card used to validate card-not-present transactions).

- Never store the personal identification number (PIN) or PIN Block. Be sure to mask PAN whenever it is displayed. The first six and last four digits are the maximum number of digits that may be displayed. This requirement does not apply to those authorized with a specific need to see the full PAN, nor does it supersede stricter requirements in place for displays of cardholder data such as in a point-of-sale receipt.

Incorrect Answers:
A: The Primary Account Number can be stored by the merchant according to the PCI Data Storage Guidelines.
B: The Cardholder Name can be stored by the merchant according to the PCI Data Storage Guidelines.
C: The Expiration Date can be stored by the merchant according to the PCI Data Storage Guidelines.

References:
https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

QUESTION 7
Which of the following is NOT a proper component of Media Viability Controls?
A. Storage
B. Writing
C. Handling
D. Marking

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Writing is not a component of media viability controls.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process: ▪ Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.
- Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.
- Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
A: Storage is a media viability control used to protect the viability of data storage media.

C: Handling is a media viability control used to protect the viability of data storage media.
D: Marking is a media viability control used to protect the viability of data storage media.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 324

QUESTION 8
Degaussing is used to clear data from all of the following media except:

A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment). "

Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal. Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM which do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.

Not all clearing/ purging methods are applicable to all media— for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.

Incorrect Answers:
A: Floppy Disks can be erased by degaussing.
C: Video Tapes can be erased by degaussing.
D: Magnetic Hard Disks can be erased by degaussing.

References:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

QUESTION 9
What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The main issue with media reuse is data remanence, where residual information still resides on the media.
Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media's information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The "Orange Book" standard recommends that magnetic media be formatted seven times before discard or reuse.

Incorrect Answers:
A: Degaussing is a method used to ensure that there is no residual data left on the media. This is not the main issue with media reuse.
C: Media destruction as the name suggests is the destruction of media. This is not the main issue with media reuse.
D: Purging is another method used to ensure that there is no residual data left on the media. This is not the main issue with media reuse.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 477

QUESTION 10
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow

Correct Answer: A
Section: Asset Security
Explanation
Explanation/Reference:
Explanation:
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.

Incorrect Answers:
B: Parity has to do with disk error detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent.
C: Zeroization involves overwriting data to sanitize it. There is a drawback to this method. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
D: This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

QUESTION 11
Which of the following is NOT a media viability control used to protect the viability of data storage media?

A. clearing
B. marking
C. handling
D. storage

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Clearing is not an example of a media viability control used to protect the viability of data storage media.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process: ▪ Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

- Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.
- Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
B: Marking is a media viability control used to protect the viability of data storage media.
C: Handling is a media viability control used to protect the viability of data storage media.
D: Storage is a media viability control used to protect the viability of data storage media.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 324

QUESTION 12
An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called:

A. a magnetic field.
B. a degausser.
C. magnetic remanence.

D. magnetic saturation.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Incorrect Answers:
A: A magnetic field is not the electrical device described in the question.
C: Magnetic remanence is not the electrical device described in the question.
D: Magnetic saturation is not the electrical device described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 1282

QUESTION 13
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The information stored on a CDROM is not in electro-magnetic format, so a degausser would be ineffective.
The only way to dispose of information on a CD-ROM is to physically destroy the CD-ROM.

Incorrect Answers:
A: You cannot sanitize read-only media such as a CDROM.

B: Physical damage is not the MOST secure way to dispose of information on a CD-ROM. Data could still be recovered from the undamaged part of the CD-ROM. Only complete destruction of the CD-ROM will suffice.
C: Degaussing does not work on read-only media such as a CDROM.

QUESTION 14
Which of the following refers to the data left on the media after the media has been erased?

A. remanence
B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media's information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The "Orange Book" standard recommends that magnetic media be formatted seven times before discard or reuse.
Incorrect Answers:
B: Recovery is not the term that refers to the data left on the media after the media has been erased.
C: Sticky bits is not the term that refers to the data left on the media after the media has been erased.
D: Semi-hidden is not the term that refers to the data left on the media after the media has been erased.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 477

QUESTION 15
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

A. Data fiddling
B. Data diddling
C. Salami techniques

D. Trojan horses

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. In this case, the employee has been shaving off pennies from multiple accounts in the hope that no one notices. Shaving pennies from an account is the small crime in this example. However, the cumulative effect of the multiple 'small crimes' is that a larger amount of money is stolen in total.

Incorrect Answers:
A: Data fiddling is not a defined attack type. The term could refer to entering incorrect data in a similar way to data diddling. However, it is not the term used to describe a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account.
B: Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20. This is not what is described in the question.
D: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.

References:
S Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 16
Which of the following logical access exposures involvers changing data before, or as it is entered into the computer?

A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

Incorrect Answers:
B: Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. This is not what is described in the question.
C: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.
D: A Virus is a small application or a string of code that infects applications. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 17
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B
Section: Asset Security
Explanation
Explanation/Reference:
Explanation:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Incorrect Answers:
A: It is not true that clearing completely erases the media or that purging only removes file headers, allowing the recovery of files.
C: Clearing does not involve rewriting the media.
D: It is not true that clearing renders information unrecoverable against a laboratory attack or purging renders information unrecoverable to a keyboard attack.

QUESTION 18
Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

A. Degaussing
B. Overwrite every sector of magnetic media with pattern of 1's and 0's
C. Format magnetic media
D. Delete File allocation table

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Degaussing is the most effective method out of all the provided choices to erase sensitive data on magnetic media.
A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information.

Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist.
Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degaussers can destroy drives. The security professional should exercise caution when recommending or using degaussers on media for reuse.

Incorrect Answers:
B: Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the

head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
C: Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply removes the pointers to the information.
D: Deleting the File allocation table will not erase all data. The data can be recoverable using software tools.

QUESTION 19
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.
SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:
▪ Issuer (cardholder's bank) The financial institution that provides a credit card to the individual. ▪
Cardholder The individual authorized to use a credit card.
▪ Merchant The entity providing goods.
▪ Acquirer (merchant's bank) The financial institution that processes payment cards.
▪ Payment gateway This processes the merchant payment. It may be an acquirer.

Incorrect Answers:
A: SSH is a network protocol that allows for a secure connection to a remote system. Developed to replace Telnet and other insecure remote shell methods. This is not what is described in the question.
B: S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which outlines how public key cryptography can be used to secure MIME data types. This is not what is described in the question.

D: SSL (Secure Sockets Layer) is most commonly used to Internet connections and e-commerce transactions. It is used instead of SET but is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 856

QUESTION 20
In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The item's need to know

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A sensitivity label is required for every subject and object when using the Mandatory Access Control (MAC) model. The sensitivity label is made up of a classification and different categories.

Incorrect Answers:
A: The item's classification on its own is incorrect. It has to have a category as well.
C: The item's category on its own is incorrect. It has to have a classification as well.
D: Need-to-know rules are applied by the categories section of the label.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 223
http://en.wikipedia.org/wiki/Mandatory_Access_Control

QUESTION 21
Which of the following European Union (EU) principles pertaining to the protection of information on private individuals is incorrect?
A. Data collected by an organization can be used for any purpose and for as long as necessary, as long as it is never communicated outside of the organization by which it was collected.
B. Individuals have the right to correct errors contained in their personal data.
C. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
D. Records kept on an individual should be accurate and up to date.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
EU's Data Protection Data Integrity states that Data must be relevant and reliable for the purpose it was collected for.

Incorrect Answers:
B: EU's Data Protection Directive includes the access directive which states that individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
C: EU's Data Protection Directive includes the Onward Transfer directive which states that transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
D: EU's Data Protection Directive includes the Data Integrity directive which states that Data must be relevant and reliable for the purpose it was collected for.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1064-1065

QUESTION 22
Who should DECIDE how a company should approach security and what security measures should be implemented?

A. Senior management
B. Data owner
C. Auditor
D. The information security specialist

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible.
For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent.

Incorrect Answers:
B: The data owner can grant access to the data. However, the data owner should not decide how a company should approach security and what security measures should be implemented.
C: Systems Auditors ensure the appropriate security controls are in place. However, they should not decide how a company should approach security and what security measures should be implemented.
D: The information security specialist may be the ones who implement the security measures. However, they should not decide how a company should approach security and what security measures should be implemented.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 101

QUESTION 23
The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:

A. Confidentiality, Integrity, and Entity (C.I.E.).
B. Confidentiality, Integrity, and Authenticity (C.I.A.).
C. Confidentiality, Integrity, and Availability (C.I.A.).
D. Confidentiality, Integrity, and Liability (C.I.L.).

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Fundamental Principles of Security which are to provide confidentiality, availability, and integrity, and Confidentiality (the CIA triad).

Incorrect Answers:
A: The three tenets do not include Entity.

B: The three tenets do not include Authenticity.
D: The three tenets do not include Liability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 22

QUESTION 24
Controlling access to information systems and associated networks is necessary for the preservation of their:

A. Authenticity, confidentiality and availability
B. Confidentiality, integrity, and availability.
C. Integrity and availability.
D. Authenticity, confidentiality, integrity and availability.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Information security is made up of the following main attributes:
- Availability - Prevention of loss of, or loss of access to, data and resources
- Integrity - Prevention of unauthorized modification of data and resources
- Confidentiality - Prevention of unauthorized disclosure of data and resources

Incorrect Answers:
A: Authenticity is an attribute that stems from the three main attributes.
C: Information security is made up of three main attributes, which includes confidentiality.
D: Authenticity is an attribute that stems from the three main attributes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 298, 299

QUESTION 25
What security model is dependent on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control

D. Non-discretionary access control

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory Access Control begins with security labels assigned to all resource objects on the system. These security labels contain two pieces of information - a classification (top secret, confidential etc.) and a category (which is essentially an indication of the management level, department or project to which the object is available).
Similarly, each user account on the system also has classification and category properties from the same set of properties applied to the resource objects. When a user attempts to access a resource under Mandatory Access Control the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's credentials match the MAC security label properties of the object access is allowed. It is important to note that both the classification and categories must match. A user with top secret classification, for example, cannot access a resource if they are not also a member of one of the required categories for that object.

Incorrect Answers:
A: Discretionary access control is not dependent on security labels.
B: Label-based access control is not one of the defined access control types.
D: Non-discretionary access control is not dependent on security labels.

References:
http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control

QUESTION 26
At which temperature does damage start occurring to magnetic media?

A. 100 degrees Fahrenheit or 37.7 degrees Celsius
B. 125 degrees Fahrenheit or 51.66 degrees Celsius
C. 150 degrees Fahrenheit or 65.5 degrees Celsius
D. 175 degrees Fahrenheit or 79.4 degrees Celsius

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

Maintaining appropriate temperature and humidity is important in any facility, especially facilities with computer systems. Improper levels of either can cause damage to computers and electrical devices.
Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down. Damage can start to occur on magnetic media at 100 degrees Fahrenheit or 37'7º Celsius.

Incorrect Answers:
B: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 125 degrees Fahrenheit. Therefore, this answer is incorrect.
C: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 150 degrees Fahrenheit. Therefore, this answer is incorrect.
D: Damage can start to occur on magnetic media at 100 degrees Fahrenheit, not 175 degrees Fahrenheit. Damage can start to occur in computer systems and peripheral devices at 175 degrees Fahrenheit. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 466

QUESTION 27
Which of the following access control models requires defining classification for objects?

A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

Incorrect Answers:
A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
B: Access in a DAC model is restricted based on the authorization granted to the users.
C: Identity-based access control is a type of DAC system that allows or prevents access based on the identity of the subject.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 28
In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?
A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The BellLaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. **The subject's clearance is compared to the object's classification and then specific rules are applied to control how subjectto-object interactions can take place.**
This model uses subjects, objects, access operations (read, write, and read/write), and security levels. Subjects and objects can reside at different security levels and will have relationships and rules dictating the acceptable activities between them.

Incorrect Answers:
B: The Biba Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. This is not what is described in the question.
C: An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. This is not what is described in the question.
D: The take-grant protection model is used to establish or disprove the safety of a given computer system that follows specific rules. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 229

QUESTION 29
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

A. B
B. A
C. C

D. D

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Level B: Mandatory Protection: Mandatory access control is enforced by the use of security labels. The architecture is based on the Bell-LaPadula security model, and evidence of reference monitor enforcement must be available.

Incorrect Answers:
B: Level A is defined as verified protection, not mandatory protection.
C: Level C is defined as discretionary protection, not mandatory protection.
D: Level D is defined as minimal security, not mandatory protection.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 395

QUESTION 30
Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

A. C
B. B
C. A
D. D

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book.
TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels:
A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Level C: Discretionary Protection: The C rating category has two individual assurance ratings within it. The higher the number of the assurance rating, the greater the protection.

Incorrect Answers:
B: Level B is defined as mandatory protection, not discretionary protection.
C: Level A is defined as verified protection, not discretionary protection.
D: Level D is defined as minimal security, not discretionary protection.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 394

QUESTION 31
Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

A. Division D
B. Division C
C. Division B
D. Division A

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal protection

Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Division D: Minimal Protection: There is only one class in Division D. It is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions.

Incorrect Answers:
B: Level C is defined as discretionary protection, not minimal protection.
C: Level B is defined as mandatory protection, not minimal protection.
D: Level A is defined as verified protection, not mandatory minimal.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392, 395

QUESTION 32
Which of the following establishes the minimal national standards for certifying and accrediting national security systems?

A. NIACAP
B. DIACAP
C. HIPAA
D. TCSEC

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.

Incorrect Answers:
B: The DoD Information Assurance Certification and Accreditation Process (DIACAP) is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply risk management to information systems (IS). This is not what is described in the question.
C: HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs. This is not what is described in the question.

D: Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. This is not what is described in the question.

References:
http://infohost.nmt.edu/~sfs/Regs/nstissi_1000.pdf

QUESTION 33
Which of the following places the Orange Book classifications in order from MOST secure to LEAST secure?

A. A, B, C, D
B. D, C, B, A
C. D, B, A, CD. C, D, B, A

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal security
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

Incorrect Answers:
B: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
C: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
D: Classification A represents the highest level of assurance, and D represents the lowest level of assurance.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 34
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.

C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A Trojan horse.

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:
- Improper oversight in the development of the product
- Improper implementation of access controls within the software
- Existence of a shared resource between the two entities which are not properly controlled

Incorrect Answers:
A: An undocumented backdoor that has been left by a programmer in an operating system could be used in a covert channel. However, this is not the BEST definition of a covert channel.
B: An open system port that should be closed could be used in a covert channel. However, an open port is not the definition of a covert channel.
D: A Trojan horse could be used in a covert channel. However, a Trojan horse is not the definition of a covert channel.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 378-379

QUESTION 35
Which of the following Orange Book ratings represents the highest level of trust?

A. B1
B. B2
C. F6
D. C2

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protectionD. Minimal security
Classification A represents the highest level of assurance, and D represents the lowest level of assurance.
Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating. The classes with higher numbers offer a greater degree of trust and assurance. So B2 would offer more assurance than B1, and C2 would offer more assurance than C1.

Incorrect Answers:
A: B1 has a lower level of trust than B2.
C: F6 is not a valid rating.
D: Division C has a lower level of trust than division B.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 36
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

A. A
B. D
C. E
D. F

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

Classification A represents the highest level of assurance, and D represents the lowest level of assurance. Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating.
There is only one class in Division D. It is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions.
Incorrect Answers:
A: Division A is the highest level.
C: The lowest division/level (reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions) is D, not E.
D: The lowest division/level (reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions) is D, not F.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-393

QUESTION 37
Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The U.S. Department of Defense developed the Trusted Computer System Evaluation Criteria (TCSEC), which was used to evaluate operating systems, applications, and different products. These evaluation criteria are published in a book known as the Orange Book. TCSEC provides a classification system that is divided into hierarchical divisions of assurance levels: A. Verified protection
B. Mandatory protection

C. Discretionary protection
D. Minimal security

C1: Discretionary Security Protection: Discretionary access control is based on individuals and/or groups. It requires a separation of users and information, and identification and authentication of individual entities. Some type of access control is necessary so users can ensure their data will not be accessed and corrupted by others. The system architecture must supply a protected execution domain so privileged system processes are not adversely affected by lower-privileged processes. There must be specific ways of validating the system's operational integrity. The documentation requirements include design documentation, which shows that the system was built to include protection mechanisms, test documentation (test plan and results), a facility manual (so companies know how to install and configure the system correctly), and user manuals.

Incorrect Answers:
A: Division C, not D deals with discretionary protection.
C: Division C, not B deals with discretionary protection.
D: Division C, not A deals with discretionary protection.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-394

QUESTION 38
Which of the following computer crime is MORE often associated with INSIDERS?

A. IP spoofing
B. Password sniffing
C. Data diddling
D. Denial of service (DoS)

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

Incorrect Answers:
A: IP Spoofing attacks are more commonly performed by outsiders.
B: Password sniffing can be performed by insiders or outsiders. However, Data Diddling is MORE commonly performed by insiders.
D: Most Denial of service attacks occur over the internet and are performed by outsiders.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 39
Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Employees represent the leading source of computer crime losses. This can be through hardware theft, data theft, physical damage and interruptions to services. Laptop theft is increasing at incredible rates each year. They have been stolen for years, but in the past they were stolen mainly to sell the hardware. Now laptops are also being stolen to gain sensitive data for identity theft crimes. Since employees use laptops as they travel, they may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands.

Incorrect Answers:
A: Losses caused by hackers can be high. However, this is rare in comparison to losses caused by employees.
B: Losses caused by industrial saboteurs can be high. However, this is very rare in comparison to losses caused by employees.
C: Foreign intelligence officers are not a cause of computer crime losses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 457

QUESTION 40
Which of the following term BEST describes a weakness that could potentially be exploited?

A. Vulnerability

B. Risk
C. Threat
D. Target of evaluation (TOE)

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is the absence of a countermeasure or a weakness in an in-place countermeasure, and can therefore be exploited.

Incorrect Answers:
B: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.
C: A threat is any potential danger that is associated with the exploitation of a vulnerability.
D: Target Of Evaluation (TOE) refers to the product or system that is the subject of the evaluation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 26
https://en.wikipedia.org/wiki/Common_Criteria

QUESTION 41
Which of the following BEST describes an exploit?

A. An intentional hidden message or feature in an object such as a piece of software or a movie.
B. A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software.
C. An anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer.
D. A condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

An exploit refers to a piece of software or data, or a sequence of commands that takes advantage of a bug or vulnerability with the aim of causing unplanned or unexpected behavior to take place on computerized hardware, or its software.

Incorrect Answers:
A: An intentional hidden message, in-joke, or feature in a work such as a computer program, web page, video game, movie, book, or crossword is known as a virtual Easter egg.
C: The anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer is known as buffer overflow.
D: In computing, a condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system is known as a crash.

References:
https://en.wikipedia.org/wiki/Exploit_%28computer_security%29
https://www.quora.com/topic/Easter-Eggs-media
https://en.wikipedia.org/wiki/Buffer_overflow http://www.article-buzz.com/Article/Avoiding-Data-Loss---A-Guide-To-The-Best-Online-Data-Storage-Websites/328757#.Vjc757crKHu

QUESTION 42
Virus scanning and content inspection of S/MIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
E-mail encryption solutions such as S/MIME have been available for a long time. These encryption solutions have seen varying degrees of adoption in organizations of different types. However, such solutions present some challenges:
Inability to apply messaging policies: Organizations also face compliance requirements that require inspection of messaging content to make sure it adheres to messaging policies. However, messages encrypted with most client-based encryption solutions, including S/MIME, prevent content inspection on the server. Without content inspection, an organization can't validate that all messages sent or received by its users comply with messaging policies.
Decreased security: Antivirus software is unable to scan encrypted message content, further exposing an organization to risk from malicious content such as viruses and worms. Encrypted messages are generally considered to be trusted by most users, thereby increasing the likelihood of a virus spreading throughout your organization.

Incorrect Answers:
B: Virus scanning and content inspection of S/MIME encrypted e-mail is not possible even with a key recovery scheme of all user keys.
C: Virus scanning and content inspection of S/MIME encrypted e-mail is not possible even if X509 Version 3 certificates are used.
D: Using "brute force" decryption on S/MIME encrypted e-mail for the purpose of virus scanning and content inspection is not practical and unlikely to be successful.

References: https://technet.microsoft.com/en-us/library/dd638122(v=exchg.150).aspx

QUESTION 43
What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Steganography is a method of hiding data in another media type so the very existence of the data is concealed.
Only the sender and receiver are supposed to be able to see the message because it is secretly hidden in a graphic, wave file, document, or other type of media. The message is not encrypted, just hidden. Encrypted messages can draw attention because it tells the bad guy, “This is something sensitive.” A message hidden in a picture of your grandmother would not attract this type of attention, even though the same secret message can be embedded into this image. Steganography is a type of security through obscurity.

Incorrect Answers:
A: Clustering describes multiple instances of a component working together as a single unit. This is not what is described in the question.
C: Cryptology is the study of cryptography and cryptanalysis. This is not what is described in the question.
D: Vernam cipher is another name for one-time pad because one-time pad was invented by Gilbert Vernam. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 774-775

QUESTION 44
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Steganography allows you to hide data in another media type, concealing the very existence of the data.

Incorrect Answers:
B, D: Alternate data stream (ADS) is a feature of Windows New Technology File System (NTFS) that includes metadata for locating a specific file by author or title.
C: Encryption is a method of transforming readable data into a form that appears to be random and unreadable.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 774

http://searchsecurity.techtarget.com/definition/alternate-data-stream

QUESTION 45
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Digital watermarking is defined as “Computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data -- text, graphics, images, video, or audio -- and for detecting or extracting the marks later.”

A "digital watermark", i.e., the set of embedded bits, is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. Depending on the particular technique that is used, digital watermarking can assist in proving ownership, controlling duplication, tracing distribution, ensuring data integrity, and performing other functions to protect intellectual property rights.

Incorrect Answers:
A: Steganography is a method of hiding data in another media type so the very existence of the data is concealed. Digital Watermarking is considered to be a type of steganography. However, steganography is not what is described in the question.
C: A digital envelope is another term used to describe hybrid cryptography where a message is encrypted with a symmetric key and the symmetric key is encrypted with an asymmetric key. This is not what is described in the question.
D: A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. This is not what is described in the question.

References:
http://tools.ietf.org/html/rfc4949

QUESTION 46
What is Dumpster Diving?

A. Going through dust bin
B. Running through another person's garbage for discarded document, information and other various items that could be used against that person or company
C. Performing media analysis
D. performing forensics on the deleted items

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Dumpster diving refers to the concept of rummaging through a company or individual’s garbage for discarded documents, information, and other precious items that could then be used in an attack against that company or person.

Incorrect Answers:
A: Dumpster Diving is more specific than going through dust bins.
C: Dumpster Diving does not refer to media analysis.
D: Dumpster Diving does not refer to forensics on deleted items.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1060

QUESTION 47
The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?

A. Test equipment is easily damaged.
B. Test equipment can be used to browse information passing on a network.
C. Test equipment is difficult to replace if lost or stolen.
D. Test equipment must always be available for the maintenance personnel.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A Protocol Analyzer (also known as a packet sniffer) is a useful tool for testing or troubleshooting network communications.
A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing.
The ability to browse information passing on a network is a security risk which means access to a protocol analyzer should be carefully managed and therefore addressed by security policy.
Incorrect Answers:
A: Damage to test equipment is not a 'security' risk so does not need to be addressed by security policy.
C: Test equipment is generally not difficult to replace if lost or stolen. Even if it was, that would not constitute a 'security' risk so it would not need to be addressed by security policy.
D: The need for test equipment to always be available for the maintenance personnel would not constitute a 'security' risk so it would not need to be addressed by security policy.

QUESTION 48
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?

A. A threat.
B. A vulnerability.
C. A risk.
D. An exposure.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is defined as “the absence or weakness of a safeguard that could be exploited”.
A vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 49
Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

A. A risk.
B. A residual risk.
C. An exposure.
D. A countermeasure.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

Incorrect Answers:
B: Residual risk is the risk that remains after countermeasures have been implemented.
C: An exposure is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages.
D: A countermeasure is a step taken to mitigate a risk.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 50
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Personnel represent the leading source of computer crime losses. This can be through hardware theft, data theft, physical damage and interruptions to services. Laptop theft is increasing at incredible rates each year. They have been stolen for years, but in the past they were stolen mainly to sell the hardware. Now laptops are also being stolen to gain sensitive data for identity theft crimes. Since employees use laptops as they travel, they may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands.

Incorrect Answers:
A: Losses caused by industrial outside espionage can be high. However, this is very rare in comparison to losses caused by personnel.
B: Losses caused by hackers can be high. However, this is rare in comparison to losses caused by personnel.
D: Equipment failure can be a cause of security issues. However, security issues caused by personnel are more common.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 457

QUESTION 51
Passwords can be required to change monthly, quarterly, or at other intervals:

A. depending on the criticality of the information needing protection.
B. depending on the criticality of the information needing protection and the password's frequency of use.
C. depending on the password's frequency of use.
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

A password that is the same for each log-on is called a static password. A password that changes with each log-on is termed a dynamic password. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.

Incorrect Answers:
A: This answer is not complete. Passwords can also be required to change depending on the password's frequency of use.
C: This answer is not complete. Passwords can also be required to change depending on the criticality of the information needing protection.
D: Passwords CAN be required to change depending on the criticality of the information needing protection.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 52
Computer security should be first and foremost which of the following?

A. Cover all identified risks
B. Be cost-effective.
C. Be examined in both monetary and non-monetary terms.
D. Be proportionate to the value of IT systems.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Each organization is different in its size, security posture, threat profile, and security budget. One organization may have one individual responsible for information risk management (IRM) or a team that works in a coordinated manner. The overall goal of the team is to ensure the company is protected in the most cost-effective manner.

Incorrect Answers:
A: Not all identified risks are mitigated. Some risks are accepted.
C: It is not true that computer security should be first and foremost examined in both monetary and non-monetary terms.
D: It is not true that computer security should be first and foremost proportionate to the value of IT systems. The value of IT systems does not necessarily mean that more or less security is required.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 87

QUESTION 53
IT security measures should:

A. be complex.
B. be tailored to meet organizational security goals.
C. make sure that every asset of the organization is well protected.
D. not be developed in a layered fashion.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The National Institute of Standards and Technology (NIST) defines 33 IT Security principles.
Principle 8 states:
"Implement tailored system security measures to meet organizational security goals."
In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

Incorrect Answers:
A: According to the NIST IT security principles, IT security measures should strive for simplicity not be complex.
C: According to the NIST IT security principles, you should not implement unnecessary security mechanisms. Protecting 'every' asset may be unnecessary.
D: According to the NIST IT security principles, IT security measures should be developed in a layered fashion.

References: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf, p.10

QUESTION 54
The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?

A. Threat
B. Exposure
C. Vulnerability
D. Risk

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A vulnerability is defined as “the absence or weakness of a safeguard that could be exploited”.
A vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be a software, hardware, procedural, or human weakness that can be exploited. A vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

Incorrect Answers:
A: A threat is any potential danger that is associated with the exploitation of a vulnerability.
B: An exposure is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages.
D: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26
QUESTION 55
What can be defined as an event that could cause harm to the information systems?

A. A risk

B. A threat
C. A vulnerability
D. A weakness

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A threat is any potential danger that is associated with the exploitation of a vulnerability. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a threat agent. A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information.

Incorrect Answers:
A: A risk is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.
C: A vulnerability is the absence or weakness of a safeguard that could be exploited.
D: A weakness is the state of something being weak. For example, a weak security measure would be a vulnerability. A weakness is not what is described in this question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 26

QUESTION 56
Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A. Business and functional managers
B. IT Security practitioners
C. System and information owners
D. Chief information officer

Correct Answer: C
Section: Asset Security
Explanation
Explanation/Reference:
Explanation:

Both the system owner and the information owner (data owner) are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner. The data owner (information owner) is usually a member of management who is in charge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information. The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data she is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers.

Incorrect Answers:
A: Business and functional managers are not responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
B: IT Security practitioners implement the security controls. However, they are not ultimately responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.
D: The Chief Information Officer (CIO) is responsible for the strategic use and management of information systems and technology within the organization. The CIO is not responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 121

QUESTION 57
Which of the following BEST defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:

Add-on security is defined as “Security protection mechanisms that are hardware or software retrofitted to a system to increase that system’s protection level.”
Incorrect Answers:
A: Add-on security can be physical security (hardware) but it is often software as well.
B: An add-on is something ‘added’ to an existing system; it is not an integral part of a system.
C: Add-on security can be a layer of security. However, layered security does not refer specifically to security add-ons.

QUESTION 58
Which of the following is BEST practice to employ in order to reduce the risk of collusion?

A. Least Privilege
B. Job Rotation
C. Separation of Duties
D. Mandatory Vacations

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The objective of separation of duties is to ensure that one person acting alone cannot compromise the company’s security in any way. High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the company does not need to put a dangerously high level of trust in certain individuals. For fraud to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time. Job rotation in the workplace is a system where employees work at several jobs in a business, performing each job for a relatively short period of time. By moving people willing to collude to commit fraud, we can reduce the risk of collusion.

Incorrect Answers:
A: Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more. It is not the best control for reducing collusion.
C: Separation of Duties prevents one person being able to commit fraud. With separation of duties, collusion between two or more people would be required to commit the fraud. However, separation of duties does not prevent the collusion.
D: Mandatory vacations are a way of detecting fraud. If a fraudulent activity stops while an employee is on vacation, it is easy to determine who was committing the fraud. Mandatory vacations do not prevent the collusion.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1235-1236

QUESTION 59

What are the four domains that make up CobiT?

A. Plan and Organize, Maintain and Implement, Deliver and Support, and Monitor and Evaluate
B. Plan and Organize, Acquire and Implement, Support and Purchase, and Monitor and Evaluate
C. Acquire and Implement, Deliver and Support, Monitor, and Evaluate
D. Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs. CobiT is broken down into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

Incorrect Answers:
A: Maintain and Implement is not one of the four domains; it should be Acquire and Implement.
B: Support and Purchase is not one of the four domains; it should be Deliver and Support.
C: This answer is missing the first domain, Plan and Organize.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 55

QUESTION 60
CobiT was developed from the COSO framework. Which of the choices below best describe the COSO's main objectives and purpose?

A. COSO main purpose is to help ensure fraudulent financial reporting cannot take place in an organization
B. COSO main purpose is to define a sound risk management approach within financial companies.
C. COSO addresses corporate culture and policy development.
D. COSO is risk management system used for the protection of federal systems.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
COSO is a model for corporate governance, and CobiT is a model for IT governance. COSO deals more at the strategic level, while CobiT focuses more at the operational level. You can think of CobiT as a way to meet many of the COSO objectives, but only from the IT perspective. COSO deals with non-IT items also, as in company culture, financial accounting principles, board of director responsibility, and internal communication structures. COSO was formed to provide sponsorship for the National Commission on Fraudulent Financial Reporting, an organization that studies deceptive financial reports and what elements lead to them.
There have been laws in place since the 1970s that basically state that it was illegal for a corporation to cook its books (manipulate its revenue and earnings reports), but it took the Sarbanes–Oxley Act (SOX) of 2002 to really put teeth into those existing laws. SOX is a U.S. federal law that, among other things, could send executives to jail if it was discovered that their company was submitting fraudulent accounting findings to the Security Exchange Commission (SEC). SOX is based upon the COSO model, so for a corporation to be compliant with SOX, it has to follow the COSO model. Companies commonly implement ISO/IEC 27000 standards and CobiT to help construct and maintain their internal COSO structure.

Incorrect Answers:
B: It is not the main purpose of COSO to define a sound risk management approach within financial companies.
C: It is not the main purpose of COSO to address corporate culture and policy development.
D: COSO is not a risk management system used for the protection of federal systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 59

QUESTION 61
What are the three MOST important functions that Digital Signatures perform?

A. Integrity, Confidentiality and Authorization
B. Integrity, Authentication and Nonrepudiation
C. Authorization, Authentication and Nonrepudiation
D. Authorization, Detection and Accountability

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Digital Signatures can be used to provide Integrity, Authentication and Nonrepudiation.

A digital signature is a hash value that has been encrypted with the sender's private key.

If Kevin wants to ensure that the message he sends to Maureen is not modified and he wants her to be sure it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message, and then Kevin would encrypt that hash value with his private key. When Maureen receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Kevin's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Kevin because the value was encrypted with his private key. The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation.

Incorrect Answers:
A: Digital signatures do not provide Confidentiality or Authorization.
C: Digital signatures do not provide Authorization.
D: Digital signatures do not provide Authorization, Detection or Accountability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829

QUESTION 62
Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data loss often lead to business failure. Data loss has the most negative impact on business functions.

Incorrect Answers:
A: Software can be reinstalled and hardware can replaced, and are therefore less critical compared to loss of data.
C: Communication links can quite easily put back again, compared to loss of data.
D: Loss of applications is Critical as they can be reinstalled.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 957

QUESTION 63
Which one of the following is used to provide authentication and confidentiality for e-mail messages?

A. Digital signature
B. PGP
C. IPSEC AH
D. MD4

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Incorrect Answers:
A: Digital signature is used only to ensure the origin, but cannot do any authentication.
C: IPSec can provide encryption and authentication, but work on packets not on email messages.
D: MD4 is an algorithm used to verify data integrity, but it cannot be used to provide authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 850-851

QUESTION 64
Which of the following access control models is based on sensitivity labels?

A. Discretionary access control
B. Mandatory access control
C. Rule-based access control
D. Role-based access control

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:

Explanation:
Mandatory Access control is considered nondiscretionary and is based on a security label system

Incorrect Answers:
A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: Rule-based access control is considered nondiscretionary because the users cannot make access decisions based upon their own discretion.
D: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 65
Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

A. Discretionary Access Control
B. Mandatory Access Control
C. Sensitive Access Control
D. Role-based Access Control

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.

Incorrect Answers:
B: Mandatory Access control is considered nondiscretionary and is based on a security label system
C: Sensitive access control is not a valid access control.
D: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 66
Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?

A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.
To prevent possible intrusion or damage from wardialing attacks, you should configure the system to require authentication before a network connection can be established. This will ensure that an attacker cannot gain access to the network without knowing a username and password.

Incorrect Answers:
A: Monitoring wardialing attacks would not prevent an attacker gaining access to the network. It would just tell you that at attack has happened.
C: Making sure only necessary phone numbers are made public will not protect against intrusion. An attacker would still be able to gain access through one of the 'necessary' phone numbers.
D: Using completely different numbers for voice and data accesses will not protect against intrusion. An attacker would still be able to gain access through one of the data access phone numbers.

References:
http://en.wikipedia.org/wiki/War_dialing

QUESTION 67
Which of the following access control models introduces user security clearance and data classification?

A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control

Correct Answer: D

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

Incorrect Answers:
A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
B: Access in a DAC model is restricted based on the authorization granted to the users.
C: Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228
http://www.answers.com/Q/What_is_Non_discretionary_access_control

QUESTION 68
Kerberos can prevent which one of the following attacks?

A. Tunneling attack.
B. Playback (replay) attack.
C. Destructive attack.
D. Process attack.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
In a Kerberos implementation that is configured to use an authenticator, the user sends to the server her identification information, a timestamp, as well as sequence number encrypted with the session key that they share. The server then decrypts this information and compares it with the identification data the KDC sent to it regarding this requesting user. The server will allow the user access if the data is the same. The timestamp is used to help fight against replay attacks.

Incorrect Answers:
A: Tunneling attack is not a valid type of attack with regards to Kerberos.
C: Destructive attack is not a valid type of attack with regards to Kerberos.
D: Process attack is not a valid type of attack with regards to Kerberos.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 212

QUESTION 69
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Password sniffing sniffs network traffic with the hope of capturing passwords being sent between computers.
Incorrect Answers:
A: Data diddling refers to the alteration of existing data.
C: Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.
D: Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 599, 1059, 1060

QUESTION 70
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

A. active attack.
B. outside attack.
C. inside attack.
D. passive attack.

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
An attack by an authorized user is known as an inside attack.
An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.
Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.
An insider attack is also known as an insider threat.

Incorrect Answers:
A: In an active attack, the attacker attempts to make changes to data on the target or data as it is transmitted to the target. An attack by an authorized user could be an active type of attack but it is not known as an active attack. B: An attack by an authorized user is not known as an outside attack.
D: In a passive attack, the attacker attempts to learn information but does not affect resources. An attack by an authorized user could be passive in nature but it is not known as a passive attack.
References: https://www.techopedia.com/definition/26217/insider-attack

QUESTION 71
MOST access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
In security circles, people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel cause more serious and hard-to-detect security issues than hacker attacks, outside espionage, or equipment failure.
A common accidental access violation is a user discovering a feature of an application that they should not be accessing.

Incorrect Answers:
B: Most access violations are not caused by internal hackers.
C: Most access violations are not caused by external hackers.
D: Most access violations are not related to Internet.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 129

QUESTION 72
Which of the following tools is less likely to be used by a hacker?

A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Tripwire is a tool that detects when files have been altered by regularly recalculating hashes of them and storing the hashes in a secure location. The product triggers when changes to the files have been detected. By using cryptographic hashes, tripwire is often able to detect subtle changes. Contrast: The simplistic form of tripwire is to check file size and last modification time. l0phtcrack, OphCrack and John the Ripper are password cracking tools and are therefore more likely to be used by hackers than Tripwire.

Incorrect Answers:
A: l0phtcrack is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, hybrid attacks, and rainbow tables. It is more likely to be used by a hacker than Tripwire.
C: Ophcrack is a free Windows password cracker based on rainbow tables. It is more likely to be used by a hacker than Tripwire.
D: John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. It is more likely to be used by a hacker than Tripwire.

References:
http://linux.about.com/cs/linux101/g/tripwire.htm

QUESTION 73
What refers to legitimate users accessing networked services that would normally be restricted to them?

A. Spoofing
B. Piggybacking
C. Eavesdropping
D. Logon abuse

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Logon abuse refers to legitimate users accessing networked services that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who may be internal to the network, legitimate users of a different system, or users who have a lower security classification.

Incorrect Answers:
A: Spoofing refers to an attacker deliberately inducing a user (subject) or device (object) into taking an incorrect action by giving it incorrect information. This is not what is described in the question.
B: Piggy-backing refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A user leaves a session open or incorrectly logs off, enabling an attacker to resume the session. This is not what is described in the question.
C: Eavesdropping is the unauthorized interception of network traffic. This is not what is described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 173

QUESTION 74
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What BEST describes this scenario?

A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Privilege is a term used to describe what a user can do on a computer or system. It covers rights, access and permissions. A user who has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill is said to have 'excessive privileges'.

Incorrect Answers:
A: Rights are just one aspect of what a user can do with a computer or system. Access and permissions are other aspects. Privileges cover all three.
B: Access is just one aspect of what a user can do with a computer or system. Rights and permissions are other aspects. Privileges cover all three.
C: Permissions are just one aspect of what a user can do with a computer or system. Access and rights are other aspects. Privileges cover all three.

QUESTION 75
Which answer BEST describes information access permissions where, unless the user is specifically given access to certain data they are denied any access by default?

A. Implicit Deny
B. Explicit Deny
C. Implied Permissions
D. Explicit Permit

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Implicit Deny means that a user is denied access by default. To be given access, the user must (explicitly) be permitted access to the resource.

Incorrect Answers:
B: Explicit Deny means the user has been denied access to the data. It does not mean the user is denied by default.

C: Implied Permissions does not describe information access permissions where, unless the user is specifically given access to certain data they are denied any access by default.
D: Explicit Permit means that a user is specifically given access to the data. However, it does not mean that the user is denied by default.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 205

QUESTION 76
Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating?

A. Security administrators
B. Operators
C. Data owners
D. Data custodians

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Typical security administrator functions may include the following:
- Setting user clearances, initial passwords, and other security characteristics for new users
- Changing security profiles for existing users
- Setting or changing file sensitivity labels
- Setting the security characteristics of devices and communications channels
- Reviewing audit data

Incorrect Answers:
B: System operators provide day-to-day operations of computer systems. They do not perform the tasks listed in the question.
C: Data owners are primarily responsible for determining the data's sensitivity or classification levels. They can also be responsible for maintaining the information's accuracy and integrity. They do not perform the tasks listed in the question.
D: Data custodians are delegated the responsibility of protecting data by its owner. They do not perform the tasks listed in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 211

QUESTION 77
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Incorrect Answers:
A: Implementing the initial program load is a function that should be performed by an operator.
B: Monitoring execution of the system is a function that should be performed by an operator.
D: Controlling job flow is a function that should be performed by an operator.

QUESTION 78
Which of the following should be performed by an operator?
A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.

Incorrect Answers:
A: Changing profiles should not be performed by an operator; this should be performed by a security administrator.
B: Approving changes should not be performed by an operator; this should be performed by a change control analyst or panel.
C: Adding and removal of users should not be performed by an operator; this should be performed by a security administrator.

QUESTION 79
Which of the following is NOT appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they're no longer needed.
B. Deleting files on disk before reusing the space.
C. Clearing memory blocks before they are allocated to a program or data.
D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them.
Deleting files on disk before reusing the space does not meet this requirement and is therefore not appropriate in addressing object reuse.
Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.

Incorrect Answers:
A: Degaussing magnetic tapes when they're no longer needed protects files from unauthorized access by destroying the data on the tapes. This is a valid method of addressing object reuse.
C: Clearing memory blocks before they are allocated to a program or data removes any residual data from the memory thus preventing unauthorized access. This is a valid method of addressing object reuse.
D: Clearing buffered pages, documents, or screens from the local memory of a terminal or printer removes any residual data from the memory thus preventing unauthorized access. This is a valid method of addressing object reuse.

QUESTION 80
What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.

C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.

Object reuse refers to the allocation or reallocation of system resources to a user or, more appropriately, to an application or process. Applications and services on a computer system may create or use objects in memory and in storage to perform programmatic functions. In some cases, it is necessary to share these resources between various system applications. However, some objects may be employed by an application to perform privileged tasks on behalf of an authorized user or upstream application. If object usage is not controlled or the data in those objects is not erased after use, they may become available to unauthorized users or processes.

Disclosure of residual data and Unauthorized obtaining of a privileged execution state are both a problem with shared memory and resources. Not clearing the heap/stack can result in residual data and may also allow the user to step on somebody's session if the security token/identify was maintained in that space. This is generally more malicious and intentional than accidental though. The MOST common issue would be Disclosure of residual data.

Incorrect Answers:
B: Unauthorized obtaining of a privileged execution state is not a problem with Object Reuse.
C: A covert channel is a communication path. Data leakage would not be a problem created by Object Reuse. In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, originated in 1973 by Lampson is defined as "(channels) not intended for information transfer at all, such as the service program's effect on system load." to distinguish it from Legitimate channels that are subjected to access controls by COMPUSEC.
D: Denial of service through a deadly embrace is not a problem with Object Reuse.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 424 https://www.fas.org/irp/nsa/rainbow/tg018.htm http://en.wikipedia.org/wiki/Covert_channel

QUESTION 81
Which of the following categories of hackers poses the greatest threat?

A. Disgruntled employees
B. Student hackers
C. Criminal hackers

D. Corporate spies

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Employee sabotage can become an issue if an employee is knowledgeable enough about the IT infrastructure of an organization, has sufficient access.

Incorrect Answers:
B: Student hackers are a lesser threat as a disgruntled employee already has access to the system.
C: A disgruntled employee is a larger threat compared to a criminal hacker as the employee already has access to the system.
D: A disgruntled employee is a larger threat compared to a corporate spy as the employee already has access to the system.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 602

QUESTION 82
At which of the basic phases of the System Development Life Cycle are security requirements formalized?

A. Disposal
B. System Design Specifications
C. Development and Implementation
D. Functional Requirements Definition

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Requirements, including security requirements, are formalized in the Functional Requirements Definition phase.

Incorrect Answers:
A: Disposal activities need to ensure that an orderly termination of the system takes place and that all necessary data are preserved. Security requirements are not formalized at the disposal phase.

B: Within the Systems Development Life Cycle (DSLC) model the design phase, also known as the System Design Specifications phase, transforms requirements, including the security requirements, into a complete System Design Document.
C: In the implementation phase the system is implemented into a product production environment. The security requirements have already been developed long before this phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1095

QUESTION 83
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Within the Systems Development Life Cycle (DSLC) model the design phase, also known as the security requirement phase, transforms requirements, including the security requirements, into a complete System Design Document.

Incorrect Answers:
A: The operation phase describes tasks to operate in a production environment, and is not concerned with development of security requirements.
B: The initiation phase starts when a sponsor identifies a need or an opportunity. During this phase a Concept Proposal, but no security requirements, is created.
D: In the implementation phase the system is implemented into a product production environment. The security requirements have already been developed long before this phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1095
QUESTION 84
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

A. Development/acquisition
B. Implementation
C. Initiation

D. Maintenance

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Within the SDLC model during the initiation phase the need for a new system is defined. The initiation phase includes security categorization and preliminary risk assessment including a security policy.
The security policy is a documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability, and integrity goals.

Incorrect Answers:
A: The Development/acquisition phase does not establish a good security policy; instead it includes risk assessment and risk analysis.
B: The implementation phase includes security certification and security accreditation. Establishing a good security policy is not included in the implementation phase.
D: The maintenance phase include continuous monitoring, and configuration management and control. It does include creation of a security policy.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1088, 1422

QUESTION 85
When considering an IT System Development Life-cycle, security should be:

A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Correct Answer: C
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
Within the System Development Life-cycle (SDLC) model, security is critical in each phase of the life cycle.

Incorrect Answers:
A: Security is critical to each phase of the SDLC model, not only the initiation phase.

B: Security is critical to each phase of the SDLC model, not only the development phase.
D: Security is critical to each phase of the SDLC model, and is not added when the design is completed.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 1087

QUESTION 86
Risk reduction in a system development life-cycle should be applied:

A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Risk reduction should be applied equally to the initiation phase, the development phase, and to the disposal phase.
Within the initiation phase a preliminary risk assessment should be carried out to develop an initial description of the confidentiality, integrity, and availability requirements of the system.
The development phase include formal risk assessment which identifies vulnerabilities and threats in the proposed system and the potential risk levels as they pertain to confidentiality, integrity, and availability. This builds upon the initial risk assessment carried out in the previous phase (the initiation phase). The results of this assessment help the team build the system's security plan.
Disposal activities need to ensure that an orderly termination of the system takes place and that all necessary data are preserved. The storage medium of the system may need to be degaussed, put through a zeroization process, or physically destroyed.

Incorrect Answers:
A: Risk reduction should be applied to all phases equally, not mostly to the initiation phase.
B: Risk reduction should be applied to all phases equally, not mostly to the development phase.
C: Risk reduction should be applied to all phases equally, not mostly to the disposal phase.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 1091-1093

QUESTION 87
Who developed one of the first mathematical models of a multilevel-security computer system?

A. Diffie and Hellman.
B. Clark and Wilson.
C. Bell and LaPadula.
D. Gasser and Lipner.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access.

Incorrect Answers:
A: Diffie and Hellman developed the first asymmetric key agreement algorithm, not the first multilevel security policy computer system.
B: The question asks for the developers of the first mathematical models of a multilevel-security computer system. This was Bell and LaPadula, not Clark and Wilson.
D: The question asks for the developers of the first mathematical models of a multilevel-security computer system. This was Bell and LaPadula, not Gasser and Lipner.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 369, 812

QUESTION 88
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
The mechanism that automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters is known as an auxiliary station alarm.
Alarm systems may have auxiliary alarms that ring at the local fire or police stations. Most central station systems include this feature, which requires permission form the local authorities before implementation.

Incorrect Answers;
A: Central Station Systems are operated and monitored around the clock by private security firms. The central stations are signaled by detectors over leased lines. Most central station systems include auxiliary alarms that ring at the local fire or police stations. However, the name of the alarm system that rings at the local fire or police stations is 'auxiliary alarm'. Therefore, this answer is incorrect.
B: Proprietary Systems are similar to the central station systems, except that the monitoring system is owned and operated by the customer. Proprietary alarm is not name of the alarm that rings at the local fire or police stations. Therefore, this answer is incorrect.
C: A remote station alarm is not the alarm that rings at the local fire or police stations. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 474

QUESTION 89
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With the Clark–Wilson model, users are unable to modify critical data (CDI) directly. Users have to be authenticated to a piece of software, and the software procedures (TPs) will carry out the operations on behalf of the user.

Incorrect Answers:
A: The Biba model allows access to sensitive data based on a lattice of integrity levels.
B: The Bell-LaPadula model allows access to sensitive data based on a lattice of security levels.
D: The information flow model, on which both the Bell-LaPadula and Biba models are based, allows direct access to data.
References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 369-378 https://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 90
What security model implies a central authority that defines rules and sometimes global rules, dictating what subjects can have access to what objects?

A. Flow Model
B. Discretionary access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task-based). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual's role or title within the organization. These access controls do not need to be changed whenever a new person takes over that role. Another type of non-discretionary access control is lattice-based access control. In this type of control, a lattice model is applied. In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. To apply this concept to access control, the pair of elements is the subject and object, and the subject has the greatest lower bound and the least upper bound of access rights to an object.

Incorrect Answers:
A: A flow model does not use a central authority that defines rules and sometimes global rules, dictating what subjects can have access to what objects. B: Discretionary access control does not use a central authority that defines rules and sometimes global rules, dictating what subjects can have access to what objects.
C: Mandatory access control does not use a central authority that defines rules and sometimes global rules, dictating what subjects can have access to what objects.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 48

QUESTION 91
Which of the following is not a physical control for physical security?

A. lighting

B. fences C. training
D. facility construction materials

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Training is an administrative control, not a physical control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Lighting is an example of a physical control. Therefore, this answer is incorrect.
B: Fences are an example of a physical control. Therefore, this answer is incorrect.
D: Facility construction materials are an example of a physical control. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 92
Which access control model would a lattice-based access control model be an example of?

A. Mandatory access control.
B. Discretionary access control.

C. Non-discretionary access control.
D. Rule-based access control.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A lattice-based access control model, which is a type of label-based mandatory access control model, is used to define the levels of security that an object may have and that a subject may have access to.

Incorrect Answers:
B: Access in a DAC model is restricted based on the authorization granted to the users, not on their security labels.
C: Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network, not on their security labels.
D: Rule-based access control makes use of explicit rules that specify what can and cannot happen between a subject and an object, not on their security labels.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228 https://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 93
Which of the following is an example of discretionary access control?

A. Identity-based access control
B. Task-based access control
C. Role-based access control
D. Rule-based access control

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Identity-based access control is a type of DAC system that allows or prevents access based on the identity of the subject.

Incorrect Answers:
B: Task-based access control is a non-discretionary access control model, which is based on the tasks each subject must perform.

C: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
D: Rule-based access control makes use of explicit rules that specify what can and cannot happen between a subject and an object, not on their security labels.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 94
Which of the following would be used to implement Mandatory Access Control (MAC)?

A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A lattice is a mathematical construct that is built upon the notion of a group. The most common definition of the lattice model is “a structure consisting of a finite partially ordered set together with least upper and greatest lower bound operators on the set.” Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching: - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Incorrect Answers:
A: Clark-Wilson Access Control is not used to implement Mandatory Access Control (MAC).
B: Role-based Access Control is not used to implement Mandatory Access Control (MAC).
D: User dictated Access Control is not used to implement Mandatory Access Control (MAC).

References:
https://en.wikipedia.org/wiki/Computer_access_control

QUESTION 95

For maximum security design, what type of fence is most effective and cost-effective method (Foot is being used as measurement unit below)?

A. 3' to 4' high.
B. 6' to 7' high.
C. 8' high and above with strands of barbed wire.
D. Double fencing

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Fences come in varying heights, and each height provides a different level of security:

- Fences three to four feet high only deter casual trespassers.
- Fences six to seven feet high are considered too high to climb easily.
- Fences eight feet high (possibly with strands of barbed or razor wire at the top) means you are serious about protecting your property. They often deter the more determined intruder.

The barbed wire on top of fences can be tilted in or out, which also provides extra protection. If the organization is a prison, it would have the barbed wire on top of the fencing pointed in, which makes it harder for prisoners to climb and escape. If the organization is a military base, the barbed wire would be tilted out, making it harder for someone to climb over the fence and gain access to the premises.
Critical areas should have fences at least eight feet high to provide the proper level of protection. The fencing should not sag in any areas and must be taut and securely connected to the posts. The fencing should not be easily circumvented by pulling up its posts. The posts should be buried sufficiently deep in the ground and should be secured with concrete to ensure the posts cannot be dug up or tied to vehicles and extracted. If the ground is soft or uneven, this might provide ways for intruders to slip or dig under the fence. In these situations, the fencing should actually extend into the dirt to thwart these types of attacks.

Incorrect Answers:
A: Fences three to four feet high only deter casual trespassers. They are not the most effective maximum security design. Therefore, this answer is incorrect.
B: Fences six to seven feet high are considered too high to climb easily. They are not the most effective maximum security design. Therefore, this answer is incorrect.
D: Double fencing is not the most cost effective maximum security design. Two fences would cost more than one good fence. Furthermore, this answer does not state how high the two fences are. Two 3' to 4' fences would not be very secure. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 486

QUESTION 96
The Orange Book is founded upon which security policy model?

A. The Biba Model
B. The Bell LaPadula Model
C. Clark-Wilson Model
D. TEMPEST

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-La Padula (BLP) model is a model of computer security that focuses on mandatory and discretionary access control. It was spelled out in an influential paper by David E Bell and Leonard J. La Padula.
The Bell-La Padula paper formed the basis of the "Orange Book" security classifications, the system that the US military used to evaluate computer security for decades.

Incorrect Answers:
A: The Orange Book is not founded upon the Biba model.
C: The Orange Book is not founded upon the Clark-Wilson model.
D: The Orange Book is not founded upon the TEMPEST model.

References:
https://sites.google.com/site/cacsolin/bell-lapadula

QUESTION 97
Which of the following is NOT a basic component of security architecture?

A. Motherboard
B. Central Processing Unit (CPU)
C. Storage Devices
D. Peripherals (input/output devices)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The system architecture aspect of security architecture includes the following:

- CPU – Central Processing Unit
- Storage devices – includes both long and short-term storage, such as memory and disk
- Peripherals – includes both input and output devices, such as keyboards and printer

The components and devices connect to the motherboard. However, the motherboard is not considered a basic component of security architecture.

Incorrect Answers:
B: The Central Processing Unit (CPU) is a basic component of security architecture.
C: Storage Devices are a basic component of security architecture.
D: Peripherals (input/output devices) are a basic component of security architecture.

QUESTION 98
Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?

A. B2
B. B1
C. A1
D. A2

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
B2: Structured Protection: The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. **Operator and administration functions are separated within the system to provide more trusted and protected operational functionality**. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system.
The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
B: Separate operator and system administrator roles are not required at level B1.
C: Separate operator and system administrator roles are required at level A1. However, they are also required at the lower level of B2.
D: Separate operator and system administrator roles are required at level A2. However, they are also required at the lower level of B2.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 396
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

QUESTION 99
In which of the following models are Subjects and Objects identified and the permissions applied to each subject/object combination are specified? Such a model can be used to quickly summarize what permissions a subject has for various system objects.

A. Access Control Matrix model
B. Take-Grant model
C. Bell-LaPadula model
D. Biba model

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system. This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).

Incorrect Answers:
B: The take-grant protection model is used to establish or disprove the safety of a given computer system that follows specific rules. This is not what is described in the question.
C: The Bell–LaPadula Model is a state machine model used for enforcing access control in government and military applications. This is not what is described in the question.
D: The Biba Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 229

QUESTION 100
Which of the following is NOT a precaution you can take to reduce static electricity?

A. power line conditioning
B. anti-static sprays
C. maintain proper humidity levels

D. anti-static flooring

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Power line conditioning is not a precaution you can take to reduce static electricity.
Some precautions you can take to reduce static electricity damage are:
- Use anti-static sprays where possible.
- Operations or computer centers should have anti-static flooring.
- Building and computer rooms should be grounded properly.
- Anti-static table or floor mats may be used.
- HVAC should maintain the proper level of relative humidity in computer rooms.

Fire Detection and Suppression

Incorrect Answers:
B: Anti-static sprays are a precaution you can take to reduce static electricity. Therefore, this answer is incorrect.
C: Maintaining proper humidity levels is a precaution you can take to reduce static electricity. Therefore, this answer is incorrect.
D: Anti-static flooring is a precaution you can take to reduce static electricity. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 460

QUESTION 101
Which of the following is currently the most recommended water system for a computer room?

A. preaction
B. wet pipe
C. dry pipe
D. deluge

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
Preaction systems are similar to dry pipe systems in that the water is not held in the pipes, but is released when the pressurized air within the pipes is reduced. Once this happens, the pipes are filled with water, but it is not released right away. A thermal-fusible link on the sprinkler head has to melt before the water is released. The purpose of combining these two techniques is to give people more time to respond to false alarms or to small fires that can be handled by other means. Putting out a small fire with a handheld extinguisher is better than losing a lot of electrical equipment to water damage. These systems are usually used only in data processing environments rather than the whole building, because of the higher cost of these types of systems.

Incorrect Answers:
B: Wet pipe systems always contain water in the pipes and are usually discharged by temperature control–level sensors. This type is not the most recommended water system for a computer room. Therefore, this answer is incorrect.
C: In dry pipe systems, the water is not actually held in the pipes. The water is contained in a "holding tank" until it is released. This type is not the MOST recommended water system for a computer room. Therefore, this answer is incorrect.
D: A deluge system has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period. Because the water being released is in such large volumes, these systems are usually not used in data processing environments. This type is not the most recommended water system for a computer room. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 474-475

QUESTION 102
Which of the following is electromagnetic interference (EMI) that is noise from the radiation generated by the difference between the hot and ground wires?

A. traverse-mode noise
B. common-mode noise
C. crossover-mode noise
D. transversal-mode noise

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Noise in power systems refers to the presence of electrical radiation in the system that is unintentional and interferes with the transmission of clean power. There are several types of noise, the most common being Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI).
EMI is noise that is caused by the generation of radiation due to the charge difference between the three electrical wires — the hot, neutral, and ground wires. Two common types of EMI generated by electrical systems are:
1. Common-mode noise. Noise from the radiation generated by the difference between the hot and ground wires.
2. Traverse-mode noise. Noise from the radiation generated by the difference between the hot and neutral wires.

Incorrect Answers:
A: Traverse-mode noise is noise from the radiation generated by the difference between the hot and neutral wires, not between the hot and ground wires. Therefore, this answer is incorrect.
C: Crossover-mode noise is not one of the two defined types of EMI generated by electrical systems. Therefore, this answer is incorrect.
D: Transversal -mode noise is not one of the two defined types of EMI generated by electrical systems. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 458

QUESTION 103
The "vulnerability of a facility" to damage or attack may be assessed by all of the following EXCEPT:
A. Inspection
B. History of losses
C. Security controls
D. security budget

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
There are many types of tests that can be performed to assess the vulnerability of a facility. These include inspection, history of losses and security controls.
Inspection covers many aspects of vulnerability testing ranging from checking the perimeter fencing to penetration testing of systems.
History of losses (losses from previous attacks or security breaches) is a good way of assessing the vulnerability of a facility. Examining how previous breaches occurred can help determine whether the facility is protected against another similar breach.
Testing the security controls in place to ensure they are sufficient is an obvious way of assessing the vulnerability of a facility. Security controls cover everything from the locks on the doors to intrusion detection systems.
One thing that cannot be used to assess the vulnerability of a facility is the security budget. The amount of money spent on security is irrelevant. A large security budget does not guarantee that a facility is secure and a small budget does not mean it is insecure.

Incorrect Answers:
A: Inspection of the security systems can be used to assess the vulnerability of a facility. Therefore, this answer is incorrect.
B: History of losses (losses from previous attacks or security breaches) can be used to assess the vulnerability of a facility. Therefore, this answer is incorrect.
C: Examining the security controls can be used to assess the vulnerability of a facility. Therefore, this answer is incorrect.

QUESTION 104
Which of the following is not an EPA-approved replacement for Halon?

A. Bromine
B. Inergen
C. FM-200
D. FE-13

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
At one time, Halon was considered the perfect fire suppression method in computer operations centers, due to the fact that it is not harmful to the equipment, mixes thoroughly with the air, and spreads extremely fast. The benefits of using Halons are that they do not leave liquid or solid residues when discharged. Therefore, they are preferred for sensitive areas, such as computer rooms and data storage areas.
However, several issues arose with its deployment, such as that it cannot be breathed safely in concentrations greater than 10 percent, and when deployed on fires with temperatures greater than 900°, it degrades into seriously toxic chemicals — hydrogen fluoride, hydrogen bromide, and bromine. Some common EPA-acceptable Halon replacements are

- FM-200 (HFC-227ea)
- CEA-410 or CEA-308
- NAF-S-III (HCFC Blend A)
- FE-13 (HFC-23)
- Argon (IG55) or Argonite (IG01)
- Inergen (IG541)
- Low pressure water mists

Incorrect Answers:
B: Inergen is an EPA-approved replacement for Halon. Therefore, this answer is incorrect.
C: FM-200 is an EPA-approved replacement for Halon. Therefore, this answer is incorrect.
D: FE-13 is an EPA-approved replacement for Halon. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 464-465

QUESTION 105
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense?

A. TCSEC
B. ITSEC

C. DIACAP
D. NIACAP

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.
The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Initially issued in 1983 by the National Computer Security Center (NCSC), an arm of the National Security Agency, and then updated in 1985. TCSEC was replaced by the Common Criteria international standard originally published in 2005.

Incorrect Answers:
B: The Information Technology Security Evaluation Criteria (ITSEC) was the first attempt at establishing a single standard for evaluating security attributes of computer systems and products by many European countries. This is not what is described in the question.
C: The DoD Information Assurance Certification and Accreditation Process (DIACAP) is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply risk management to information systems (IS). This is not what is described in the question.
D: The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum-standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. This is not what is described in the question.

References:
https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 399

QUESTION 106
The Computer Security Policy Model the Orange Book is based on is which of the following?

A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Orange Book used the Bell-LaPadula Computer Security Policy model as a comparative evaluation for all systems.

Incorrect Answers:
B: The Data Encryption Standard (DES) is a cryptographic algorithm, not a Computer Security Policy model.
C: Kerberos is an authentication protocol, not a Computer Security Policy model.
D: TEMPEST is related to limiting the electromagnetic emanations from electronic equipment.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209, 254, 402, 800

QUESTION 107
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
A. integrity and confidentiality B.
confidentiality and availability
C. integrity and availability
D. none of the above

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A difference between ITSEC and TCSEC is that TCSEC bundles functionality and assurance into one rating, whereas ITSEC evaluates these two attributes separately. The other differences are that ITSEC was developed to provide more flexibility than TCSEC, and ITSEC addresses integrity, availability, and confidentiality, whereas TCSEC addresses only confidentiality. ITSEC also addresses networked systems, whereas TCSEC deals with stand-alone systems.

Incorrect Answers:
A: Both ITSEC and TCSEC address confidentiality.
B: Both ITSEC and TCSEC address confidentiality.
D: One of the answers given is correct.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 401

QUESTION 108
Which of the following is NOT a type of motion detector?

A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A photoelectric sensor does not detect motion; it detects a break in a beam of light.
A photoelectric system, or photometric system, detects the change in a light beam. These systems work like photoelectric smoke detectors, which emit a beam that hits the receiver. If this beam of light is interrupted, an alarm sounds. The beams emitted by the photoelectric cell can be cross-sectional and can be invisible or visible beams. Cross-sectional means that one area can have several different light beams extending across it, which is usually carried out by using hidden mirrors to bounce the beam from one place to another until it hits the light receiver.

Incorrect Answers:
B: A passive infrared system (PIR) identifies the changes of heat waves in an area it is configured to monitor. If the particles' temperature within the air rises, it could be an indication of the presence of an intruder, so an alarm is sounded. A PIR is a type of motion detector. Therefore, this answer is incorrect.
C: Wave-pattern motion detectors differ in the frequency of the waves they monitor. The different frequencies are microwave, ultrasonic, and low frequency. All of these devices generate a wave pattern that is sent over a sensitive area and reflected back to a receiver. If the pattern is returned undisturbed, the device does nothing. If the pattern returns altered because something in the room is moving, an alarm sounds. A Microwave Sensor is a type of motion detector. Therefore, this answer is incorrect.
D: An Ultrasonic Sensor is an example of a wave-pattern motion detector. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 495

QUESTION 109
What is the minimum static charge able to cause disk drive data loss?

A. 550 volts
B. 1000 voltsC. 1500 volts
D. 2000 volts

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Low humidity of less than 40 percent increases the static electricity damage potential. A static charge of 4000 volts is possible under normal humidity conditions on a hardwood or vinyl floor, and charges up to 20,000 volts or more are possible under conditions of very low humidity with non-static—free carpeting. Although you cannot control the weather, you certainly can control your relative humidity level in the computer room through your HVAC systems. The list below lists the damage various static electricity charges can do to computer hardware:

- 40 volts: Sensitive circuits and transistors
- 1,000 volts: Scramble monitor display
- 1,500 volts: Disk drive data loss
- 2,000 volts: System shutdown
- 4,000 volts: Printer Jam
- 17,000 volts: Permanent chip damage

Incorrect Answers:
A: 550 volts is not enough to cause disk drive data loss. Therefore, this answer is incorrect.
B: 1000 volts is not enough to cause disk drive data loss. Therefore, this answer is incorrect.
D: Only 1500 volts is enough to cause disk drive data loss, not 2000 volts. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 460

QUESTION 110
Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used)?

A. A subject is not allowed to read up.
B. The *- property restriction can be escaped by temporarily downgrading a high level subject.
C. A subject is not allowed to read down.
D. It is restricted to confidentiality.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The statement that a subject is not allowed to read down in the Bell-LaPadula security model is FALSE.

The Bell-LaPadula model was developed to make sure secrets stay secret; thus, it provides and addresses confidentiality only.
The Bell-LaPadula model is a subject-to-object model. An example would be how you (subject) could read a data element (object) from a specific database and write data into that database.

Three main rules are used and enforced in the Bell-LaPadula model: the simple security rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level. For example, if Bob is given the security clearance of secret, this rule states he cannot read data classified as top secret. If the organization wanted Bob to be able to read top-secret data, it would have given him that clearance in the first place.
The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the **"no read up" rule**, and the *-property rule is referred to as the **"no write down"** rule. The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:
A: It is true that a subject is not allowed to read up in the Bell-LaPadula model.
B: It is true that the *- property restriction in the Bell-LaPadula model can be escaped by temporarily downgrading a high level subject.
D: It is true that the Bell-LaPadula model is restricted to confidentiality.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-372

QUESTION 111
Which of the following is a class A fire?

A. common combustibles
B. liquid
C. electrical
D. Halon

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class A fires involve "common combustibles"; these are ordinary combustible materials, such as cloth, wood, paper, rubber, and many plastics.

Incorrect Answers:
B: A flammable liquid fire (such as gasoline, oil, lacquers) is a Class B fire. Therefore, this answer is incorrect.
C: Electrical fires are Class C fires. Therefore, this answer is incorrect.
D: Halon is not flammable; it is a gas used to suppress fires. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 112
Which of the following statements relating to the Biba security model is FALSE?

A. It is a state machine model.
B. A subject is not allowed to write up.
C. Integrity levels are assigned to subjects and objects.
D. Programs serve as an intermediate layer between subjects and objects.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The statement, “Programs serve as an intermediate layer between subjects and objects” in the Biba model is FALSE. The Clark–Wilson model uses programs as an intermediate layer between subjects and objects.
The Biba model was developed after the Bell-LaPadula model. It is a state machine model similar to the Bell-LaPadula model. Biba addresses the integrity of data within applications. The Bell-LaPadula model uses a lattice of security levels (top secret, secret, sensitive, and so on). These security levels were developed mainly to ensure that sensitive data were only available to authorized individuals. The Biba model is not concerned with security levels and confidentiality, so it does not base access decisions upon this type of lattice. Instead, the Biba model uses a lattice of integrity levels.
If implemented and enforced properly, the Biba model prevents data from any integrity level from flowing to a higher integrity level. Biba has three main rules to provide this type of protection:
▪ *-integrity axiom A subject cannot write data to an object at a higher integrity level (referred to as “no write up”).
▪ Simple integrity axiom A subject cannot read data from a lower integrity level (referred to as “no read down”). ▪
Invocation property A subject cannot request service (invoke) of higher integrity.

Incorrect Answers:
A: The Biba model is a state machine model.
B: It is true that a subject is not allowed to write up in the Biba model.
C: It is true that integrity levels are assigned to subjects and objects in the Biba model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 372

QUESTION 113
Which of the following organizations PRODUCES and PUBLISHES the Federal Information Processing Standards (FIPS)?

A. The National Computer Security Center (NCSC)
B. The National Institute of Standards and Technology (NIST)

C. The National Security Agency (NSA)
D. The American National Standards Institute (ANSI)

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Federal Information Processing Standards (FIPS) is a standard for adoption and use by United States Federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce. FIPS describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies. The standards cover a specific topic in information technology (IT) and strive to achieve a common level of quality or interoperability.
Incorrect Answers:
A: The National Computer Security Center (NCSC) does not produce or publish the Federal Information Processing Standards (FIPS).
C: The National Security Agency (NSA) does not produce or publish the Federal Information Processing Standards (FIPS).
D: The American National Standards Institute (ANSI) does not produce or publish the Federal Information Processing Standards (FIPS).

References" http://whatis.techtarget.com/definition/Federal-Information-Processing-Standards-FIPS

QUESTION 114
What is the main focus of the Bell-LaPadula security model?

A. Accountability
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model was developed to ensure that secrets stay secret. Therefore, it provides and addresses confidentiality only.

Incorrect Answers:

A: The main focus of the Bell- LaPadula security model is confidentiality, not accountability.
B: The main focus of the Bell- LaPadula security model is confidentiality, not integrity. The Biba model is focused on Integrity.
D: The main focus of the Bell- LaPadula security model is confidentiality, not availability.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 369-373 https://en.wikipedia.org/wiki/Bell-La_Padula_model

QUESTION 115
Which of the following suppresses combustion by disrupting a chemical reaction, by doing so it kills the fire?

A. Halon
B. CO2
C. water
D. soda acid
Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Halon is a gas that was widely used in the past to suppress fires because it interferes with the chemical combustion of the elements within a fire. It mixes quickly with the air and does not cause harm to computer systems and other data processing devices. It was used mainly in data centers and server rooms.
It was discovered that halon has chemicals (chlorofluorocarbons) that deplete the ozone and that concentrations greater than 10 percent are dangerous to people. Halon used on extremely hot fires degrades into toxic chemicals, which is even more dangerous to humans.
Halon has not been manufactured since January 1, 1992, by international agreement. The Montreal Protocol banned halon in 1987, and countries were given until 1992 to comply with these directives. The most effective replacement for halon is FM-200, which is similar to halon but does not damage the ozone.

Incorrect Answers:
B: CO2 suppresses fire by starving it of oxygen, not by disrupting a chemical reaction. Therefore, this answer is incorrect.
C: Water suppresses fire by lowering the temperature of the fuel to below its ignition point or by dispersing the fuel, not by disrupting a chemical reaction. Therefore, this answer is incorrect.
D: Soda acid fire extinguishers are CO2-based fire extinguishers. The soda and the acid react to produce CO2. CO2 suppresses fire by starving it of oxygen, not by disrupting a chemical reaction. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 473

QUESTION 116

Which of the following is a class C fire?

A. electrical
B. liquid
C. common combustibles
D. soda acid

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class C fires are electrical fires.
Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use gas, CO2 or dry powders as these extinguishing agents are non-conductive.
Incorrect Answers:
B: A flammable liquid fire (such as gasoline, oil, lacquers) is a Class B fire. Therefore, this answer is incorrect.
C: A common combustibles fire (such as wood, paper, cloth) is a Class A fire. Therefore, this answer is incorrect.
D: Soda acid is not a type of fire; it's a type of fire extinguisher. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 117
Which of the following statements pertaining to the Bell-LaPadula model is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."
B. It addresses covert channels.
C. It addresses management of access controls.
D. It allows "write up."

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Three main rules are used and enforced in the Bell-LaPadula model:
The simple security rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.
The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to as the “no write down” rule.
The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

If you are NOT making use of the strong star property, then there is no rule preventing you from writing up.

Incorrect Answers:
A: The simple security rule, referred to as the “no read up” rule, will prevent you from reading up.
B: The Bell-LaPadula model does not address covert channels.
C: The Bell-LaPadula model does not address management of access controls.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370

QUESTION 118

Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

A. The Bell-LaPadula model
B. The information flow model
C. The noninterference model
D. The Clark-Wilson model

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Multilevel security properties can be expressed in many ways, one being noninterference. This concept is implemented to ensure any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level. This type of model does not concern itself with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level.
If a lower-level entity was aware of a certain activity that took place by an entity at a higher level and the state of the system changed for this lower-level entity, the entity might be able to deduce too much information about the activities of the higher state, which in turn is a way of leaking information. Users at a lower security level should not be aware of the commands executed by users at a higher level and should not be affected by those commands in any way.

Incorrect Answers:
A: The Bell–LaPadula model is a state machine model used for enforcing access control in government and military applications. This is not what is described in the question.
B: The information flow model forms the basis of other models such as Bell–LaPadula or Biba. This is not what is described in the question.
D: The Clark-Wilson model prevents unauthorized users from making modifications, prevents authorized users from making improper modifications, and maintains internal and external consistency through auditing. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 380

QUESTION 119
Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model
B. The Biba model
C. The Bell-LaPadula model
D. The noninterference model

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Multilevel security properties can be expressed in many ways, one being noninterference. This concept is implemented to ensure any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level. **This type of model does not concern itself with the flow of data**, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level.

If a lower-level entity was aware of a certain activity that took place by an entity at a higher level and the state of the system changed for this lower-level entity, the entity might be able to deduce too much information about the activities of the higher state, which in turn is a way of leaking information. Users at a lower security level should not be aware of the commands executed by users at a higher level and should not be affected by those commands in any way.

Incorrect Answers:
A: The information flow model does concern itself with the flow of data.
B: The Biba model does concern itself with the flow of data.
C: The Bell-LaPadula model does concern itself with the flow of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 380

QUESTION 120
Which of the following is the preferred way to suppress an electrical fire in an information center?

A. CO2
B. CO2, soda acid, or Halon
C. water or soda acid
D. ABC Rated Dry Chemical

Correct Answer: A
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
Class C fire extinguishers are used for fires involving electrical equipment.
Class C fires are electrical fires which that may occur in electrical equipment or wiring. Class C fire extinguishers use gas, CO2 or dry powders as these extinguishing agents are non-conductive.
Of the answers given, CO2 is the preferred way to suppress an electrical fire in an information center.

Incorrect Answers:
B: Soda acid is corrosive. For this reason, it is not suitable for use in an information center. Therefore, this answer is incorrect.
C: Soda acid is corrosive. For this reason, it is not suitable for use in an information center. Water is conductive which makes it unsuitable for electrical fires. Therefore, this answer is incorrect.
D: ABC Rated Dry Chemical is corrosive. For this reason, it is not suitable for use in an information center. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472
https://en.wikipedia.org/wiki/ABC_dry_chemical

QUESTION 121
What are the four basic elements of Fire?

A. Heat, Fuel, Oxygen, and Chain Reaction
B. Heat, Fuel, CO2, and Chain Reaction
C. Heat, Wood, Oxygen, and Chain Reaction
D. Flame, Fuel, Oxygen, and Chain Reaction

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The fire triangle or combustion triangle is a simple model for understanding the necessary ingredients for most fires.
The triangle illustrates the three elements a fire needs to ignite: heat, fuel, and an oxidizing agent (usually oxygen). A fire naturally occurs when the elements are present and combined in the right mixture, meaning that fire is actually an event rather than a thing. A fire can be prevented or extinguished by removing any one of the elements in the fire triangle. For example, covering a fire with a fire blanket removes the oxygen part of the triangle and can extinguish a fire.
The fire tetrahedron represents the addition of a component, the chemical chain reaction, to the three already present in the fire triangle. Once a fire has started, the resulting exothermic chain reaction sustains the fire and allows it to continue until or unless at least one of the elements of the fire is blocked. Foam can be used to deny the fire the oxygen it needs. Water can be used to lower the temperature of the fuel below the ignition point or to remove or disperse the fuel. Halon can be used to remove free radicals and create a barrier of inert gas in a direct attack on the chemical reaction responsible for the fire.

Incorrect Answers:
B: CO2 is not one of the four basic elements of fire. CO2 is a fire suppressant. Therefore, this answer is incorrect.
C: Wood is not one of the four basic elements of fire. Wood would be an example of the 'fuel' element of fire. Therefore, this answer is incorrect.
D: Flame is not one of the four basic elements of fire. Flame is just another name for fire. Therefore, this answer is incorrect.

References:
https://en.wikipedia.org/wiki/Fire_triangle

QUESTION 122
Which Orange book security rating introduces the object reuse protection?

A. C1
B. C2
C. B1
D. B2

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
C2: Controlled Access Protection: Users need to be identified individually to provide more precise access control and auditing functionality. Logical access control mechanisms are used to enforce authentication and the uniqueness of each individual's identification. Security-relevant events are audited, and these records must be protected from unauthorized modification. The architecture must provide resource, or object, isolation so proper protection can be applied to the resource and any actions taken upon it can be properly audited. The **object reuse concept must also be invoked**, meaning that any medium holding data must not contain any remnants of information after it is released for another subject to use. If a subject uses a segment of memory, that memory space must not hold any information after the subject is done using it. The same is true for storage media, objects being populated, and temporary files being created—all data must be efficiently erased once the subject is done with that medium.

Incorrect Answers:
A: Object reuse protection is not required at level C1.
C: Object reuse protection is required at level B1; however, it was introduced at level C2.
D: Object reuse protection is required at level B2; however, it was introduced at level C2.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-395

QUESTION 123
Which Orange book security rating introduces security labels?

A. C2
B. B1 C. B2
D. B3

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
B1: Labeled Security: Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject's and object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement, and the design specifications are reviewed and verified.
This security rating is intended for environments that require systems to handle classified data.

Incorrect Answers:
A: Security labels are not required at level C2.
C: Security labels are required at level B2; however, they were introduced at level B1.
D: Security labels are required at level B3; however, they were introduced at level B1.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 395

QUESTION 124
Which Orange book security rating is the FIRST to be concerned with covert channels?

A. A1
B. B3
C. B2
D. B1

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In the Orange Book, covert channels in operating systems are not addressed until security level B2 and above because these are the systems that would be holding data sensitive enough for others to go through all the necessary trouble to access data in this fashion.
B2: Structured Protection: The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system **must not allow covert channels**. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
A: Level B2, not A1 is the FIRST to be concerned with covert channels.
B: Level B2, not B3 is the FIRST to be concerned with covert channels.
D: Level B2, not B1 is the FIRST to be concerned with covert channels.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-396

QUESTION 125
Which of the following is true about a "dry pipe" sprinkler system?

A. It is a substitute for carbon dioxide systems.
B. It maximizes chances of accidental discharge of water.
C. It reduces the likelihood of the sprinkler system pipes freezing.
D. It uses less water than "wet pipe" systems.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In dry pipe systems, the water is not actually held in the pipes. The water is contained in a “holding tank” until it is released. The pipes hold pressurized air, which is reduced when a fire or smoke alarm is activated, allowing the water valve to be opened by the water pressure. Water is not allowed into the pipes that feed the sprinklers until an actual fire is detected. First, a heat or smoke sensor is activated; then, the water fills the pipes leading to the sprinkler heads, the fire alarm sounds, the electric power supply is disconnected, and finally water is allowed to flow from the sprinklers. These pipes are best used in colder climates because the pipes will not freeze.

Incorrect Answers:
A: A "dry pipe" sprinkler system is not a replacement for a carbon dioxide system. Dry pipe systems still use water which is not suitable for many fires. Therefore, this answer is incorrect.
B: A "dry pipe" sprinkler system does not maximize the chances of accidental discharge of water. The chances are reduced as there is no water held in the pipes. Therefore, this answer is incorrect.
D: A "dry pipe" sprinkler system uses no less water than "wet pipe" systems. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 474

QUESTION 126
According to the Orange Book, which security level is the first to require a system to protect against covert timing channels?

A. A1
B. B3
C. B2

D. B1

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The TCSEC defines two kinds of covert channels:
- Storage channels - Communicate by modifying a "storage location"
- Timing channels - Perform operations that affect the "real response time observed" by the receiver

The TCSEC, also known as the Orange Book, requires analysis of covert storage channels to be classified as a B2 system and analysis of covert timing channels is a requirement for class B3.

Incorrect Answers:
A: Level A1 requires a system to protect against covert timing channels. However, the lower level B3 also requires it.
C: Level B2 does not require a system to protect against covert timing channels.
D: Level B1 does not require a system to protect against covert timing channels.

References:
https://en.wikipedia.org/wiki/Covert_channel

QUESTION 127
What does the Clark-Wilson security model focus on?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model deals only with confidentiality, while the Biba and Clark-Wilson models deal only with integrity.

The Clark-Wilson model addresses all three integrity goals: prevent unauthorized users from making modifications, prevent authorized users from making improper modifications, and maintain internal and external consistency.

Incorrect Answers:
A: The Clark-Wilson security model does not focus on confidentiality; it focuses on integrity.
C: The Clark-Wilson security model does not focus on accountability; it focuses on integrity.
D: The Clark-Wilson security model does not focus on availability; it focuses on integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 414, 416

QUESTION 128
What does the simple security (ss) property mean in the Bell-LaPadula model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Three main rules are used and enforced in the Bell-LaPadula model:
The simple security (SS) rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.
The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to as the “no write down” rule.
The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:
B: The simple security rule is referred to as the “no read up” rule, not the “no write down” rule. The *-property rule is referred to as the “no write down” rule. C: The simple security rule is referred to as the “no read up” rule, not the “no read down” rule. D: The simple security rule is referred to as the “no read up” rule, not the “no write up” rule.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370

QUESTION 129
What does the * (star) property mean in the Bell-LaPadula model?

A. No write up
B. No read up
C. No write down
D. No read down

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Three main rules are used and enforced in the Bell-LaPadula model:
The simple security (SS) rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.
The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to as the “no write down”rule.
The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:
A: The *-property rule is referred to as the “no write down” rule, not the “no write up” rule.
B: The *-property rule is referred to as the “no write down” rule, not the “no read up” rule.
D: The *-property rule is referred to as the “no write down” rule, not the “no read down” rule.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370
QUESTION 130
What does the * (star) integrity axiom mean in the Biba model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Biba model was developed after the Bell-LaPadula model. It is a state machine model similar to the Bell-LaPadula model. Biba addresses the integrity of data within applications.
The Biba model uses a lattice of integrity levels. If implemented and enforced properly, the Biba model prevents data from any integrity level from flowing to a higher integrity level.
Biba has three main rules to provide this type of protection:
▪ *-integrity axiom: A subject cannot write data to an object at a higher integrity level (referred to as “no write up”).
▪ Simple integrity axiom: A subject cannot read data from a lower integrity level (referred to as “no read down”). ▪
Invocation property: A subject cannot request service (invoke) of higher integrity.

Incorrect Answers:
A: The * (star) integrity axiom means “no write up”, not “no read up”.
B: The * (star) integrity axiom means “no write up”, not “no write down”.
C: The * (star) integrity axiom means “no write up”, not “no read down”.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 372

QUESTION 131
What does the simple integrity axiom mean in the Biba model?

A. No write down
B. No read down
C. No read up
D. No write up

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Biba model was developed after the Bell-LaPadula model. It is a state machine model similar to the Bell-LaPadula model. Biba addresses the integrity of data within applications.

The Biba model uses a lattice of integrity levels. If implemented and enforced properly, the Biba model prevents data from any integrity level from flowing to a higher integrity level.
Biba has three main rules to provide this type of protection:
- *-integrity axiom: A subject cannot write data to an object at a higher integrity level (referred to as “no write up”).
- Simple integrity axiom: A subject cannot read data from a lower integrity level (referred to as “no read down”).
- Invocation property: A subject cannot request service (invoke) of higher integrity.

Incorrect Answers:
A: The * (star) integrity axiom means “no write up”, not “no read up”.
B: The * (star) integrity axiom means “no write up”, not “no write down”.
C: The * (star) integrity axiom means “no write up”, not “no read down”.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 372

QUESTION 132
What is the Biba security model concerned with?

A. Confidentiality
B. Reliability
C. Availability
D. Integrity

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Biba model was developed after the Bell-LaPadula model. It is a state machine model similar to the Bell-LaPadula model. Biba addresses the integrity of data within applications. The Bell-LaPadula model uses a lattice of security levels (top secret, secret, sensitive, and so on). These security levels were developed mainly to ensure that sensitive data were only available to authorized individuals. The Biba model is not concerned with security levels and confidentiality, so it does not base access decisions upon this type of lattice. Instead, the Biba model uses a lattice of integrity levels.
Incorrect Answers:
A: The Biba security model is not concerned with confidentiality; it is only concerned with integrity.
B: The Biba security model is not concerned with reliability; it is only concerned with integrity.
C: The Biba security model is not concerned with availability; it is only concerned with integrity.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 372

QUESTION 133
Which security model uses division of operations into different parts and requires different users to perform each part?

A. Bell-LaPadula model
B. Biba model
C. Clark-Wilson model
D. Non-interference model

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Clark-Wilson security model uses division of operations into different parts and requires different users to perform each part. This is known as Separation of Duties.
The Clark-Wilson model outlines how to incorporate separation of duties into the architecture of an application. If a customer needs to withdraw over $10,000, the application may require a supervisor to log in and authenticate this transaction. This is a countermeasure against potential fraudulent activities. The model provides the rules that the developers must follow to properly implement and enforce separation of duties through software procedures.

Incorrect Answers:
A: The Bell-LaPadula model does not use division of operations into different parts and require different users to perform each part.
B: The Biba model does not use division of operations into different parts and require different users to perform each part.
D: The Non-interference model does not use division of operations into different parts and require different users to perform each part.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 376

QUESTION 134
What is the name of the FIRST mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

A. Clark and Wilson Model
B. Harrison-Ruzzo-Ullman Model
C. Rivest and Shamir Model
D. Bell-LaPadula Model

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns. It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access. Its development was funded by the U.S. government to provide a framework for computer systems that would be used to store and process sensitive information. The model's main goal was to prevent secret information from being accessed in an unauthorized manner.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels.

Incorrect Answers:
A: The Clark-Wilson Model is an integrity model. This is not what is described in the question.
B: The HRU security model (Harrison, Ruzzo, Ullman model) is an operating system level computer security model which deals with the integrity of access rights in the system. This is not what is described in the question.
C: Rivest and Shamir is not a model. They created RSA cryptography. This is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 369

QUESTION 135
Which of the following models does NOT include data integrity or conflict of interest?

A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns. It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access.
An important thing to note is that the Bell-LaPadula model was developed to make sure secrets stay secret; thus, it provides and addresses confidentiality only. This model does not address the integrity of the data the system maintains—only who can and cannot access the data and what operations can be carried out.

Incorrect Answers:
A: The Biba model deals with data integrity.
B: The Clark-Wilson model deals with data integrity.
D: The Brewer and Nash Model deals with conflict of interest. In this model, no information can flow between the subjects and objects in a way that would create a conflict of interest.

References:
Harris, Shon, *All In One CISSP Exam Guide, 6th Edition*, McGraw-Hill, New York, 2013, p. 370

QUESTION 136
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
When an application uses the Clark-Wilson model, it separates data into one subset that needs to be highly protected, which is referred to as a constrained data item (CDI), and another subset that does not require a high level of protection, which is called an unconstrained data item (UDI). Users cannot modify critical data (CDI) directly. Instead, the subject (user) must be authenticated to a piece of software, and the software procedures (Transformation Procedures) will carry out the operations on behalf of the user. For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to a program, which is acting as a front end for the database, and then the program will control what Kathy can and cannot do to the information in the database.

Incorrect Answers:
A: The take-grant protection model is used to establish or disprove the safety of a given computer system that follows specific rules. This is not what is described in the question.

B: The Biba Model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. However, it does not define a constrained data item and a transformation procedure.
C: The Bell-LaPadula model does not deal with integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 374

QUESTION 137
The BIGGEST difference between System High Security Mode and Dedicated Security Mode is:

A. The clearance required
B. Object classification
C. Subjects cannot access all objects
D. Need-to-know

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A system is operating in a dedicated security mode if all users have a clearance for, and a formal need-to-know about, all data processed within the system. All users have been given formal access approval for all information on the system and have signed nondisclosure agreements (NDAs) pertaining to this information. The system can handle a single classification level of information.
A system is operating in system high-security mode when all users have a security clearance to access the information but not necessarily a need-to-know for all the information processed on the system. So, unlike in the dedicated security mode, in which all users have a need-to-know pertaining to all data on the system, in system high-security mode, all users have a need-to-know pertaining to some of the data. This mode also requires all users to have the highest level of clearance required by any and all data on the system. However, even though a user has the necessary security clearance to access an object, the user may still be restricted if he does not have a need-to-know pertaining to that specific object.

Incorrect Answers:
A: The clearance required is not the difference between the two. All users have clearance in both systems. However, in high-security mode, access is further restricted by need-to-know.
B: Object classification is not the difference between the two. The classification of objects can be the same or it can be different; however, high-security mode is further restricted by need-to-know.
C: Subjects cannot access all objects is not the difference between the two. All subjects CAN access all objects providing they have the 'need-to-know'.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 4th Edition, McGraw-Hill, New York, 2007, p. 387

QUESTION 138
For competitive reasons, the customers of a large shipping company called the "Integrated International Secure Shipping Containers Corporation" (IISSCC) like to keep private the various cargos that they ship. IISSCC uses a secure database system based on the Bell-LaPadula access control model to keep this information private. Different information in this database is classified at different levels. For example, the time and date a ship departs is labeled Unclassified, so customers can estimate when their cargos will arrive, but the contents of all shipping containers on the ship are labeled Top Secret to keep different shippers from viewing each other's cargos.

An unscrupulous fruit shipper, the "Association of Private Fruit Exporters, Limited" (APFEL) wants to learn whether or not a competitor, the "Fruit Is Good Corporation" (FIGCO), is shipping pineapples on the ship "S.S. Cruise Pacific" (S.S. CP). APFEL can't simply read the top secret contents in the IISSCC database because of the access model. A smart APFEL worker, however, attempts to insert a false, unclassified record in the database that says that FIGCO is shipping pineapples on the S.S. CP, reasoning that if there is already a FIGCO-pineapple-SSCP record then the insertion attempt will fail. But the attempt does not fail, so APFEL can't be sure whether or not FIGCO is shipping pineapples on the S.S. CP.

What is the name of the access control model property that prevented APFEL from reading FIGCO's cargo information? What is a secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples?

A. *-Property and Polymorphism
B. Strong *-Property and Polyinstantiation
C. Simple Security Property and Polymorphism
D. Simple Security Property and Polyinstantiation

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level. Simple Security Property is the name of the access control model property that prevented APFEL from reading FIGCO's cargo information.

The secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples is Polyinstantiation. Polyinstantiation enabled the false record to be created.
Polyinstantiation enables a table that contains multiple tuples with the same primary keys, with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects must be restricted from it. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking the information actually means something else.

Incorrect Answers:
A: The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. This is not the access control model property that prevented APFEL from reading FIGCO's cargo information.

Polymorphism takes place when different objects respond to the same command, input, or message in different ways. This is not the secure database technique used in this question.
B: The strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal. This is not the access control model property that prevented APFEL from reading FIGCO's cargo information.
C: Polymorphism takes place when different objects respond to the same command, input, or message in different ways. This is not the secure database technique used in this question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 4th Edition, McGraw-Hill, New York, 2007, pp. 370, 1186

QUESTION 139
Which security model uses an access control triple and also requires separation of duty?

A. DAC
B. Lattice
C. Clark-Wilson
D. Bell-LaPadula

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Clark-Wilson model enforces the three goals of integrity by using access triple (subject, software [TP], object), separation of duties, and auditing. This model enforces integrity by using well-formed transactions (through access triple) and separation of duties.
When an application uses the Clark-Wilson model, it separates data into one subset that needs to be highly protected, which is referred to as a constrained data item (CDI), and another subset that does not require a high level of protection, which is called an unconstrained data item (UDI). Users cannot modify critical data (CDI) directly. Instead, the subject (user) must be authenticated to a piece of software, and the software procedures (TPs) will carry out the operations on behalf of the user. For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to a program, which is acting as a front end for the database, and then the program will control what Kathy can and cannot do to the information in the database.
This is referred to as access triple: subject (user), program (TP), and object (CDI). A user cannot modify CDI without using a TP.
The Clark-Wilson security model uses division of operations into different parts and requires different users to perform each part. This is known as Separation of Duties.
The Clark-Wilson model outlines how to incorporate separation of duties into the architecture of an application. If a customer needs to withdraw over $10,000, the application may require a supervisor to log in and authenticate this transaction. This is a countermeasure against potential fraudulent activities. The model provides the rules that the developers must follow to properly implement and enforce separation of duties through software procedures.

Incorrect Answers:
A: DAC (Discretionary Access Control) is not a security model that uses an access control triple and requires separation of duty.
B: Lattice-based access control model A mathematical model that allows a system to easily represent the different security levels and control access attempts based on those levels. It is not a security model that uses an access control triple and requires separation of duty.
D: The Bell–LaPadula Model is a state machine model used for enforcing access control in government and military applications. It is not a security model that uses an access control triple and requires separation of duty.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 370-377

QUESTION 140
You have been approached by one of your clients. They are interested in doing some security re-engineering. The client is looking at various information security models. It is a highly secure environment where data at high classifications cannot be leaked to subjects at lower classifications. Of primary concern to them, is the identification of potential covert channel. As an Information Security Professional, which model would you recommend to the client?

A. Information Flow Model combined with Bell LaPadula
B. Bell LaPadula
C. Biba
D. Information Flow Model

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Bell-LaPadula model focuses on preventing information from flowing from a high security level to a low security level. Information Flow Model deals with covert channels.

Subjects can access files. Processes can access memory segments. When data are moved from the hard drive's swap space into memory, information flows. Data are moved into and out of registers on a CPU. Data are moved into different cache memory storage devices. Data are written to the hard drive, thumb drive, CDROM drive, and so on. Properly controlling all of these ways of how information flows can be a very complex task. This is why the information flow model exists—to help architects and developers make sure their software does not allow information to flow in a way that can put the system or data in danger. One way that the information flow model provides this type of protection is by ensuring that covert channels do not exist in the code.

Incorrect Answers:
B: The Bell LaPadula model on its own is not sufficient because it does not deal with the identification of covert channels.
C: The Biba model is an integrity model. It will not prevent information from flowing from a high security level to a low security level or identify covert channels.
D: The Information Flow model on its own is not sufficient because it will not prevent information from flowing from a high security level to a low security level.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 377-378

QUESTION 141
Which of the following security models introduced the idea of mutual exclusivity which generates dynamically changing permissions?
A. Biba
B. Brewer & Nash
C. Graham-Denning
D. Clark-Wilson

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Brewer and Nash model, also called the Chinese Wall model, was created to provide access controls that can change dynamically depending upon a user's previous actions. The main goal of the model is to protect against conflicts of interest by users' access attempts.
Under the Brewer and Nash model, company sensitive information is categorized into mutually disjointed conflict-of-interest categories. If you have access to one set of data, you cannot access the other sets of data.

Incorrect Answers:
A: The Biba model deals with integrity. It does not use dynamically changing permissions.
C: The Graham-Denning model shows how subjects and objects should be securely created and deleted. It also addresses how to assign specific access rights. It does not use dynamically changing permissions.
D: The Clark-Wilson model deals with integrity. It does not use dynamically changing permissions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 383

QUESTION 142
Which of the following was the FIRST mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access, and to outline rules of access?

A. Biba
B. Bell-LaPadula
C. Clark-Wilson
D. State machine

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In the 1970s, the U.S. military used time-sharing mainframe systems and was concerned about the security of these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns. It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access, and outlined rules of access. Its development was funded by the U.S. government to provide a framework for computer systems that would be used to store and process sensitive information. The model's main goal was to prevent secret information from being accessed in an unauthorized manner.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels.

Incorrect Answers:
A: The Biba Model is an integrity model. This is not what is described in the question.
C: The Clark-Wilson Model is an integrity model. This is not what is described in the question.
D: State machine is not a specific model; it is a type of model. For example, the Bell-LaPadula model is a state machine model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 369

QUESTION 143
Which of the following answers BEST describes the Bell La-Padula model of storage and access control of classified information?

A. No read up and No write down
B. No write up, no read down
C. No read over and no write up
D. No reading from higher classification levels

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Three main rules are used and enforced in the Bell-LaPadula model:
The simple security (SS) rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.

The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the “no read up” rule, and the *-property rule is referred to as the “no write down” rule.
The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:
B: No write up, no read down is not the best description of the Bell-LaPadula model.
C: No read over and no write up is not the best description of the Bell-LaPadula model.
D: No reading from higher classification levels is not the best description of the Bell-LaPadula model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370

QUESTION 144
Individual accountability does not include which of the following?

A. unique identifiers
B. policies and procedures
C. access rules
D. audit trails

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Accountability would not include policies & procedures because while important on an effective security program they cannot be used in determining accountability.

References:
A: Accountability would include unique identifiers so that you can identify the individual.
C: Accountability would include access rules to define access violations.
D: Accountability would include audit trails to be able to trace violations or attempted violations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 248-250

QUESTION 145
Which of the following components are considered part of the Trusted Computing Base?

A. Trusted hardware and firmware.
B. Trusted hardware and software.
C. Trusted hardware, software and firmware.
D. Trusted computer operators and system managers.

Correct Answer: C
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
The trusted computing base (TCB) is a collection of all the hardware, software, and firmware components within a system that provide some type of security and enforce the system's security policy. The TCB does not address only operating system components, because a computer system is not made up of only an operating system. Hardware, software components, and firmware components can affect the system in a negative or positive manner, and each has a responsibility to support and enforce the security policy of that particular system. Some components and mechanisms have direct responsibilities in supporting the security policy, such as firmware that will not let a user boot a computer from a USB drive, or the memory manager that will not let processes overwrite other processes' data. Then there are components that do not enforce the security policy but must behave properly and not violate the trust of a system. Examples of the ways in which a component could violate the system's security policy include an application that is allowed to make a direct call to a piece of hardware instead of using the proper system calls through the operating system, a process that is allowed to read data outside of its approved memory space, or a piece of software that does not properly release resources after use.

To assist with the evaluation of secure products, TCSEC introduced the idea of the Trusted Computing Base (TCB) into product evaluation. In essence, TCSEC starts with the principle that there are some functions that simply must be working correctly for security to be possible and consistently enforced in a computing system. For example, the ability to define subjects and objects and the ability to distinguish between them is so fundamental that no system could be secure without it. The TCB then are these fundamental controls implemented in a given system, whether that is in hardware, software, or firmware. Each of the TCSEC levels describes a different set of fundamental functions that must be in place to be certified to that level.

Incorrect Answers:
A: Software is also considered part of the Trusted Computing Base.
B: Firmware is also considered part of the Trusted Computing Base.
D: Trusted computer operators and system managers are not considered part of the Trusted Computing Base.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 360
https://www.freepracticetests.org/documents/TCB.pdf

QUESTION 146
The high availability of multiple all-inclusive, easy-to-use hacking tools that do NOT require much technical knowledge has brought a growth in the number of which type of attackers?

A. Black hats
B. White hats
C. Script kiddies
D. Phreakers

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Script kiddies are hackers who do not necessarily have the skill to carry out specific attacks without the tools provided for them on the Internet and through friends. Since these people do not necessarily understand how the attacks are actually carried out, they most likely do not understand the extent of damage they can cause.

Incorrect Answers:
A: Black hats are malicious, skilled hackers. Easy-to-use hacking tools have not brought a growth in black hats.
B: White hats are security professionals; ethical hackers who hack systems to test their security. Easy-to-use hacking tools have not brought a growth in white hats. D: Phreakers are telephone/PBX (private branch exchange) hackers. Easy-to-use hacking tools have not brought a growth in Phreakers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 986

QUESTION 147
Which is the last line of defense in a physical security sense?

A. people
B. interior barriers

C. exterior barriers
D. perimeter barriers

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In terms of physical security, people are the last line of defense for your company's assets. If an intruder gets past the perimeter barriers, then the external barriers and finally the internal barriers, there are no more physical defenses remaining other than people in the facility.

Incorrect Answers:
B: Interior barriers are behind external barriers and perimeter barriers in terms of physical security. However, internal barriers are not the last line of defense; people are. Therefore, this answer is incorrect.
C: Exterior barriers are between perimeter barriers and internal barriers in terms of physical security. Therefore, they are not the last line of defense so this answer is incorrect.
D: Perimeter barriers are the first line of defense; not the last line of defense. Therefore, this answer is incorrect.

QUESTION 148
What is an error called that causes a system to be vulnerable because of the environment in which it is installed?

A. Configuration error
B. Environmental error
C. Access validation error
D. Exceptional condition handling error

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Environmental errors include utility failure, service outage, natural disasters, or neighboring hazards. Any issue with the environment in which a system is installed is known as an environmental error.
Maintaining appropriate temperature and humidity is important in any facility, especially facilities with computer systems. Improper levels of either can cause damage to computers and electrical devices. High humidity can cause corrosion, and low humidity can cause excessive static electricity. This static electricity can short out devices, cause the loss of information, or provide amusing entertainment for unsuspecting employees. Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down.

Incorrect Answers:
A: A configuration error is a problem caused by the configuration of the settings in a system, not the environment in which the system is installed.
C: An access validation error is a problem caused a user not having the correct permissions or access rights to the system. An access validation error is not caused by the environment in which the system is installed.
D: An exceptional condition handling error is a problem caused by the software code of the system, not the environment in which the system is installed.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 466

QUESTION 149
Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners
B. uninterruptible power supplies
C. power filters
D. power dividers

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An uninterruptible power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, supercapacitors, or flywheels. The on-battery runtime of most uninterruptible power sources is relatively short (often only a few minutes) but sufficient to start a standby power source or properly shut down the protected equipment.

Incorrect Answers:
A: A power conditioner is a device intended to improve the quality of the power that is delivered to electrical equipment. It does not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.
C: A power filter is similar to a power conditioner in that it is intended to improve the quality of the power that is delivered to electrical equipment. It does not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.
D: Power dividers are used in radio technology. They do not supply power when the commercial utility power system fails. Therefore, this answer is incorrect.

References:
https://en.wikipedia.org/wiki/Uninterruptible_power_supply

QUESTION 150

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

A. specify what users can do.
B. specify which resources they can access.
C. specify how to restrain hackers.
D. specify what operations they can perform on a system.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Access controls are security features that control how users and systems communicate and interact with other systems and resources. Access controls give organization the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality.
Access controls do not enable management to specify how to restrain hackers. Access controls can only prevent hackers accessing a system.

Incorrect Answers:
A: Access control does enable managers of a system to specify what users can do within the system.
B: Access control does enable managers of a system to specify which resources they can access.
D: Access control does enable managers of a system to specify what operations they can perform on a system.

References:
https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems

QUESTION 151
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.

Incorrect Answers:
B: RADIUS is a network protocol that allows for client/server authentication and authorization, and audits remote users. It was not developed to address some of the weaknesses in Kerberos.
C: KryptoKnight provides authentication and key distribution services to applications and communicating entities in a network environment. It was not developed to address some of the weaknesses in Kerberos.
D: TACACS+ is a network protocol that allows for client/server authentication and authorization. It was not developed to address some of the weaknesses in Kerberos.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 214, 234-236
http://www.eurecom.fr/~nsteam/Papers/kryptoknight.pdf

QUESTION 152
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card
B. passive device
C. field-powered device
D. transponder

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A system sensing device recognizes the presence of a card and communicates with it without the user needing to carry out any activity.
A magnetically striped card is a card with a magnetic strip along one edge of the card. Credit cards today still have magnetic strips although they are rarely used for reading the card. To obtain information from the card by using the magnetic strip, the card needs to be 'swiped' through a card reader. The physical contact required between the card and the card reader means that a magnetically striped card is not a wireless proximity card.
System sensing access control readers, also called transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

Incorrect Answers:
B: A passive device is a wireless proximity card. Passive devices contain no battery or power on the card, but sense the electromagnetic field transmitted by the reader and transmit at different frequencies using the power field of the reader. Therefore, this answer is incorrect.
C: A field-powered device is a wireless proximity card. They contain active electronics, a radio frequency transmitter, and a power supply circuit on the card. Therefore, this answer is incorrect.
D: A transponder is a wireless proximity card. The reader and card communicate directly. The card and reader have a receiver, transmitter, and battery. The reader sends signals to the card to request information. The card sends the reader an access code. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 484

QUESTION 153
Which of the following is the most costly countermeasure to reducing physical security risks?

A. Procedural Controls
B. Hardware Devices
C. Electronic Systems
D. Security Guards

Correct Answer: D
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
One drawback of security guards is that the cost of maintaining a guard function either internally or through an external service is expensive.
With common physical security risk countermeasures such as door entry control systems or perimeter fencing, there is typically a one-off cost when the countermeasure is implemented. With security guards, you have the ongoing cost of paying the salary of the security guard.

Incorrect Answers:
A: Procedural controls consist of approved written policies, procedures, standards and guidelines. The cost of implement procedural controls is not more costly than the ongoing costs associated with security guards. Therefore, this answer is incorrect.
B: Hardware Devices typically have a one-off cost when they are implemented and they may have a small cost for maintenance. However, this cost not more costly than the ongoing costs associated with security guards. Therefore, this answer is incorrect.
C: Electronic Systems typically have a one-off cost when they are implemented and they may have a small cost for maintenance. However, this cost not more than the ongoing costs associated with security guards. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 535

QUESTION 154
Which one of the following authentication mechanisms creates a problem for mobile users?

A. Mechanisms based on IP addresses B.
Mechanism with reusable passwords
C. One-time password mechanism.
D. Challenge response mechanism.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Authentication mechanisms based on IP addresses are useful if a user has a fixed IP address. This could be a fixed IP address at work or even a fixed IP address at home. With authentication mechanisms based on IP addresses, a user can access a resource only from a defined IP address.
However, authentication mechanisms based on IP addresses are a problem for mobile users. This is because mobile users will connect to different networks on their travels such as different WiFi networks or different mobile networks. This means that the public IP address that the mobile user will be connecting from will change frequently.

Incorrect Answers:
B: Authentication mechanisms with reusable passwords are not a problem for mobile users. As long as the mobile user knows the password, he can access the resource.
C: One-time password authentication mechanisms are not a problem for mobile users. The mobile user will have a token device that provides the one-time password which will enable the user to access the resource.
D: Challenge response authentication mechanisms are not a problem for mobile users. As long as the user has network connectivity to the authenticating server (usually over the Internet) the challenge-response authentication will succeed.

QUESTION 155
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack

Correct Answer: B

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In this question, the attacker is trying to obtain the key from several “encrypted messages”. When the attacker has only encrypted messages to work from, this is known as a Ciphertext-only attack.

Cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack.
The following are example of some common attacks:
Chosen Ciphertext. Portions of the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext
Known Plaintext. The attacker has a copy of the plaintext corresponding to the ciphertext
Chosen Plaintext. Chosen plaintext is encrypted and the output ciphertext is obtained
Ciphertext Only. Only the ciphertext is available

Incorrect Answers:
A: With a Known Plaintext attack, the attacker has a copy of the plaintext corresponding to the ciphertext. This is not what is described in the question.
C: With a Chosen-Ciphertext attack, the attacker has a copy of the plaintext corresponding to the ciphertext. This is not what is described in the question.
D: With a Plaintext-only attack, the attacker does not have the encrypted messages as stated in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154

QUESTION 156
The RSA algorithm is an example of what type of cryptography?
A. Asymmetric Key.
B. Symmetric Key.
C. Secret Key.
D. Private Key.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA is a public key algorithm that is an example of asymmetric key algorithms. RSA is used for encryption, digital signatures, and key distribution.

Incorrect Answers:
B: RSA is not an example of symmetric key algorithms.
C: Secret Key cryptography is an encryption system where a common key is used to encrypt and decrypt the message. This is not the case in RSA.
D: RSA uses Private Keys for decryption, but it is not an example of Private Key cryptography.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 815, 831
http://www.webopedia.com/TERM/S/symmetric_key_cryptography.html

QUESTION 157
What algorithm was DES derived from?

A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Lucifer was adopted and modified by the U.S. National Security Agency (NSA) to establish the U.S. Data Encryption Standard (DES) in 1976.

Incorrect Answers:
A: Twofish is a symmetric block cipher, which was a candidate for being the basis of the Advanced Encryption Standard (AES).
B: Skipjack is an algorithm that was used by Clipper Chip, which was used in the Escrowed Encryption Standard (EES).
C: Brooks-Aldeman is not a valid algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 764, 809
Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 250

QUESTION 158
What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.

C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With Electronic Code Book (ECB) Mode, a 64-bit data block is entered into the algorithm with a key, and a block of ciphertext is produced. The same block of ciphertext will always result from a given block of plaintext and a given key.

Incorrect Answers:
B: This option refers to Cipher Block Chaining (CBC).
C: This option is not a characteristic of using the Electronic Code Book mode of DES encryption, as ECB allows for ciphertext to be produced from a given block of plaintext and a given key.
D: This option refers to Cipher Block Chaining (CBC).

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 800-807

QUESTION 159
Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods. What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
For large quantities of sensitive information, symmetric key encryption (using a secret key) is more efficient.

Public key cryptography uses two keys (public and private) generated by an asymmetric algorithm for protecting encryption keys and key distribution, and a secret key is generated by a symmetric algorithm and used for bulk encryption. Then there is a hybrid use of the two different algorithms: asymmetric and symmetric. Each algorithm has its pros and cons, so using them together can be the best of both worlds.
In the hybrid approach, the two technologies are used in a complementary manner, with each performing a different function. A symmetric algorithm creates keys used for encrypting bulk data, and an asymmetric algorithm creates keys used for automated key distribution.
When a symmetric key is used for bulk data encryption, this key is used to encrypt the message you want to send. When your friend gets the message you encrypted, you want him to be able to decrypt it, so you need to send him the necessary symmetric key to use to decrypt the message. You do not want this key to travel unprotected, because if the message were intercepted and the key were not protected, an evildoer could intercept the message that contains the necessary key to decrypt your message and read your information. If the symmetric key needed to decrypt your message is not protected, there is no use in encrypting the message in the first place. So we use an asymmetric algorithm to encrypt the symmetric key. Why do we use the symmetric key on the message and the asymmetric key on the symmetric key? The reason is that the asymmetric algorithm takes longer because the math is more complex. Because your message is most likely going to be longer than the length of the key, we use the faster algorithm (symmetric) on the message and the slower algorithm (asymmetric) on the key.

Incorrect Answers:
B: For large quantities of sensitive information, symmetric key encryption (using a secret key) is more efficient. Using public and private keys for encryption and decryption is asymmetric key encryption.
C: Software encryption is not an answer on its own. We need to determine what type of software encryption to use.
D: Elliptical curve cryptography (ECC) is a public key encryption technique. Symmetric key encryption is more efficient for large amounts of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 793

QUESTION 160
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

When information is encrypted using a public key, it can only be decrypted by using the associated private key. As the recipient is the only person with the private key, the recipient is the only person who can decrypt the message. This provides a form of authentication in that the recipient's identity can be positively verified by the sender. If the receiver replies to the message, the sender knows that the intended recipient received the message.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 784-785

QUESTION 161
Kerberos depends upon what encryption method?

A. Public Key cryptography.
B. Secret Key cryptography.
C. El Gamal cryptography.
D. Blowfish cryptography.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
During the Kerberos Authentication Process, the user and the KDC share a secret key, while the service and the KDC share a different secret key. Kerberos is, therefore, dependent on Secret Key cryptography.

Incorrect Answers:
A: Kerberos is dependent on Secret Key cryptography, not Public Key cryptography.
C: El Gamal is a public key algorithm that can be used for digital signatures, encryption, and key exchange. Kerberos is not, however, dependent on it.
D: Blowfish is a block cipher that works on 64-bit blocks of data. Kerberos is not, however, dependent on it.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213, 810, 818

QUESTION 162
Which of the following statements is TRUE about data encryption as a method of protecting data?
A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The main challenge brought by improved security is that introducing encryption software also introduces management complexity, and in particular this means dealing with encryption keys.
An encryption key applies a set of complex algorithms to data and translates it into streams of seemingly random alphanumeric characters. There are two main types – private key (or symmetric) encryption and public key (or asymmetric) encryption.
In symmetric encryption, all users have access to one private key, which is used to encrypt and decrypt data held in storage media such as backup tapes and disk drives. Although considered generally secure, the downside is that there is only one key, which has to be shared with others to perform its function. Asymmetric encryption comprises two elements: a public key to encrypt data and a private key to decrypt data. The public key is used by the owner to encrypt information and can be given to third parties running a compatible application to enable them to send encrypted messages back.
Managing encryption keys effectively is vital. Unless the creation, secure storage, handling and deletion of encryption keys is carefully monitored, unauthorized parties can gain access to them and render them worthless. And if a key is lost, the data it protects becomes impossible to retrieve.

Incorrect Answers:
A: Data encryption should not 'sometimes' be used for password files; it should always be used.
B: It is not true that data encryption is usually easily administered; it is complicated.
C: It is not true that data encryption makes few demands on system resources; encrypting data requires significant processing power.

References:
http://www.computerweekly.com/feature/Encryption-key-management-is-vital-to-securing-enterprise-data-storage

QUESTION 163
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.
Some devices have limited processing capacity, storage, power supply, and bandwidth, such as wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality, requiring a smaller percentage of the resources compared to RSA and other algorithms, so it is used in these types of devices.
In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

Incorrect Answers:
A: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than RSA.
B: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than El Gamal.
D: Elliptic Curve Cryptography (ECC) has a higher strength per bit of key length than AES.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 818-819

QUESTION 164
How many bits is the effective length of the key of the Data Encryption Standard algorithm?

A. 168
B. 128
C. 56
D. 64

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Data Encryption Standard (DES) has had a long and rich history within the computer community. NIST invited vendors to submit data encryption algorithms to be used as a cryptographic standard. IBM had already been developing encryption algorithms to protect financial transactions. In 1974, IBM's 128-bit algorithm, named Lucifer, was submitted and accepted. The NSA modified this algorithm to use a key size of 64 bits (with 8 bits used for parity, resulting in an effective key length of 56 bits) instead of the original 128 bits, and named it the Data Encryption Algorithm (DEA).
NOTE DEA is the algorithm that fulfills DES, which is really just a standard. So DES is the standard and DEA is the algorithm, but in the industry we usually just refer to it as DES. The CISSP exam may refer to the algorithm by either name, so remember both.
Incorrect Answers:
A: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 168 bits.

B: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 128 bits.
D: The Data Encryption Standard algorithm has an effective key length of 56 bits, not 64 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 800

QUESTION 165
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading the password.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A one-way hash function performs a mathematical encryption operation on a password that cannot be reversed. This prevents an unauthorized person from reading the password.
Some systems and applications send passwords over the network in cleartext, but a majority of them do not anymore. Instead, the software performs a one-way hashing function on the password and sends only the resulting value to the authenticating system or service. The authenticating system has a file containing all users' password hash values, not the passwords themselves, and when the authenticating system is asked to verify a user's password, it compares the hashing value sent to what it has in its file.

Incorrect Answers:
A: One-way hashing of user passwords does not prevent an unauthorized person from trying multiple passwords in one logon attempt. This is not the purpose of one-way hashing.
C: One-way hashing of user passwords does not minimize the amount of storage required for user passwords; it increases it because a hashed password is typically much longer than the password itself.
D: One-way hashing of user passwords does not minimize the amount of processing time used for encrypting passwords.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1059

QUESTION 166
Which of the following issues is not addressed by digital signatures?

A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Digital signatures offer no protection against denial-of-service attacks.
A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

A digital signature is a hash value that has been encrypted with the sender's private key.
If Kevin wants to ensure that the message he sends to Maureen is not modified and he wants her to be sure it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message, and then Kevin would encrypt that hash value with his private key. When Maureen receives the message, she will perform the hashing function on the message and come up with her own hash value. Then she will decrypt the sent hash value (digital signature) with Kevin's public key. She then compares the two values, and if they are the same, she can be sure the message was not altered during transmission. She is also sure the message came from Kevin because the value was encrypted with his private key. The hashing function ensures the integrity of the message, and the signing of the hash value provides authentication and nonrepudiation.

Incorrect Answers:
A: Digital signatures can be used to address the issue of nonrepudiation.
B: Digital signatures can be used to address the issue of authentication.
D: Digital signatures can be used to address the issue of data integrity.

References:
https://www.techopedia.com/definition/24841/denial-of-service-attack-dos
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829

QUESTION 167
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?
A. The use of good key generators.

B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A session key is a single-use symmetric key that is used to encrypt messages between two users during a communication session.
If Tanya has a symmetric key she uses to always encrypt messages between Lance and herself, then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However, using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If, on the other hand, a new symmetric key were generated each time Lance and Tanya wanted to communicate, it would be used only during their one dialogue and then destroyed. If they wanted to communicate an hour later, a new session key would be created and shared.
A session key provides more protection than static symmetric keys because it is valid for only one session between two computers. If an attacker were able to capture the session key, she would have a very small window of time to use it to try to decrypt messages being passed back and forth.

Incorrect Answers:
A: A strong encryption key offers no protection against brute force attacks. If the same key is always used, once an attacker obtains the key, he would be able to decrypt the data.
C: It is not true that nothing can defend you against a brute force crypto key attack. Using a different key every time is a good defense.
D: There are no algorithms that are immune to brute force key attacks. This is why it is a good idea to use a different key every time.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 798-799

QUESTION 168
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output

Correct Answer: C
Section: Security Engineering

Explanation
Explanation/Reference:
Explanation:
DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity.
When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. The blocks are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key used with the algorithm. The result is 64-bit blocks of ciphertext

Incorrect Answers:
A: When 64-bit blocks of plaintext go in, 64-bit blocks of encrypted data come out.
B: DES uses a 64-bit key (not 128-bit): 56 bits make up the true key, and 8 bits are used for parity.
D: DES uses 64-bit blocks, not 56-bit.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 801

QUESTION 169
PGP uses which of the following to encrypt data?

A. An asymmetric encryption algorithm B.
A symmetric encryption algorithm
C. A symmetric key distribution system
D. An X.509 digital certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program.
PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions.
PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP uses its own type of digital certificates rather than what is used in PKI, but they both have similar purposes.

Incorrect Answers:
A: PGP uses a symmetric encryption algorithm, not an asymmetric encryption algorithm to encrypt data.
C: PGP does not use a symmetric 'key distribution system' to encrypt data.
D: An X.509 digital certificate is used in asymmetric cryptography. PGP does not use asymmetric cryptography.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 850

QUESTION 170
A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA
B. DES
C. IDEA
D. Diffie-Hellman

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a public key algorithm that is the most popular when it comes to asymmetric algorithms. RSA is a worldwide de facto standard and can be used for digital signatures, key exchange, and encryption. It was developed in 1978 at MIT and provides authentication as well as key encryption.
One advantage of using RSA is that it can be used for encryption and digital signatures. Using its one-way function, RSA provides encryption and signature verification, and the inverse direction performs decryption and signature generation.

Incorrect Answers:
B: DES is a symmetric block encryption algorithm. It is not a public key algorithm.
C: IDEA is a symmetric block encryption algorithm. It is not a public key algorithm.
D: Diffie-Hellman is used for key distribution. It is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 815

QUESTION 171
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A capacitance detector, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted. These devices are usually used to protect specific objects (artwork, cabinets, or a safe) versus protecting a whole room or area.
An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges. All objects have a static electric charge. They are all made up of many subatomic particles, and when everything is stable and static, these particles constitute one holistic electric charge. This means there is a balance between the electric capacitance and inductance. Now, if an intruder enters the area, his subatomic particles will mess up this balance in the electrostatic field, causing a capacitance change, and an alarm will sound.

Incorrect Answers:
A: Wave pattern motion detectors are used overall room security monitoring. Therefore, this answer is incorrect.
C: Field-powered devices are not intrusion detection devices. Field-powered device refers to a type of system-sensing proximity card. Therefore, this answer is incorrect.
D: Audio detectors are used overall room security monitoring. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 496
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 850

QUESTION 172
Which of the following Kerberos components holds all users' and services' cryptographic keys?

A. The Key Distribution Service
B. The Authentication Service
C. The Key Distribution Center
D. The Key Granting Service

Correct Answer: C

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Key Distribution Center (KDC) is the most important component within a Kerberos environment as it holds all users' and services' secret keys.
Incorrect Answers:
A: Key Distribution Service is not a valid Kerberos term.
B: The authentication service is a part of the KDC that authenticates a principal. It does not hold all users' and services' cryptographic keys
D: Key Granting Service is not a valid Kerberos term.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213

QUESTION 173
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

A. public keys
B. private keys
C. public-key certificates
D. private-key certificates

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Public Key describes a system that uses certificates or the underlying public key cryptography on which the system is based.
In the traditional public key model, clients are issued credentials or "certificates" by a Certificate Authority (CA). The CA is a trusted third party. Public key certificates contain the user's name, the expiration date of the certificate etc. The most common certificate format is X.509. Public key credentials in the form of certificates and public-private key pairs can provide a strong distributed authentication system.
The Kerberos and public key trust models are very similar. A Kerberos ticket is analogous to a public key certificate (a Kerberos ticket is supplied to provide access to resources). However, Kerberos tickets usually have lifetimes measured in days or hours rather than months or years.

Incorrect Answers:
A: Kerberos tickets do not actually contain public keys. They use symmetric cryptography which uses one shared key instead of asymmetric cryptography which uses public-private key pairs.

B: Kerberos tickets do not contain private keys. They use symmetric cryptography which uses one shared key instead of asymmetric cryptography which uses public-private key pairs.
D: Private-key certificates are always kept by the authentication provider; they are never distributed to subjects that require access to resources. The public key is given to the subject to provide access to a resource in a similar way to a Kerberos ticket.

References:
Tipton, Harold F. and Micki Krause, *Information Security Management Handbook*, 5th Edition, Auerbach Publications, Boca Raton, 2006, p. 1438

QUESTION 174
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is NOT a component that achieves this type of security?

A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Integrity controls are not one of the three defined security control types.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Security procedures are an example of administrative controls. Therefore, this answer is incorrect.
C: An intrusion detection system is an example of technical controls. Therefore, this answer is incorrect.
D: The facility construction, fire and water protection are examples of physical controls. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 28

QUESTION 175
Which of the following is TRUE about digital certificate?

A. It is the same as digital signature proving Integrity and Authenticity of the data
B. Electronic credential proving that the person the certificate was issued to is who they claim to be.
C. You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.
D. Can't contain geography data such as country for example.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Each person who wants to participate in a PKI requires a digital certificate, which is a credential that contains the public key for that individual along with other identifying information. The certificate is created and signed (digital signature) by a trusted third party, which is a certificate authority (CA). When the CA signs the certificate, it binds the individual's identity to the public key, and the CA takes liability for the authenticity of that individual. It is this trusted third party (the CA) that allows people who have never met to authenticate to each other and to communicate in a secure method. If Kevin has never met Dave but would like to communicate securely with him, and they both trust the same CA, then Kevin could retrieve Dave's digital certificate and start the process.

Incorrect Answers:
A: A digital certificate is not the same as a digital signature proving Integrity and Authenticity of the data. A digital certificate binds a key to an identity.
C: It is not true that you can only get a digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user; you can get a digital certificate from any CA. The CA needs to be trusted however for the certificate to be effective. The CA can be one of many 'public' CAs or it can be part of a private PKI.
D: A digital certificate can contain geography data such as country for example.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 834

QUESTION 176
What kind of encryption technology does SSL utilize?

A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)
C. Public Key
D. Private Key

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SSL uses asymmetric encryption to securely share a key. That key is then used for symmetric encryption to encrypt the data.

IPsec and SSL use asymmetric encryption to establish the encryption protocol when the session starts and then to securely exchange a private key used during the session. This private key is similar to the single secret key used in symmetric encryption.

Asymmetric encryption uses a key pair -- both a public and a private one -- for encryption. The sender uses the receiver's public key to encrypt the data and the receiver uses their private key to decrypt it. The transmission is secure because the recipient always has the private key in their possession and never exposes it by sending it over a public connection, such as the Internet.
There is a catch to using asymmetric encryption. It runs about 1,000 times slower than symmetric encryption and eats up just as much processing power, straining already overburdened servers. That means asymmetric encryption is only used (by IPsec and SSL) to create an initial and secure encrypted connection to exchange a private key. Then, that key is used to create a shared secret, or session key, that is only good during the session when the two hosts are connected.

Incorrect Answers:
A: SSL uses both symmetric and asymmetric encryption, not just symmetric encryption.
C: SSL does not use only public key encryption; shared key (symmetric) encryption is also used.
D: SSL does not use private key encryption. Initially, encryption is performed using public keys and decryption is performed using private keys (asymmetric). Then both encryption and decryption are performed using a shared key (symmetric).

References:
http://searchsecurity.techtarget.com/answer/How-IPsec-and-SSL-TLS-use-symmetric-and-asymmetric-encryption

QUESTION 177
What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed.

A. One-way hash
B. DES

C. Transposition
D. Substitution

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the *message*, and the hash value is often called the *message digest* or simply the *digest*.
The ideal cryptographic hash function has four main properties:
▪ it is easy to compute the hash value for any given message
▪ it is infeasible to generate a message from its hash
▪ it is infeasible to modify a message without changing the hash ▪ it
is infeasible to find two different messages with the same hash.
▪ Most cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length hash value.

Incorrect Answers:
B: Data Encryption Standard (DES) is a symmetric block cipher. Data encrypted using DES can be decrypted using the symmetric key.
C: A transposition cipher does not replace the original text with different text, but rather moves the original values around. This encryption can be reversed and does not produce a fixed length output.
D: A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters, or blocks. This encryption can be reversed and does not produce a fixed length output.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 178
Which of the following is NOT an asymmetric key algorithm?

A. RSA
B. Elliptic Curve Cryptosystem (ECC)
C. El Gamal
D. Data Encryption Standard (DES)

Correct Answer: D

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Data Encryption Standard (DES) is not an asymmetric key algorithm; it's a symmetric key algorithm.
DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity. When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. The blocks are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution functions depend on the value of the key used with the algorithm. The result is 64-bit blocks of ciphertext.

Incorrect Answers:
A: RSA is an asymmetric key algorithm.
B: Elliptic Curve Cryptosystem (ECC) is an asymmetric key algorithm.
C: El Gamal is an asymmetric key algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 801

QUESTION 179
Which of the following is NOT a symmetric key algorithm?

A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Digital Signature Standard (DSS) is not a symmetric key algorithm; it is an asymmetric key algorithm.
Because digital signatures are so important in proving who sent which messages, the U.S. government decided to establish standards pertaining to their functions and acceptable use. In 1991, NIST proposed a federal standard called the Digital Signature Standard (DSS). It was developed for federal departments and agencies, but most vendors also designed their products to meet these specifications. The federal government requires its departments to use DSA, RSA, or the elliptic curve digital signature algorithm (ECDSA) and SHA. SHA creates a 160-bit message digest output, which is then inputted into one of the three mentioned

digital signature algorithms. SHA is used to ensure the integrity of the message, and the other algorithms are used to digitally sign the message. This is an example of how two different algorithms are combined to provide the right combination of security services. RSA and DSA are the best known and most widely used digital signature algorithms. DSA was developed by the NSA. Unlike RSA, DSA can be used only for digital signatures, and DSA is slower than RSA in signature verification. RSA can be used for digital signatures, encryption, and secure distribution of symmetric keys.

Incorrect Answers:
A: Blowfish is a block symmetric cipher that uses 64-bit block sizes and variable-length keys.
C: Triple DES is a symmetric cipher that applies DES three times to each block of data during the encryption process.
D: RC5 is a block symmetric cipher that uses variable block sizes (32, 64, 128) and variable-length key sizes (0–2040).

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 832

QUESTION 180
Which of the following asymmetric encryption algorithms is based on the difficulty of factoring LARGE numbers?

A. El Gamal
B. Elliptic Curve Cryptosystems (ECCs)
C. RSA
D. International Data Encryption Algorithm (IDEA)

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA is derived from the last names of its inventors, Rivest, Shamir, and Addleman.
This algorithm is based on the difficulty of factoring a number, N, which is the product of two large prime numbers. These numbers may be 200 digits each. Thus, the difficulty in obtaining the private key from the public key is a hard, one-way function that is equivalent to the difficulty of finding the prime factors of N.
In RSA, public and private keys are generated as follows:
- Choose two large prime numbers, p and q, of equal length, compute p3q 5 n, which is the public modulus.
- Choose a random public key, e, so that e and (p – 1)(q – 1) are relatively prime.
- Compute e x d = 1 mod (p – 1)(q – 1), where d is the private key. ▪

Thus, d = e–1 mod [(p – 1)(q – 1)]

From these calculations, (d, n) is the private key and (e, n) is the public key.

Incorrect Answers:

A: El Gamal is based not on the difficulty of factoring large numbers but on calculating discrete logarithms in a finite field.
B: Elliptic Curve Cryptosystems (ECCs) are not based on the difficulty of factoring large numbers.
D: International Data Encryption Algorithm (IDEA) is not based on the difficulty of factoring large numbers.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 148

QUESTION 181
The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Diffie–Hellman key exchange (D–H) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Incorrect Answers:
A: The Diffie-Hellman algorithm is not primarily used to provide confidentiality.
C: The Diffie-Hellman algorithm is not primarily used to provide integrity.
D: The Diffie-Hellman algorithm is not primarily used to provide non-repudiation.

References:
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

QUESTION 182
FIPS-140 is a standard for the security of which of the following?

A. Cryptographic service providers

B. Smartcards
C. Hardware and software cryptographic modules
D. Hardware security modules

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The National Institute of Standards and Technology (NIST) issues the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government. FIPS 140 does not purport to provide sufficient conditions to guarantee that a module conforming to its requirements is secure, still less that a system built using such modules is secure. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code.

Incorrect Answers:
A: FIPS-140 is not a standard for cryptographic service providers.
B: FIPS-140 is not a standard for smartcards.
D: FIPS-140 is not a standard for hardware security modules.

References:
https://en.wikipedia.org/wiki/FIPS_140

QUESTION 183
Which of the following can best define the "revocation request grace period"?

A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Occasionally, a certificate authority needs to revoke a certificate. This might occur for one of the following reasons: ▪
The certificate was compromised.
▪ The certificate was erroneously issued.
▪ The details of the certificate changed. ▪
The security association changed.

The revocation request grace period is the maximum response time within which a CA will perform any requested revocation. This is defined in the certificate practice statement (CPS). The CPS states the practices a CA employs when issuing or managing certificates.

Incorrect Answers:
A: The revocation request grace period is not the period of time allotted within which the user must make a revocation request upon a revocation reason.
B: The revocation request grace period is the maximum response time, not the minimum response time within which a CA will perform any requested revocation.
D: The revocation request grace period is not the period of time between the arrival of a revocation request and the publication of the revocation information. Publication of a certificate revocation list does not always happen as soon as a certificate has been revoked.

QUESTION 184
Which is NOT a suitable method for distributing certificate revocation information?

A. CA revocation mailing list
B. Delta CRL
C. OCSP (online certificate status protocol)
D. Distribution point CRL

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A CA revocation mailing list is NOT a suitable method for distributing certificate revocation information.
There are several mechanisms to represent revocation information; RFC 2459 defines one such method. This method involves each CA periodically issuing a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.
There are several types of CRLs: full CRLs (also known as base CRLs), delta CRLs, and CRL Distribution Points (CDPs). Full CRLs contain the status of all certificates. Delta CRLs contain only the status of all certificates that have changed status between the issuance the last Base CRL.
CRL Distribution Point (CDP) is a certificate extension that indicates where the certificate revocation list for a CA can be retrieved. This extension can contain multiple HTTP, FTP, File or LDAP URLs for the retrieval of the CRL.

Online Certificate Status Protocol (OCSP) is a protocol that allows real-time validation of a certificate's status by having the CryptoAPI make a call to an OCSP responder and the OCSP responder providing an immediate validation of the revocation status for the presented certificate. Typically, the OCSP responder uses CRLs for retrieving certificate status information.

Incorrect Answers:
B: A Delta CRL is a suitable method for distributing certificate revocation information.
C: OCSP (online certificate status protocol) is a suitable method for distributing certificate revocation information.
D: Distribution point CRL is a suitable method for distributing certificate revocation information.

References:
https://technet.microsoft.com/en-us/library/cc700843.aspx

QUESTION 185
Which encryption algorithm is BEST suited for communication with handheld wireless devices?

A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Elliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.
Some devices have limited processing capacity, storage, power supply, and bandwidth, such as wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality, requiring a smaller percentage of the resources compared to RSA and other algorithms, so it is used in these types of devices.
In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

Incorrect Answers:
B: RSA is less efficient than ECC which makes RSA less suited for communication with handheld wireless devices.
C: SHA is a hashing algorithm; it is not an encryption algorithm suited for communication with handheld wireless devices.
D: RC4 is a symmetric algorithm whereas ECC is asymmetric which makes ECC more suited for communication with handheld wireless devices.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 818-819

QUESTION 186
Which of the following keys has the SHORTEST lifespan?

A. Secret key
B. Public key
C. Session key
D. Private key

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A session key is a single-use symmetric key that is used to encrypt messages between two users during a single communication session.
If Tanya has a symmetric key she uses to always encrypt messages between Lance and herself, then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However, using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If, on the other hand, a new symmetric key were generated each time Lance and Tanya wanted to communicate, it would be used only during their one dialogue and then destroyed. If they wanted to communicate an hour later, a new session key would be created and shared.
A session key provides more protection than static symmetric keys because it is valid for only one session between two computers. If an attacker were able to capture the session key, she would have a very small window of time to use it to try to decrypt messages being passed back and forth.

Incorrect Answers:
A: A secret key is static in nature. It has no fixed lifespan and is used until someone decides to change the key. Session keys are used for single communication sessions so they have a much shorter lifespan.
B: A public key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.
D: A private key is issued by a CA and typically has a lifespan of one or two years. Session keys are used for single communication sessions so they have a much shorter lifespan.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 798-799

QUESTION 187
What is the RESULT of a hash algorithm being applied to a message?

A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

Incorrect Answers:
A: To create a digital signature, a message digest is calculated (by the hash algorithm being applied to the message) then it is encrypted with the sender's private key. However, the digital signature is not the direct output of the hash algorithm being applied to the message.
B: A ciphertext is the output of an encryption algorithm, not a hash algorithm being applied to data.
D: A plaintext is the message 'before' the hash algorithm is applied to the message; it is the input to the hash algorithm, not the output.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 188
Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. Message non-repudiation.
B. Message confidentiality.
C. Message interleave checking.
D. Message integrity.

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network.
The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.
A message authentication code (MAC) is a short piece of information used to authenticate a message—in other words, to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin.
A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

Incorrect Answers:
A: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message non-repudiation.
B: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message confidentiality; it uses symmetric cryptography for that.
C: Secure Sockets Layer (SSL) does not use a Message Authentication Code (MAC) for message interleave checking.

References:
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 189
Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption
B. Integrity
C. Digital signatureD. Authentication

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Digital signatures do not provide encryption.
The purpose of digital signatures is to detect unauthorized modifications of data, and to authenticate the identity of the signatories and non-repudiation. These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. This smaller block of data is bound to the original data and to the identity of the sender. This binding verifies the **integrity** of data and provides non-repudiation. To quote the National Institute Standards and Technology (NIST) Digital Signature Standard (DSS): Digital signatures are used to detect unauthorized modifications to data and to **authenticate** the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory.

Incorrect Answers:
B: Digital signatures do provide integrity.
C: The digital signature standard (DSS) as its name suggests is all about digital signatures.
D: Digital signatures do provide authentication.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151

QUESTION 190
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In cryptography, key clustering is said to occur when two different keys generate the same ciphertext from the same plaintext, using the same cipher algorithm. A good cipher algorithm, using different keys on the same plaintext, should generate a different ciphertext, irrespective of the key length.

Incorrect Answers:
A: Key collision is not the correct term to describe an instance of two different keys generating the same ciphertext from the same plaintext.
C: Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. This is not what is described in the question.
D: Ciphertext collision is not the correct term to describe an instance of two different keys generating the same ciphertext from the same plaintext.

References:
https://en.wikipedia.org/wiki/Key_clustering

QUESTION 191
Which of the following is TRUE about link encryption?

A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.

C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
With Link Encryption each entity has keys in common with its two neighboring nodes in the transmission chain. Thus, a node receives the encrypted message from its predecessor (the neighboring node), decrypts it, and then re-encrypts it with another key that is common to the successor node. Then, the encrypted message is sent on to the successor node where the process is repeated until the final destination is reached. Obviously, this mode does not provide protection if the nodes along the transmission path can be compromised.

Incorrect Answers:
A: It is not true that each entity has a common key with the destination node. Each entity has keys in common with only its two neighboring nodes.
B: It is not true that encrypted messages are only decrypted by the final node. Every node in the chain (except the original sending node) decrypts the message.
D: It is not true that only secure nodes are used in this type of transmission. The data is encrypted for security; the nodes themselves can be insecure.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 126

QUESTION 192
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining

Correct Answer: B
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. However, practical problems have prevented one-time pads from being widely used.

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after use.

The one-time pad has serious drawbacks in practice because it requires:
- Truly random (as opposed to pseudorandom) one-time pad values, which is a non-trivial requirement.
- Secure generation and exchange of the one-time pad values, which must be at least as long as the message. (The security of the one-time pad is only as secure as the security of the one-time pad exchange).
- Careful treatment to make sure that it continues to remain secret, and is disposed of correctly preventing any reuse in whole or part—hence "one time".

Because the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, there is often no point in using one-time padding, as one can simply send the plain text instead of the pad (as both can be the same size and have to be sent securely).
Distributing very long one-time pad keys is inconvenient and usually poses a significant security risk. The pad is essentially the encryption key, but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans to remember. Storage media such as thumb drives, DVD-Rs or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non-suspicious way, but even so the need to transport the pad physically is a burden compared to the key negotiation protocols of a modern public-key cryptosystem, and such media cannot reliably be erased securely by any means short of physical destruction (e.g., incineration).
The key material must be securely disposed of after use, to ensure the key material is never reused and to protect the messages sent. Because the key material must be transported from one endpoint to another, and persist until the message is sent or received, it can be more vulnerable to forensic recovery than the transient plaintext it protects.

Incorrect Answers:
A: Running key cipher does not use a key of the same length as the message.
C: Steganography is a method of hiding data in another media type so the very existence of the data is concealed. This is not what is described in the question.
D: Cipher block chaining is an encryption method where each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text. This is not what is described in the question.

References:
https://en.wikipedia.org/wiki/One-time_pad

QUESTION 193
Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access

Correct Answer: A
Section: Security Engineering

Explanation

Explanation/Reference:
Explanation:
Guards are appropriate whenever immediate discriminating judgement is required by the security entity.
Guards are the oldest form of security surveillance. Guards still have a very important primary function in the physical security process, particularly in perimeter control. Because of a human's ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment, a guard can make determinations that hardware or automated security devices cannot make.

Incorrect Answers:
B: The use of physical force is not the most appropriate reason to use security guards. Therefore, this answer is incorrect.
C: The operation of access control devices typically does not require the use of security guards. Most access control devices are automatic electrical and mechanical devices that unlock and lock doors as required. Therefore, this answer is incorrect.
D: Security guards are not required to detect unauthorized access. There are many systems that can detect unauthorized access such as motion sensors etc. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 535

QUESTION 194
What is the maximum number of different keys that can be used when encrypting with Triple DES?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Triple DES (3DES) can use a maximum of three keys.

3DES can work in different modes, and the mode chosen dictates the number of keys used and what functions are carried out:
- DES-EEE3 Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted.
- DES-EDE3 Uses three different keys for encryption, and the data are encrypted, decrypted, encrypted.
- DES-EEE2 The same as DES-EEE3, but uses only two keys, and the first and third encryption processes use the same key.

- DES-EDE2 The same as DES-EDE3, but uses only two keys, and the first and third encryption processes use the same key.

Incorrect Answers:
A: A maximum of 3, not 1 different keys can be used when encrypting with Triple DES.
B: A maximum of 3, not 2 different keys can be used when encrypting with Triple DES.
D: A maximum of 3, not 4 different keys can be used when encrypting with Triple DES.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 808

QUESTION 195
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?

A. RC6
B. Twofish
C. Rijndael
D. Blowfish

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
After DES was used as an encryption standard for over 20 years and it was cracked in a relatively short time once the necessary technology was available, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place. In January 1997, NIST announced its request for AES candidates and outlined the requirements in FIPS PUB 197. AES was to be a symmetric block cipher supporting key sizes of 128, 192, and 256 bits. The following five algorithms were the finalists:
- MARS Developed by the IBM team that created Lucifer -
RC6 Developed by RSA Laboratories
- Serpent Developed by Ross Anderson, Eli Biham, and Lars Knudsen
- Twofish Developed by Counterpane Systems
- Rijndael Developed by Joan Daemen and Vincent Rijmen

Out of these contestants, Rijndael was chosen. The block sizes that Rijndael supports are 128, 192, and 256 bits.
Rijndael works well when implemented in software and hardware in a wide range of products and environments. It has low memory requirements and has been constructed to easily defend against timing attacks.
Rijndael was NIST's choice to replace DES. It is now the algorithm required to protect sensitive but unclassified U.S. government information.
Incorrect Answers:

A: RC6 was a finalist; however, Rijndael was selected by NIST as the AES algorithm.
B: Twofish was a finalist; however, Rijndael was selected by NIST as the AES algorithm.
B: Blowfish was not selected by NIST as the AES algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 809

QUESTION 196
Which of the following is a symmetric encryption algorithm?

A. RSA
B. Elliptic Curve
C. RC5
D. El Gamal

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code". The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.
RC5 has a variety of parameters it can use for block size, key size, and the number of rounds used. It was created by Ron Rivest and analyzed by RSA Data Security, Inc. The block sizes used in this algorithm are 32, 64, or 128 bits, and the key size goes up to 2,048 bits. The number of rounds used for encryption and decryption is also variable. The number of rounds can go up to 255.

Incorrect Answers:
A: RSA is an asymmetric key algorithm.
B: Elliptic Curve Cryptosystem (ECC) is an asymmetric key algorithm.
D: El Gamal is an asymmetric key algorithm.

References:
https://en.wikipedia.org/wiki/RC5
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810

QUESTION 197

Which of the following protocols would BEST mitigate threats of sniffing attacks on web application traffic?

A. SSL or TLS

B. 802.1X
C. ARP Cache Security
D. SSH - Secure Shell

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SSL and TLS encrypt web application traffic to mitigate threats of sniffing attacks.
The SSL protocol was developed by Netscape in 1994 to secure Internet client-server transactions. The SSL protocol authenticates the server to the client using public key cryptography and digital certificates. In addition, this protocol also provides for optional client to server authentication. It supports the use of RSA public key algorithms, IDEA, DES and 3DES private key algorithms, and the MD5 hash function. Web pages using the SSL protocol start with HTTPs. SSL 3.0 and its successor, the Transaction Layer Security (TLS) 1.0 protocol are defacto standards. TLS implements confidentiality, authentication, and integrity above the Transport Layer, and it resides between the application and TCP layer. Thus, TLS, as with SSL, can be used with applications such as Telnet, FTP, HTTP, and email protocols. Both SSL and TLS use certificates for public key verification that are based on the X.509 standard.

Incorrect Answers:
B: The 802.1X standard is a port-based network access control that ensures a user cannot make a full network connection until he is properly authenticated. 802.1X is not used to encrypt web application traffic.
C: ARP Cache Security can prevent ARP Cache poisoning attacks. However, it is not used to encrypt web application traffic.
D: SSH (Secure Shell) is a set of protocols that are primarily used for remote access over a network by establishing an encrypted tunnel between an SSH client and an SSH server. SSH is not used to encrypt web application traffic.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 160

QUESTION 198
What type of key would you find within a browser's list of trusted root CAs?

A. Private key
B. Symmetric key
C. Recovery key

D. Public key

Correct Answer: D
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company which charges customers to issue certificates for them.
If you trust the Root CA, you'll trust all certificates issued by the CA. All web browsers come with an extensive built-in list of trusted root certificates, many of which are controlled by organizations that may be unfamiliar to the user. The built-in list of trusted root certificates is a collection of Public Key certificates from the CAs.

Incorrect Answers:
A: The private key is always retained by the owner (in this case, a CA); it is never distributed.
B: You would not find a symmetric key within a browser's list of trusted root CAs.
C: You would not find a recovery key within a browser's list of trusted root CAs.

References:
https://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 199
Where in a PKI infrastructure is a list of revoked certificates stored?

A. CRL
B. Registration Authority
C. Recovery Agent
D. Key escrow

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

In a Public Key Infrastructure (PKI), the revocation of a certificate is dealt with by the certificate authority (CA). The revoked certificate information is stored on a certificate revocation list (CRL).

Incorrect Answers:
B: The registration authority (RA) executes the certification registration tasks. It does not, however, store a list of revoked certificates.
C: Key recovery agent is one of the intended purposes of digital certificates. It does not, however, store a list of revoked certificates.
D: Key escrow is a process or entity that can recover lost or corrupted cryptographic keys. It does not, however, store a list of revoked certificates.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 833-836, 843
Miller, David R, Microsoft *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 217

QUESTION 200
The equation used to calculate the total number of symmetric keys (K) needed for a group of users (N) to communicate securely with each other is given by which of the following?

A. K(N – 1)/ 2
B. N(K – 1)/ 2
C. K(N + 1)/ 2
D. N(N – 1)/ 2

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The equation employed to determine the required number of symmetric keys is N(N – 1)/2.

Incorrect Answers:
A, B, C: These equations are not valid for calculating the required number of symmetric keys.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 782

QUESTION 201
In which mode of DES, will a block of plaintext and a key always give the same ciphertext?

A. Electronic Code Book (ECB)
B. Output Feedback (OFB)

C. Counter Mode (CTR)
D. Cipher Feedback (CFB)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Electronic Code Book (ECB) is the “native” mode of DES and is a block cipher. ECB is best suited for use with small amounts of data. It is usually applied to encrypt initialization vectors or encrypting keys. ECB is applied to 64-bit blocks of plaintext, and it produces corresponding 64-bit blocks of ciphertext.
Electronic Code Book (ECB) mode operates like a code book. A 64-bit data block is entered into the algorithm with a key, and a block of ciphertext is produced. For a given block of plaintext and a given key, the same block of ciphertext is always produced.

Incorrect Answers:
B: The DES Output Feedback Mode (OFB) is also a stream cipher that generates the ciphertext key by XORing the plaintext with a key stream. OFB mode is not the mode described in the question.
C: Counter Mode (CTR) is very similar to OFB mode, but instead of using a randomly unique IV value to generate the keystream values, this mode uses an IV counter that increments for each plaintext block that needs to be encrypted. CTR mode is not the mode described in the question.
D: The Cipher Feedback Mode (CFB) of DES is a stream cipher where the ciphertext is used as feedback into the key generation source to develop the next key stream. CFB mode is not the mode described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 803
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 143

QUESTION 202
Which of the following modes of DES is MOST likely used for Database Encryption?

A. Electronic Code Book (ECB)
B. Cipher Block Chaining (CBC)
C. Cipher Feedback (CFB)
D. Output Feedback (OFB)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
Electronic Code Book (ECB) works with blocks of data independently. As a result, data within a file does not have to be encrypted in a specific order. This is extremely accommodating when making use of encryption in databases.

Incorrect Answers:
B: Cipher Block Chaining (CBC) is mostly used for encrypting message data.
C: Cipher Feedback (CFB) is mostly used for encrypting message data.
D: Output Feedback (OFB) is used for encrypting digitized video or voice signals.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 800-807

QUESTION 203
Which of the following is a Hashing Algorithm?

A. SHA
B. RSA
C. Diffie Hellman (DH)
D. Elliptic Curve Cryptography (ECC)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
SHA was developed when a more secure hashing algorithm was needed for U.S. government applications.

Incorrect Answers:
B, C, & D: B. RSA, Diffie Hellman (DH), and Elliptic Curve Cryptography (ECC) are asymmetric key algorithms.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 786, 827

QUESTION 204
Complete the following sentence. A digital signature is a:

A. hash value that has been encrypted with the sender's private key
B. hash value that has been encrypted with the sender's public key

C. hash value that has been encrypted with the senders Session key
D. senders signature signed and scanned in a digital format

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A digital signature is a hash value that was encrypted with the sender's private key.
Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

Incorrect Answers:
B: The hash value is signed with the sender's private key, not the public key to prove that the message came from the sender and has not been altered in transit.
C: A session key is not used to encrypt the hash value in a digital signature.
D: A digital signature is not a sender's signature signed and scanned in a digital format.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829
http://searchsecurity.techtarget.com/definition/digital-signature

QUESTION 205
Which of the following is NOT an example of an asymmetric key algorithm?

A. Elliptic curve cryptosystem (ECC)
B. Diffie-Hellman
C. Advanced Encryption Standard (AES)
D. Merkle-Hellman Knapsack

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

Advanced Encryption Standard (AES) is a block symmetric cipher that makes use of 128-bit block sizes and various key lengths.

Incorrect Answers:
A, B, & D: Elliptic curve cryptosystem (ECC), Diffie-Hellman, and Merkle-Hellman Knapsack are asymmetric key algorithms.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 811, 815

QUESTION 206
Complete the following sentence. A message can be encrypted, which provides:

A. confidentiality.

B. non-repudiation.
C. authentication.
D. integrity.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Confidentiality ensures that a message can only be read by the intended recipient. Encrypting a message provides confidentiality.
Different steps and algorithms provide different types of security services:
- A message can be encrypted, which provides confidentiality.
- A message can be hashed, which provides integrity
- A message can be digitally signed, which provides authentication, nonrepudiation, and integrity.
- A message can be encrypted and digitally signed, which provides confidentiality, authentication, nonrepudiation, and integrity

Incorrect Answers:
B: A digital signature is required to provide non-repudiation for a message. Encryption alone does not provide non-repudiation.
C: A digital signature is required to provide authentication for a message. Encryption alone does not provide authentication.
D: A hash is required to provide integrity for a message. Encryption alone does not provide integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 829-830

QUESTION 207
Readable is to unreadable just as plain text is to:

A. Cipher Text
B. Encryption
C. Unplain Text
D. Digitally Signed

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
This question is asking what the opposite of plain text is. In the context of information security, plain text means unencrypted text. The opposite of plain text is cipher text. Cipher text is another term for encrypted text.
Encryption is a method of transforming readable data, called plaintext, into a form that appears to be random and unreadable, which is called ciphertext. Plaintext is in a form that can be understood either by a person (a document) or by a computer (executable code). Once it is transformed into ciphertext, neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without unauthorized disclosure.

Incorrect Answers:
B: This answer is close but incorrect. Plaintext is readable data. The opposite of that is encrypted data (known as ciphertext), not 'encryption'.
C: Unplain text is not a valid term.
D: Digitally Signed is not the opposite of plaintext.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 765

QUESTION 208

Public key infrastructure (PKI) consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion.

This infrastructure is based upon which of the following Standard?

A. X.509 B.
X.500
C. X.400
D. X.25

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Public key infrastructure (PKI) is an ISO authentication framework that makes use of public key cryptography and the X.509 standard.

Incorrect Answers:
B: X.500 is a series of computer networking standards that cover electronic directory services. It is not, however, used by PKI.
C: X.400 is a group of ITU-T Recommendations that define standards for Data Communication Networks for email.
D: X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp.
833 https://en.wikipedia.org/wiki/X.500 https://en.wikipedia.org/wiki/X.400
https://en.wikipedia.org/wiki/X.25

QUESTION 209
What would you call a microchip installed on the motherboard of modern computers and is dedicated to carrying out security functions that involve the storage and processing of symmetric and asymmetric keys, hashes, and digital certificates.

A. Trusted Platform Module (TPM)
B. Trusted BIOS Module (TBM)
C. Central Processing Unit (CPU)
D. Arithmetic Logical Unit (ALU)

Correct Answer: A

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Trusted Platform Module (TPM) is a microchip installed on the motherboard of modern computers. TPM is dedicated to executing security functions that include the storage and processing of symmetric and asymmetric keys, hashes, and digital certificates.

Incorrect Answers:
B: Trusted BIOS Module is not a valid term.
C: A central processing unit (CPU) is the electronic circuitry within a computer that carries out the instructions of a computer program by executing the basic arithmetic, logical, control and input/output (I/O) operations detailed by the instructions.
D: An arithmetic logic unit (ALU) refers to a digital electronic circuit that executes arithmetic and bitwise logical operations on integer binary numbers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 843
https://en.wikipedia.org/wiki/Central_processing_unit
https://en.wikipedia.org/wiki/Arithmetic_logic_unit

QUESTION 210
Suppose that you are the COMSEC - Communications Security custodian for a large, multinational corporation. Susie, from Finance approaches you in the break room saying that she lost her smart ID card that she uses to digitally sign and encrypt emails in the PKI.
What happens to the certificates contained on the smart card after the security officer takes appropriate action?

A. They are added to the CRL
B. They are reissued to the user
C. New certificates are issued to the user
D. The user may no longer have certificates

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A certificate that is no longer trusted should be revoked.
The CA is responsible for creating and handing out certificates, maintaining them, and revoking them if necessary. Revocation is handled by the CA, and the revoked certificate information is stored on a certificate revocation list (CRL). This is a list of every certificate that has been revoked. This list is maintained and

updated periodically. A certificate may be revoked because the key holder's private key was compromised or because the CA discovered the certificate was issued to the wrong person.
An analogy for the use of a CRL is how a driver's license is used by a police officer. If an officer pulls over Sean for speeding, the officer will ask to see Sean's license. The officer will then run a check on the license to find out if Sean is wanted for any other infractions of the law and to verify the license has not expired. The same thing happens when a person compares a certificate to a CRL. If the certificate became invalid for some reason, the CRL is the mechanism for the CA to let others know this information.

Incorrect Answers:
B: The certificates contained on the smart card should be revoked to invalidate the certificates. They should not be reissued; new certificates (with a different key) should be issued.
C: New certificates (containing new keys) should be issued to the user. However, this question is asking about the certificates stored on the lost smart card. The certificates contained on the smart card should be revoked.
D: It is not true that the user may no longer have certificates. New certificates with different keys can be issued to the user and the old certificates (the ones on the smart card) can be revoked.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 836-837

QUESTION 211
You are an information systems security officer at a mid-sized business and are called upon to investigate a threat conveyed in an email from one employee to another.
You gather the evidence from both the email server transaction logs and from the computers of the two individuals involved in the incident and prepare an executive summary.
You find that a threat was sent from one user to the other in a digitally signed email. The sender of the threat says he didn't send the email in question.
What concept of PKI - Public Key Infrastructure will implicate the sender?

A. Non-repudiation
B. The digital signature of the recipient
C. Authentication
D. Integrity

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Non-Repudiation makes sure that a sender is unable to deny sending a message.

Incorrect Answers:
B: A digital signature guarantees the authenticity and integrity of a message by making use of hashing algorithms and asymmetric algorithms. It will not implicate the sender.
C: Authentication refers to the verification of the identity of a user who is requesting the use of a system and/or access to network resources.
D: Integrity is upheld by providing assurance of the accuracy and reliability of information and systems and preventing any unauthorized modification.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 23, 162, 398, 833

QUESTION 212
When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:

0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output

What is this cryptographic operation called?

A. Exclusive-OR
B. Bit Swapping
C. Logical-NOR
D. Decryption

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A plaintext message that needs to be encrypted is converted into bits, and the one-time pad is made up of random bits. This encryption process makes use of a binary mathematic function called exclusive-OR (XOR).

Incorrect Answers:
B: Bit-swapping is the essential adaptive hand-shaking mechanism used by DMT modems to adapt to line changes.
C: Logical-NOR is a truth-functional operator which produces a result that is the denial of Logical-Or.
D: Decryption is the process of translating encrypted data back into its original form.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 771
http://web.stanford.edu/group/cioffi/documents/bit_swapping.pdf
https://en.wikipedia.org/wiki/Logical_NOR http://searchsecurity.techtarget.com/definition/data-encryption-decryption-IC

QUESTION 213
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?

A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Explanation:
The one-time pad encryption scheme is considered unbreakable only if:
- The pad is used only one time.
- The pad is as long as the message.
- The pad is securely distributed and protected at its destination.

The pad is made up of truly random values.

Incorrect Answers:
B: One time Cryptopad (OTC) is not a valid encryption type.
C: Cryptanalysis refers to the practice of discovering flaws within cryptosystems
D: Pretty Good Privacy (PGP) is a cryptosystem that makes use of cryptographic protection to protect e-mail and files.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 770-773, 850

QUESTION 214
The ideal operating humidity range is defined as 40 percent to 60 percent. Low humidity (less than 40 percent) can produce what type of problem on computer parts?

A. Static electricity

B. Electro-plating
C. Energy-plating
D. Element-plating

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
It is important to maintain the proper temperature and humidity levels within data centers, which is why an HVAC system should be implemented specifically for this room. Too high a temperature can cause components to overheat and turn off; too low a temperature can cause the components to work more slowly. If the humidity is high, then corrosion of the computer parts can take place; if humidity is low, then static electricity can be introduced. This static electricity can short out devices and cause the loss of information. Because of this, the data center must have its own temperature and humidity controls, which are separate from the rest of the building.

Incorrect Answers:
B: Electro-plating is not caused by low humidity. Therefore, this answer is incorrect.
C: Energy-plating is not caused by low humidity. Therefore, this answer is incorrect.
D: Element-plating is not caused by low humidity. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 456

QUESTION 215
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?

A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure
C. Diffie-Hellman
D. DSS - Digital Signature Standard

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A single secret key is used between entities when using symmetric key cryptography.

Incorrect Answers:
B: Public Key Infrastructure (PKI) is an ISO authentication framework that makes use of public key cryptography and the X.509 standard.
C: Diffie-Hellman is the first asymmetric key agreement algorithm.
D: The Digital Signature Standard (DSS) refers to the U.S. standard that defines the approved algorithms to be used for digital signatures for government authentication activities.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 782, 812, 833

QUESTION 216
Complete the blanks. When using PKI, I digitally sign a message using my _____ key. The recipient verifies my signature using my _____ key.

A. Private / Public
B. Public / Private
C. Symmetric / Asymmetric
D. Private / Symmetric

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A digital signature is a hash value that was encrypted with the sender's private key. The recipient uses the sender's public key to verify the digital signature. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

Incorrect Answers:
B: A private key, not a public key is used in a digital signature. The sender is the only person in possession of the private key. The public key can be freely distributed. The recipient uses the public key to verify the digital signature which authenticates the sender.
C: Symmetric / Asymmetric are two different types of encryption methods; they are not used together to encrypt or sign a message.
D: A private key is used with a public key in asymmetric cryptography. A shared key is used in symmetric cryptography. Private and Symmetric keys are not used together to encrypt or sign a message.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 829
http://searchsecurity.techtarget.com/definition/digital-signature

QUESTION 217
Which of the following is NOT a property of the Rijndael block cipher algorithm?

A. The key sizes must be a multiple of 32 bits
B. Maximum block size is 256 bits
C. Maximum key size is 512 bits
D. The key size does not have to match the block size

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The maximum key size is 256 bits, not 512 bits.

Rijndael is a block symmetric cipher that was chosen to fulfill the Advanced Encryption Standard. It uses a 128-bit block size and various key lengths (128, 192, 256).
The Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

Incorrect Answers:
A: It is true that the key sizes must be a multiple of 32 bits.
B: It is true that the maximum block size is 256 bits.
D: It is true that the key size does not have to match the block size.

References:
http://searchsecurity.techtarget.com/definition/Rijndael
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 145

QUESTION 218
Which of the following is not a property of the Rijndael block cipher algorithm?

A. It employs a round transformation that is comprised of three layers of distinct and invertible transformations.
B. It is suited for high speed chips with no area restrictions.

C. It operates on 64-bit plaintext blocks and uses a 128 bit key.
D. It could be used on a smart card.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
This option is incorrect because the block sizes supported by Rijndael are 128, 192, and 256 bits.

Incorrect Answers:
A: Rijndael is a substitution linear transformation cipher that uses triple discreet invertible uniform transformations.
B, D: The Advanced Encryption Standard (AES), also known as Rijndael, performs well on a wide variety of hardware. Hardware ranges from 8-bit smart cards to high-performance computers.

References:
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
http://searchsecurity.techtarget.com/definition/Rijndael

QUESTION 219
What is the maximum allowable key size of the Rijndael encryption algorithm?

A. 128 bits
B. 192 bits
C. 256 bits
D. 512 bits

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
AES, which Rijndael was designed for, is a symmetric block cipher that supports key sizes of 128, 192, and 256 bits. 256 bits is the maximum key size.

Incorrect Answers:
A, B: 128 bit and 192 bit keys are supported, but it is not the maximum.
D: Rijndael does not support 512 bit keys.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 809

QUESTION 220
An X.509 public key certificate with the key usage attribute "non-repudiation" can be used for which of the following?

A. encrypting messages
B. signing messages
C. verifying signed messages
D. decrypting encrypted messages

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Support for two pairs of public-private keys is a fundamental requirement for some PKIs. One key pair is for data encryption and the other key pair is for digitally signing documents.
When digitally signing a message for non-repudiation, the private key is used. The public key (with the key usage attribute "non-repudiation") associated with the private key is used to verify the signed messages.

Incorrect Answers:
A: An X.509 public key certificate with the key usage attribute "non-repudiation" cannot be used for encrypting messages.
B: When digitally signing a message for non-repudiation, the private key is used, not the public key.
D: An X.509 public key certificate with the key usage attribute "non-repudiation" cannot be used for decrypting messages.

References:
https://docs.oracle.com/cd/E13215_01/wlibc/docs81/admin/certificates.html

QUESTION 221
Which of the following would best describe certificate path validation?

A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The certification path validation algorithm is the algorithm which verifies that a given certificate path is valid under a given public key infrastructure (PKI). A path starts with the Subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted Certification Authority (CA).
Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate that is not already explicitly trusted. For example, in a hierarchical PKI, a certificate chain starting with a web server certificate might lead to a small CA, then to an intermediate CA, then to a large CA whose trust anchor is present in the relying party's web browser.

Incorrect Answers:
B: Certificate path validation is not verification of the integrity of the associated root certificate.
C: Certificate path validation is not verification of the integrity of the concerned private key.
D: Certificate path validation is not verification of the revocation status of the concerned certificate; this is a Certificate Revocation Check.

References:
https://en.wikipedia.org/wiki/Certification_path_validation_algorithm

QUESTION 222
What is the name for a substitution cipher that shifts the alphabet by 13 places?

A. Caesar cipher
B. Polyalphabetic cipher
C. ROT13 cipher
D. Transposition cipher

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
ROT13 was an encryption method that is similar to Caesar cipher, but instead of shifting 3 spaces in the alphabet it shifted 13 spaces.
Incorrect Answers:
A: Caesar cipher shifts three spaces.

B: A polyalphabetic cipher makes use of more than one alphabet.
D: Transposition cyphers moves the original values around.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 762, 774, 778

QUESTION 223
Which of the following standards concerns digital certificates?

A. X.400 B.
X.25
C. X.509
D. X.75

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
X.509 specifies standard formats for public key certificates and attribute certificates, which are digital certificates.

Incorrect Answers:
A: X.400 is a group of ITU-T Recommendations that define standards for Data Communication Networks for email.
B: X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.
C: X.75 is an International Telecommunication Union (ITU) standard that specifies the interface for interconnecting two X.25 networks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp.
833 https://en.wikipedia.org/wiki/X.509 https://en.wikipedia.org/wiki/X.400
https://en.wikipedia.org/wiki/X.25 https://en.wikipedia.org/wiki/X.75

QUESTION 224
Which fire class can water be most appropriate for?

A. Class A fires
B. Class B fires C. Class C fires
D. Class D fires

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Class A fires can be extinguished with water. Class A fire extinguishers use water or foam.
Class A fires involve “common combustibles”; these are ordinary combustible materials, such as cloth, wood, paper, and many plastics.

Incorrect Answers:
B: You cannot use water on a Class B fire. A Class B fire is a flammable liquid fire such as gasoline, oil or lacquers. Therefore, this answer is incorrect.
C: You cannot use water on a Class C fire. Class C fires are Electrical fires. Therefore, this answer is incorrect.
D: You cannot use water on a Class D fire. A Class D fire is combustible metals such as magnesium or potassium. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 472

QUESTION 225
What is the effective key size of DES?

A. 56 bits
B. 64 bits
C. 128 bits
D. 1024 bits

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
DES makes use of a 64-bit key, of which 56 bits represents the true key, and the remaining 8 bits are used for parity.

Incorrect Answers:
B: DES does make use of a 64-bit key, but the effective key size is 56 bits.
C: International Data Encryption Algorithm (IDEA) produces key that is 128 bits long.
D: RC5 support variable-length key sizes ranging from 0-2040.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 800, 809, 810

QUESTION 226
Which of the following offers confidentiality to an e-mail message?

A. The sender encrypting it with its private key.
B. The sender encrypting it with its public key.
C. The sender encrypting it with the receiver's public key.
D. The sender encrypting it with the receiver's private key.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A message encrypted using a public key can only be decrypted using the corresponding private key. The receiver should be the only person in possession of the recipient's private key. The recipient's public key can be freely distributed.
Therefore, if the sender encrypts a message with the recipient's pubic key, the sender will know that the recipient is the ONLY person who can decrypt the message. This ensures the confidentiality of the message.

Incorrect Answers:
A: A public key can be freely distributed. If the sender encrypts a message with his private key, ANYONE in possession of the sender's public key could decrypt the message. This offers no confidentiality.
B: A message encrypted using a public key can only be decrypted using the corresponding private key. If the sender encrypts a message with his public key, only the sender would be able to decrypt it as he is the only person in possession of the private key that corresponds to his public key.
D: The receiver should be the only person in possession of the recipient's private key. The sender should never be in possession of the receiver's private key.

QUESTION 227
Which of the following is not a DES mode of operation?

A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback

Correct Answer: C

Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
DES modes include the following: ▪
Electronic Code Book (ECB)
▪ Cipher Block Chaining (CBC)
▪ Cipher Feedback (CFB)
▪ Output Feedback (OFB) ▪
Counter Mode (CTR)
▪ Input feedback is not a DES mode.

Incorrect Answers:
A, B, & D: Cipher block chaining, Electronic code book, and Cipher feedback are modes of DES.

Reference:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 802-807

QUESTION 228
What size is an MD5 message digest (hash)?

A. 128 bits B.
160 bits
C. 256 bits
D. 128 bytes

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
MD5 generates a 128-bit hash.

Incorrect Options:
B: SHA generates a 160-bit hash value.
C: SHA-256 generates a 256-bit value.
D: MD5 generates a 128-bit, not a 128 byte, hash.

Reference:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 826, 827

QUESTION 229
Which of the following service is not provided by a public key infrastructure (PKI)?

A. Access control
B. Integrity
C. Authentication
D. Reliability

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
PKI provides the confidentiality, access control, integrity, authentication, and nonrepudiation security services. Reliability is not included.

Incorrect Options:
A, B, & C: Access control, integrity, and authentication are security services provided by public key infrastructure (PKI)

Reference:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 840

QUESTION 230
In a Public Key Infrastructure, how are public keys published?

A. They are sent via e-mail.

B. Through digital certificates.
C. They are sent by owners.
D. They are not published.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The main role of the CA is to digitally sign and publish the public key bound to a given user by issuing digital certificates which certifies the ownership of a public key by the named subject of the certificate.

Incorrect Options:
A: The main role of the CA is to digitally sign and publish the public key bound to a given user, so it is not sent via e-mail.
C: The main role of the CA is to digitally sign and publish the public key bound to a given user, so they are not sent by owners.
D: The main role of the CA is to digitally sign and publish the public key bound to a given user. Clearly they are published.

Reference:
https://en.wikipedia.org/wiki/Public_key_infrastructure
https://en.wikipedia.org/wiki/Certificate_authority

QUESTION 231
Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?

A. Message Authentication Code - MAC
B. PAM - Pluggable Authentication Module
C. NAM - Negative Acknowledgement Message
D. Digital Signature Certificate

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Message Authentication Code (MAC) is a keyed cryptographic hash function that is used for data integrity and data origin authentication.

Incorrect Answers:
B: A pluggable authentication module (PAM) is used to integrate multiple low-level authentication schemes into a high-level application programming interface (API). C: A Negative Acknowledgement Message is a protocol message that is sent in many communications protocols to negatively acknowledge or reject a previously received message, or to show some kind of error.
D: Digital Signature Certificate is an invalid term. Digital signatures and digital certificates are two different security measures.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 832
https://en.wikipedia.org/wiki/Pluggable_authentication_module
https://en.wikipedia.org/wiki/NAK_(protocol_message) http://searchsecurity.techtarget.com/answer/The-difference-between-a-digital-signature-and-digital-certificate

QUESTION 232
Which answer BEST describes a secure cryptoprocessor that can be used to store cryptographic keys, passwords or certificates in a component located on the motherboard of a computer?

A. TPM - Trusted Platform Module
B. TPM - Trusted Procedure Module
C. Smart Card
D. Enigma Machine

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Trusted Platform Module (TPM) is a microchip installed on the motherboard of modern computers. TPM is dedicated to executing security functions that include the storage and processing of symmetric and asymmetric keys, hashes, and digital certificates.

Incorrect Answers:
B: Trusted Procedure Module is not a valid term.
C: A smart card is not located on the motherboard of a computer.
D: The Enigma machines were a series of electro-mechanical rotor cipher machines developed and used to protect commercial, diplomatic and military communication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 200, 201, 843
https://en.wikipedia.org/wiki/Enigma_machine

QUESTION 233
Which of the following statements pertaining to stream ciphers is TRUE?

A. A stream cipher is a type of asymmetric encryption algorithm.
B. A stream cipher generates what is called a keystream.
C. A stream cipher is slower than a block cipher.
D. A stream cipher is not appropriate for hardware-based encryption.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, so it is also known as state cipher. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR).

The pseudorandom keystream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the ciphertext stream.
Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problems if used incorrectly; in particular, the same starting state (seed) must never be used twice.

Incorrect Answers:
A: A stream cipher is not a type of asymmetric encryption algorithm; it is a symmetric key cipher.
C: A stream cipher is not slower than a block cipher; it is faster.
D: Stream ciphers require a lot of randomness and encrypt individual bits at a time. This requires more processing power than block ciphers require, which is why stream ciphers are better suited to be implemented at the hardware level.

References:
https://en.wikipedia.org/wiki/Stream_cipher

QUESTION 234
Which of the following statements pertaining to block ciphers is NOT true?

A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Some Block ciphers can operate internally as a stream.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
It is not true that plain text is encrypted with a public key and decrypted with a private key with a block cipher. Block ciphers use symmetric keys.
In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data.

Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher.

Incorrect Answers:
A: It is true that a block cipher operates on fixed-size blocks of plaintext.
B: Stream ciphers require a lot of randomness and encrypt individual bits at a time. This requires more processing power than block ciphers require, which is why stream ciphers are better suited to be implemented at the hardware level. Because block ciphers do not require as much processing power, they can be easily implemented at the software level.
D: It is true that some Block ciphers can operate internally as a stream.

References:
https://en.wikipedia.org/wiki/Block_cipher
https://en.wikipedia.org/wiki/Stream_cipher

QUESTION 235
Cryptography does NOT help in:

A. detecting fraudulent insertion.
B. detecting fraudulent deletion.
C. detecting fraudulent modification.
D. detecting fraudulent disclosure.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
Cryptography can prevent unauthorized users from being able to read or modify the data. However, it cannot prevent someone deleting the encrypted data.

Modern cryptography concerns itself with the following four objectives:
1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information) 4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information.

Incorrect Answers:
A: Integrity means that the information cannot be altered in storage or transit. This also means that the data is protected against fraudulent insertion.
C: Integrity means that the information cannot be altered in storage or transit. This also means that the data is protected against fraudulent modification.
D: Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.

References:
http://searchsoftwarequality.techtarget.com/definition/cryptography
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 24

QUESTION 236
What is the difference between the OCSP (Online Certificate Status Protocol) and a Certificate Revocation List (CRL)?

A. The OCSP (Online Certificate Status Protocol) provides real-time certificate checks and a Certificate Revocation List (CRL) has a delay in the updates.
B. The OCSP (Online Certificate Status Protocol) is a proprietary certificate mechanism developed by Microsoft and a Certificate Revocation List (CRL) is an open standard.
C. The OCSP (Online Certificate Status Protocol) is used only by Active Directory and a Certificate Revocation List (CRL) is used by Certificate Authorities
D. The OCSP (Online Certificate Status Protocol) is a way to check the attributes of a certificate and a Certificate Revocation List (CRL) is used by Certificate Authorities.

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The CA is responsible for creating and handing out certificates, maintaining them, and revoking them if necessary. Revocation is handled by the CA, and the revoked certificate information is stored on a certificate revocation list (CRL). This is a list of every certificate that has been revoked. This list is maintained and updated periodically.
Online Certificate Status Protocol (OCSP) is being used more and more rather than the cumbersome CRL approach. When using just a CRL, the user's browser must either check a central CRL to find out if the certification has been revoked or the CA has to continually push out CRL values to the clients to ensure they have an updated CRL. If OCSP is implemented, it does this work automatically in the background. It carries out real-time validation of a certificate and reports back to

the user whether the certificate is valid, invalid, or unknown. OCSP checks the CRL that is maintained by the CA. So the CRL is still being used, but now we have a protocol developed specifically to check the CRL during a certificate validation process.

Incorrect Answers:
B: The OCSP (Online Certificate Status Protocol) is not a proprietary certificate mechanism developed by Microsoft; it is an open standard.
C: The OCSP (Online Certificate Status Protocol) is not used only by Active Directory.
D: The OCSP (Online Certificate Status Protocol) is not a way to check the attributes of a certificate; it is a way to check the revocation status of a certificate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 836-837

QUESTION 237
Which of the following is BEST at defeating frequency analysis?

A. Substitution cipher
B. Polyalphabetic cipher
C. Transposition cipher
D. Ceasar cipher

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A polyalphabetic cipher makes use of more than one alphabet to conquer frequency analysis.

Incorrect Answers:
A, C: Substitution and transposition ciphers are susceptible to attacks that perform frequency analysis.
D: The Ceasar Cipher is a type of substitution cipher.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 780, 781, 871

QUESTION 238
A code, as is pertains to cryptography:

A. is a generic term for encryption.
B. is specific to substitution ciphers.
C. deals with linguistic units.

D. is specific to transposition ciphers.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. For example, the word “OCELOT” might be the ciphertext for the entire phrase “TURN LEFT 90 DEGREES,” the word “LOLLIPOP” might be the ciphertext for “TURN RIGHT 90 DEGREES”.
Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word.

Incorrect Answers:
A: A code is not a generic term for encryption.
B: A code is not specific to substitution ciphers.
D: A code is not a specific to transposition ciphers.

References:
https://www.cs.duke.edu/courses/fall02/cps182s/readings/APPLYC1.pdf

QUESTION 239
Which of the following is the MOST secure form of triple-DES encryption?

A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
DES-EDE3 is the most secure form of triple-DES encryption as it uses three different keys for encryption.

3DES can work in different modes, and the mode chosen dictates the number of keys used and what functions are carried out:
- DES-EEE3: Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted.
- DES-EDE3: Uses three different keys for encryption, and the data are encrypted, decrypted, encrypted.
- DES-EEE2: The same as DES-EEE3, but uses only two keys, and the first and third encryption processes use the same key.

- DES-EDE2: The same as DES-EDE3, but uses only two keys, and the first and third encryption processes use the same key.

Incorrect Answers:
B: DES-EDE1 uses one encryption key and returns the algorithm (and strength) as DES. It is only provided for backwards compatibility. This is not the most secure form of triple-DES encryption.
C: DES-EEE4 is not a valid form of 3DES encryption.
D: DES-EDE2 uses only two keys and is not the most secure form of triple-DES encryption.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 808

QUESTION 240
Which of the following is NOT a known type of Message Authentication Code (MAC)?

A. Keyed-hash message authentication code (HMAC)
B. DES-CBC
C. Signature-based MAC (SMAC)
D. Universal Hashing Based MAC (UMAC)

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Signature-based MAC (SMAC) is not a known type of Message Authentication Code (MAC).

Message authentication code is a cryptographic function that uses a hashing algorithm and symmetric key for data integrity and system origin functions.

A keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key.
A cipher block chaining message authentication code (CBC-MAC) is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block.
A message authentication code based on universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message.

Incorrect Answers:

A: Keyed-hash message authentication code (HMAC) is a known type of Message Authentication Code (MAC).
B: DES-CBC is a known type of Message Authentication Code (MAC).
D: Universal Hashing Based MAC (UMAC) is a known type of Message Authentication Code (MAC).

References:
https://en.wikipedia.org/wiki/UMAC
https://en.wikipedia.org/wiki/Hash-based_message_authentication_code
https://en.wikipedia.org/wiki/CBC-MAC

QUESTION 241
What is the maximum key size for the RC5 algorithm?

A. 128 bits
B. 256 bits
C. 1024 bits
D. 2040 bits

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RC5 is a block cipher that has a variety of parameters it can use for block size, key size, and the number of rounds used. It was created by Ron Rivest and analyzed by RSA Data Security, Inc. The block sizes used in this algorithm are 32, 64, or 128 bits, and the key size goes up to 2,048 bits. The number of rounds used for encryption and decryption is also variable. The number of rounds can go up to 255.

Incorrect Answers:
A: The maximum key size for the RC5 algorithm is 2048 bits, not 128 bits.
B: The maximum key size for the RC5 algorithm is 2048 bits, not 256 bits.
C: The maximum key size for the RC5 algorithm is 2048 bits, not 1024 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810

QUESTION 242
Which of the following algorithms is a stream cipher?

A. RC2
B. RC4
C. RC5
D. RC6

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RC4 is one of the most commonly implemented stream ciphers.

Incorrect Answers:
A, C, & D: RC2, RC5and RC6 are block ciphers.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810
https://en.wikipedia.org/wiki/RC2

QUESTION 243
In an SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
This is a tricky question. The client generates the “pre-master” secret. See step 4 of the process below. However, the master secret that will be used as a seed to generate the symmetric keys is generated (from the pre-master secret) by both the client and server. See step 6 below.

The steps involved in the SSL handshake are as follows (note that the following steps assume the use of the cipher suites listed in Cipher Suites with RSA Key Exchange: Triple DES, RC4, RC2, DES):

1. The client sends the server the client's SSL version number, cipher settings, session-specific data, and other information that the server needs to communicate with the client using SSL.
2. The server sends the client the server's SSL version number, cipher settings, session-specific data, and other information that the client needs to communicate with the server over SSL. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client's certificate.
3. The client uses the information sent by the server to authenticate the server (see Server Authentication for details). If the server cannot be authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the server can be successfully authenticated, the client proceeds to step 4.
4. Using all data generated in the handshake thus far, the client (with the cooperation of the server, depending on the cipher being used) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret to the server.
5. If the server has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's own certificate to the server along with the encrypted pre-master secret.
6. If the server has requested client authentication, the server attempts to authenticate the client (see Client Authentication for details). If the client cannot be authenticated, the session ends. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, and then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret.
7. Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity (that is, to detect any changes in the data between the time it was sent and the time it is received over the SSL connection).
8. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.
10. The SSL handshake is now complete and the session begins. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.
11. This is the normal operation condition of the secure channel. At any time, due to internal or external stimulus (either automation or user intervention), either side may renegotiate the connection, in which case, the process repeats itself.

Incorrect Answers:
B: The client generates the “pre-master” secret, not the “master secret”. The master secret that will be used as a seed to generate the symmetric keys is generated (from the pre-master secret) by both the client and server.
C: The master certificate is not generated by the web server alone; the client also generates the master secret.
D: The merchant's Certificate Server does not generate the master secret.

References:
https://support.microsoft.com/en-us/kb/257591

QUESTION 244
Which of the following was NOT designed to be a proprietary encryption algorithm?

A. RC2
B. RC4
C. BlowfishD. Skipjack

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Blowfish is a block cipher that works on 64-bit blocks of data. The key length can be anywhere from 32 bits up to 448 bits, and the data blocks go through 16 rounds of cryptographic functions. It was intended as a replacement to the aging DES. While many of the other algorithms have been proprietary and thus encumbered by patents or kept as government secrets, this wasn't the case with Blowfish. Bruce Schneier, the creator of Blowfish, has stated, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone." Incorrect Answers:
A: RC2 was designed to be a proprietary encryption algorithm.
B: RC4 was designed to be a proprietary encryption algorithm.
D: Skipjack was designed to be a proprietary encryption algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 810

QUESTION 245
Which of the following is NOT an encryption algorithm?

A. Skipjack
B. SHA-1
C. Twofish
D. DEA

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:

SHA-1 is a hashing algorithm.

Incorrect Answers:
A: Skipjack is an algorithm used for encryption.
C: Twofish is a symmetric block cipher that is used for encryption.
D: DEA is the algorithm that fulfills DES, which provides encryption.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 800, 831
https://en.wikipedia.org/wiki/Skipjack_(cipher)
Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 236

QUESTION 246
What key size is used by the Clipper Chip?

A. 40 bits
B. 56 bits
C. 64 bits
D. 80 bits
Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Clipper Chip made use of the Skipjack algorithm, which is a symmetric cipher that uses an 80-bit key.

Incorrect Answers:
A: RC4 is able to use key sizes ranging from 40 bits to 256 bits.
B: DES makes use of a 64-bit key, of which 56 bits make up the true key, and 8 bits are used for parity.
C: DES makes use of a 64-bit key, of which 56 bits make up the true key, and 8 bits are used for parity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 800-802,
Conrad, Eric, Seth Misenar, Joshua Feldman, CISSP Study Guide, 2nd Edition, Syngress, Waltham, 2012, p. 250

QUESTION 247
Which of the following would BEST describe a Concealment cipher?

A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The concealment cipher is a symmetric key, transposition cipher where the words or characters of the plaintext message are embedded in a page of words or characters at a consistent interval.

Incorrect Answers:
A: Transposition cyphers moves the original values around.
C: The substitution cipher substitutes bits, characters, or blocks of characters with different bits, characters, or blocks.
D: Steganography is a technique used to hide data in another media type so that the presence of the data is masked.

Reference:
Miller, David R, Microsoft *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 156
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 774, 777

QUESTION 248
Which of the following is BEST provided by symmetric cryptography?

A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Symmetric cryptosystems is able to provide confidentiality, but not authentication or nonrepudiation.

Incorrect Answers:
B: Hashing algorithms provide data integrity.
C: Availability is an Access Control concern. It is not provided by symmetric cryptography.
D: Symmetric cryptosystems is unable to provide authentication or nonrepudiation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 159, 783, 873

QUESTION 249
While using IPsec, the ESP and AH protocols both provide integrity services. However, when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affects the use of AH and it´s Integrity Check Value (ICV) the MOST?

A. Key session exchange
B. Packet Header Source or Destination address
C. VPN cryptographic key size
D. Cryptographic algorithm used

Correct Answer: B
Section: Security Engineering
Explanation
Explanation/Reference:
Explanation:
AH provides authentication and integrity, and ESP can provide those two functions and confidentiality. Why even bother with AH then? In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own integrity values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.
The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically. The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.

Incorrect Answers:
A: The key session exchange does not affect the use of AH and it´s Integrity Check Value.
C: The VPN cryptographic key size does not affect the use of AH and it´s Integrity Check Value.
D: The crypotographic algorithm used does not affect the use of AH and it´s Integrity Check Value.

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 862-863

QUESTION 250
Which of the following protocols offers native encryption?

A. IPSEC, SSH, PPTP, SSL, MPLS, L2F, and L2TP
B. IPSEC, SSH, SSL, TFTP
C. IPSEC, SSH, SSL, TLS
D. IPSEC, SSH, PPTP, SSL, MPLS, and L2TP

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
IPSec (Internet Protocol Security) is a standard that provides encryption, access control, non-repudiation, and authentication of messages over an IP network. SSH (Secure Shell) is a set of protocols that are primarily used for remote access over a network by establishing an encrypted tunnel between an SSH client and an SSH server.
SSL (Secure Sockets Layer) is an encryption technology that is used to provide secure transactions such as the exchange of credit card numbers. SSL is a socket layer security protocol and is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. Similar to SSH, SSL uses symmetric encryption for private connections and asymmetric or public key cryptography for peer authentication.
Incorrect Answers:
A: MPLS (Multiprotocol Label Switching) is a WAN technology that does not provide encryption. L2F (Layer 2 Forwarding Protocol) is a tunneling protocol that does not provide encryption by itself. L2TP (Layer 2 Tunneling Protocol) is also a tunneling protocol that does not provide encryption by itself.
B: TFTP (Trivial File Transfer Protocol) is used for transferring files. TFTP does not provide encryption.
D: MPLS (Multiprotocol Label Switching) is a WAN technology that does not provide encryption. L2TP (Layer 2 Tunneling Protocol) is a tunneling protocol that does not provide encryption by itself.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 86

QUESTION 251
Which of the following is NOT a disadvantage of symmetric cryptography when compared with asymmetric ciphers?

A. Provides Limited security services
B. Has no built in Key distribution
C. Speed

D. Large number of keys are needed

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Symmetric cryptography is much faster than asymmetric systems, and is difficult to crack if a large key size is used.

Incorrect Answers:
A, B, D: Symmetric cryptography provides confidentiality, but not authenticity or nonrepudiation, and therefore deemed limited. It requires a secure mechanism to deliver keys correctly. Each pair of users needs a unique key. Therefore, as the number of individuals increase, so does the number of keys.
These are all considered weaknesses of symmetric cryptography.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 783

QUESTION 252
Which of the following is more suitable for a hardware implementation?

A. Stream ciphers
B. Block ciphers
C. Cipher block chaining
D. Electronic code book

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Stream ciphers require a lot of randomness and encrypt individual bits at a time. This requires more processing power than block ciphers require, which is why stream ciphers are better suited to be implemented at the hardware level. Because block ciphers do not require as much processing power, they can be easily implemented at the software level.

Incorrect Answers:
B: Block ciphers can be easily implemented at the software level because they do not require as much processing power as stream ciphers.

C: Cipher block chaining is a block encryption method where each block of text, the key, and the value based on the previous block are processed in the algorithm and applied to the next block of text. Cipher block chaining is not more suitable for a hardware implementation.
D: Electronic code book is a block encryption method. It is not more suitable for a hardware implementation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 791

QUESTION 253
How many rounds are used by DES?

A. 16
B. 32
C. 64
D. 48

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
DES uses a 64-bit key, of which 8 bits are used for parity, and 56 bits make up the true key. DES divides the message into blocks, which are put through 16 rounds of transposition and substitution functions, and operates on them one at a time.

Incorrect Answers:
B, C, & D: RC5 is a block cipher that has a selection of parameters that it can use for block size, key size, and the number of rounds used. The number of rounds can go from 0 up to 255.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 809, 810

QUESTION 254
What is the key size of the International Data Encryption Algorithm (IDEA)?

A. 64 bits
B. 128 bitsC. 160 bits
D. 192 bits

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64-bit blocks of data, which is divided into 16 smaller blocks, with eight rounds of mathematical functions performed on each to produce a key that is 128 bits long.

Incorrect Answers:
A: The block of data that the International Data Encryption Algorithm (IDEA) operates on is 64 bit in size.
C: SHA produces a 160-bit hash value.
D: Tiger produces a hash size of 192 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 809, 810, 826

QUESTION 255
Which of the following is NOT an example of a block cipher?
A. Skipjack B.
IDEA
C. Blowfish
D. RC4

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RC4 is one of the most commonly used stream ciphers.

Incorrect Answers:
A: Skipjack is a symmetric key block cipher.
B: International Data Encryption Algorithm (IDEA) is a block cipher and runs on 64-bit blocks of data.
C: Blowfish is a block cipher that works on 64-bit blocks of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 809, 810
Miller, David R, Microsoft *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 159

QUESTION 256
The Diffie-Hellman algorithm is used for:

A. Encryption
B. Digital signature
C. Key agreement
D. Non-repudiation

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The Diffie-Hellman algorithm is the first asymmetric key agreement algorithm, which was developed by Whitfield Diffie and Martin Hellman.

Incorrect Answers:
A, B: The Diffie-Hellman algorithm does not offer encryption or digital signature functionality.
D: Non-repudiation requires digital signature functionality, which the Diffie-Hellman algorithm does not offer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 812, 813, 830

QUESTION 257
A one-way hash provides which of the following?

A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The verification of message integrity is an important application of secure hashes.

Incorrect Answers:
A, D: A hash function provides Integrity, not confidentiality or authentication.
B: A hash function provides Integrity, not availability.

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 825

QUESTION 258
Which of the following is not a one-way hashing algorithm?

A. MD2
B. RC4
C. SHA-1
D. HAVAL

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
RC4 is a Symmetric Key Algorithm.

Incorrect Answers:
A: MD2 is a one-way hashing algorithm.
C: SHA-1 is a one-way hashing algorithm.
D: HAVAL is a one-way hashing algorithm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 831

QUESTION 259
Which of the following statements pertaining to key management is NOT true?

A. The more a key is used, the shorter its lifetime should be.
B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The rules for keys and key management advise that the keys must be extremely random. It also states that the algorithm must make use of the full spectrum of the keyspace.

Incorrect Answers:
A, C, D: These options are included in the rules for keys and key management.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 842

QUESTION 260
Which of the following statements pertaining to link encryption is FALSE?

A. It encrypts all the data along a specific communication path.

B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.
Link encryption, which is sometimes called online encryption, is usually provided by service providers and is incorporated into network protocols. All of the information is encrypted, and the packets must be decrypted at each hop so the router, or other intermediate device, knows where to send the packet next. The router must decrypt the header portion of the packet, read the routing and address information within the header, and then re-encrypt it and send it on its way.

Incorrect Answers:
A: It is true that link encryption encrypts all the data along a specific communication path.
B: It is true that link encryption provides protection against packet sniffers and eavesdroppers.
C: It is true that user information, header, trailers, addresses and routing data that are part of the packets are encrypted.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 845-846

QUESTION 261
Which key agreement scheme uses implicit signatures?

A. MQV
B. DH
C. ECC
D. RSA

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
MQV (Menezes-Qu-Vanstone) is an authentication key agreement cryptography function very similar to Diffie-Hellman. The users' public keys are exchanged to create session keys. It provides protection from an attacker figuring out the session key because she would need to have both users' private keys.

The MQV elliptic curve key agreement method is used to establish a shared secret between parties who already possess trusted copies of each other's static public keys. Both parties still generate dynamic public and private keys and then exchange public keys. However, upon receipt of the other party's public key, each party calculates a quantity called an implicit signature using its own private key and the other party's public key. The shared secret is then generated from the implicit signature. The term implicit signature is used to indicate that the shared secrets do not agree if the other party's public key is not employed, thus giving implicit verification that the public secret is generated by the public party. An attempt at interception will fail as the shared secrets will not be the same shared secrets because the adversary's private key is not linked to the trusted public key.

Incorrect Answers:
B: DH (Diffie-Hellman) does not use implicit signatures.
C: ECC (Elliptic Curve Cryptosystem) does not use implicit signatures.
D: RSA does not use implicit signatures.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 815
https://www.certicom.com/index.php/mqv

QUESTION 262
Cryptography does NOT concern itself with which of the following choices?

A. Availability
B. Integrity
C. Confidentiality
D. Validation

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cryptography ensures the integrity of data, the confidentiality of the data and the validation of the sender and receiver of the data. Cryptography does not ensure the availability of the data.

Modern cryptography concerns itself with the following four objectives:

1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information) 4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information.

Incorrect Answers:
B: Cryptography does concern itself with integrity of data.
C: Cryptography does concern itself with confidentiality of data.
D: Cryptography does concern itself validation (of the source and destination of the data).

References:
http://searchsoftwarequality.techtarget.com/definition/cryptography

QUESTION 263
Which of the following does NOT concern itself with key management?

A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)
D. Key Exchange Algorithm (KEA)

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Cryptology involves 'hiding' data to make it unreadable by unauthorized parties. Keys are used to provide the encryption used in cryptology. However, cryptology itself is not concerned with the management of the keys used by the encryption algorithms.
Modern cryptography concerns itself with the following four objectives:
1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information) 4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information.

Incorrect Answers:
A: Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange.
B: The Diffie-Hellman protocol is a key agreement protocol.
D: Key Exchange Algorithm as its name suggests is used for the exchange of keys.

References:
http://searchsoftwarequality.techtarget.com/definition/cryptography

QUESTION 264
Which of the following encryption algorithms does NOT deal with discrete logarithms?
A. El Gamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
RSA does not deal with discrete logarithms.
RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a public key algorithm that is the most popular when it comes to asymmetric algorithms. RSA is a worldwide de facto standard and can be used for digital signatures, key exchange, and encryption. It was developed in 1978 at MIT and provides authentication as well as key encryption.
The security of this algorithm comes from the difficulty of factoring large numbers into their original prime numbers. The public and private keys are functions of a pair of large prime numbers, and the necessary activity required to decrypt a message from ciphertext to plaintext using a private key is comparable to factoring a product into two prime numbers.

Incorrect Answers:
A: El Gamal is a public key algorithm that can be used for digital signatures, encryption, and key exchange. It is based not on the difficulty of factoring large numbers but on calculating discrete logarithms in a finite field.
B: The Diffie-Hellman algorithm enables two systems to generate a symmetric key securely without requiring a previous relationship or prior arrangements. The algorithm allows for key distribution, but does not provide encryption or digital signature functionality. The algorithm is based on the difficulty of calculating discrete logarithms in a finite field.
D: The Elliptic Curve algorithm computes discrete logarithms of elliptic curves, which is different from calculating discrete logarithms in a finite field.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 815, 818

QUESTION 265
Which of the following statements pertaining to message digests is NOT true?

A. The original file cannot be created from the message digest.

B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Message digests are usually of fixed size.

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A message digest should be calculated using all of the original file's data regardless of whether the original data is more or less than 128 bytes.
The output of a hash function is called a message digest. The message digest is uniquely derived from the input file and, if the hash algorithm is strong, the message digest has the following characteristics:
1. The hash function is considered one-way because the original file cannot be created from the message digest.
2. Two files should not have the same message digest.
3. Given a file and its corresponding message digest, it should not be feasible to find another file with the same message digest.
4. The message digest should be calculated using all of the original file's data.

Incorrect Answers:
A: It is true that the original file cannot be created from the message digest.
B: It is true that two different files should not have the same message digest.
D: It is true that message digests are usually of fixed size.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 151152

QUESTION 266
Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis
B. Differential linear cryptanalysis
C. Birthday attack
D. Statistical attack

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Birthday Attack: Usually applied to the probability of two different messages using the same hash function that produces a common message digest; or given a message and its corresponding message digest, finding another message that when passed through the same hash function generates the same specific message digest. The term “birthday” comes from the fact that in a room with 23 people, the probability of two or more people having the same birthday is greater than 50%.

Incorrect Answers:
A: Differential Cryptanalysis is applied to private key cryptographic systems by looking at ciphertext pairs, which were generated through the encryption of plaintext pairs, with specific differences and analyzing the effect of these differences. This is not what is described in the question.
B: Linear Cryptanalysis is using pairs of known plaintext and corresponding ciphertext to generate a linear approximation of a portion of the key. Differential Linear Cryptanalysis is using both differential and linear approaches. This is not what is described in the question.
D: A statistical attack is exploiting the lack of randomness in key generation. This is not what is described in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 154155
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 828

QUESTION 267
Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

A. Timestamping
B. Repository
C. Certificate revocation
D. Internet Key Exchange (IKE)

Correct Answer: D
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Internet Key Exchange (IKE) is not included in a Public Key Infrastructure (PKI). IKE is a key management protocol used in IPSec.
A PKI may be made up of the following entities and functions:
- Certification authority
- Registration authority
- Certificate repository
- Certificate revocation system

- Key backup and recovery system
- Automatic key update
- Management of key histories
- Timestamping
- Client-side software

Incorrect Answers:
A: Timestamping is included in a Public Key Infrastructure (PKI).
B: Repository (certificate repository) is included in a Public Key Infrastructure (PKI).
C: Certificate revocation is included in a Public Key Infrastructure (PKI).
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 839

QUESTION 268
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
In order to protect against fraud in electronic fund transfers, the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC). A MAC is appended to the message before it is transmitted. At the receiving end, a MAC is generated from the received message and is compared to the MAC of an original message. A match indicates that the message was received without any modification occurring while en route.

Incorrect Answers:
A: A consortium including MasterCard and Visa developed SET in 1997 as a means of preventing fraud from occurring during electronic payments. SET provides confidentiality for purchases by encrypting the payment information. Thus, the seller cannot read this information. This is not what is described in the question. C: Cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16- or 32bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code (CRC) to the block. This is not what is described in the question.

D: The Secure Hash Standard (SHS) is a set of cryptographically secure hash algorithms specified by the National Institute of Standards and Technology (NIST). This is not what is described in the question.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 160
https://en.wikipedia.org/wiki/Secure_Hash_Standard

QUESTION 269
Which of the following statements pertaining to Secure Sockets Layer (SSL) is FALSE?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:

Explanation:
The SSL protocol was developed by Netscape in 1994 to secure Internet client-server transactions. The SSL protocol authenticates the server to the client using public key cryptography and digital certificates. In addition, this protocol also provides for optional client to server authentication. It supports the use of RSA public key algorithms, IDEA, DES and 3DES private key algorithms, and the MD5 hash function. Web pages using the SSL protocol start with HTTPs. SSL 3.0 and its successor, the Transaction Layer Security (TLS) 1.0 protocol are de-facto standards, but they do not provide the end-to-end capabilities of SET. TLS implements confidentiality, authentication, and integrity above the Transport Layer, and it resides between the application and TCP layer. Thus, TLS, as with SSL, can be used with applications such as Telnet, FTP, HTTP, and email protocols. Both SSL and TLS use certificates for public key verification that are based on the X.509 standard.

Incorrect Answers:
A: It is true that the SSL protocol was developed by Netscape to secure Internet client-server transactions.
C: It is true that Web pages using the SSL protocol start with HTTPS.
D: It is true that SSL can be used with applications such as Telnet, FTP and email protocols.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 160

QUESTION 270
What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

A. Internet Key Exchange (IKE)
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol

Correct Answer: A
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
Internet Key Exchange (IKE) is the protocol employed to establish a security association (SA) in the IPsec protocol suite.

Incorrect Answers:
B: Secure Key Exchange Mechanism allows different key distribution methods to be applied.
C: OAKLEY is a key-agreement protocol that enables authenticated parties to exchange keying material via an insecure link by making use of the Diffie–Hellman key exchange algorithm.
D: Internet Security Association and Key Management Protocol is a protocol defined for instituting Security Associations (SA) and cryptographic keys in an Internet environment.

References:
https://en.wikipedia.org/wiki/Internet_Key_Exchange
Miller, David R, Microsoft *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 226
https://en.wikipedia.org/wiki/Oakley_protocol
https://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol

QUESTION 271
Which of the following binds a subject name to a public key value?

A. A public-key certificate
B. A public key infrastructure
C. A secret key infrastructure
D. A private key certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

Incorrect Answers:
A: A public-key certificate contains a public key. However, it is the PKI (in particular the certificate authority) that verifies the subject's identity and binds the subject name to the public key value.
C: A secret key infrastructure is not a valid answer. A secret key can refer to a private key or more commonly to a shared key used in symmetric encryption. D: A private key (and its corresponding public key) is usually generated by a user or application. The public key is then validated and signed by a CA. A private key does not bind a subject name to a public key value.

References:
http://searchsecurity.techtarget.com/definition/PKI

QUESTION 272
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?

A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
The US American National Standards Institute (ANSI) X9 committee developed the concept of attribute certificate as a data structure that binds some attributes values with the identification information about its holder.
According to RFC 2828 [24], an attribute certificate is "a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate.
One of the advantages of attribute certificate is that it can be used for various other purposes. It may contain group membership, role clearance, or any other form of authorization.

Incorrect Answers:

A: An attribute certificate can be used to supplement a public-key certificate by storing additional information or attributes. However, an attribute certificate, not a public-key certificate is what is described in the question.
C: A digital certificate is another name for a public key certificate. It is an electronic document used to prove ownership of a public key. This is not what is described in the question.
D: A descriptive certificate is not a defined certificate type.

QUESTION 273
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Correct Answer: C
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
An Authority Revocation List (ARL) is a list of serial numbers for public key certificates issued to certificate authorities that have been revoked, and therefore should not be relied upon.

Incorrect Answers:
A: A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked, and should therefore, no longer trust entities presenting them.
B: A certificate revocation tree is a mechanism for distributing notices of certificate revocations, but is not supported in X.509.
D: A list of untrusted certificates is known as an untrusted CTL. It does not contain revoked certificates, but untrusted ones.

References:
https://en.wikipedia.org/wiki/Revocation_list
http://zvon.org/comp/r/ref-Security_Glossary.html#Terms~certificate_revocation_tree
https://technet.microsoft.com/en-us/library/dn265983.aspx

QUESTION 274
Who vouches for the binding between the data items in a digital certificate?

A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority

Correct Answer: B
Section: Security Engineering
Explanation

Explanation/Reference:
Explanation:
A certification authority issues digital certificates that include a public key and the identity of the owner. The matching private key is not publicly available, but kept secret by the end user who created the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A certification authority's duty in such schemes is to verify an applicant's credentials, so that users and relying parties are able to trust the information in the CA's certificates.

Incorrect Answers:
A: A registration authority (RA) confirms user requests for a digital certificate and informs the certificate authority (CA) to distribute it.
C: An issuing authority does not vouch for the binding between the data items in a digital certificate.
D: A vouching authority does not vouch for the binding between the data items in a digital certificate.

References:
https://en.wikipedia.org/wiki/Certificate_authority
http://searchsecurity.techtarget.com/definition/registration-authority

QUESTION 275
In the Open Systems Interconnect (OSI) Reference Model, at what level are TCP and UDP provided?

A. Transport
B. Network

C. Presentation
D. Application

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP and UDP are examples of protocols working at the transport layer.

Incorrect Answers:
B: TCP and UDP work at the transport layer, not at the network layer.
C: TCP and UDP work at the transport layer, not at the presentation layer.
D: TCP and UDP work at the transport layer, not at the application layer.

References:
https://en.wikipedia.org/wiki/Network_layer

QUESTION 276
Which of the following is TRUE regarding Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?

A. TCP is connection-oriented, UDP is not.

B. UDP provides for Error Correction, TCP does not.
C. UDP is useful for longer messages, rather than TCP.
D. TCP does not guarantee delivery of data, while UDP does guarantee data delivery.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP is a connection-oriented protocol, while UDP is a connectionless protocol.

Incorrect Answers:
B: TCP provides error corrections, while UDP does not. Not vice versa.
C: As UDP is a connectionless protocol it is less useful for longer messages, compared to the connection oriented protocol TCP.

D: As TCP is a connection-oriented protocol it guarantees delivery of data, while UDP does not guarantee data delivery as it is connectionless.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 525

QUESTION 277
The standard server port number for HTTP is which of the following?

A. 81
B. 80
C. 8080
D. 8180

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
HTTP uses port 80.

Incorrect Answers:
A: HTTP uses port 80, not port 81.
C: HTTP uses port 80, not port 8080.
D: HTTP uses port 80, not port 8180.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 537

QUESTION 278
Looking at the choices below, which ones would be the most suitable protocols/tools for securing e-mail?

A. PGP and S/MIME
B. IPsec and IKE
C. TLS and SSL
D. SSH

Correct Answer: A

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Secure MIME (S/MIME) is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.
PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Incorrect Answers:
B: IPSec is not used to protect e-mails. IPsec is used to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec can be implemented with the help of the IKE security architecture.
C: SSL and TLS are primarily used to protect HTTP traffic.
D: SSH is not used to protect e-mails. SSH allows remote login and other network services to operate securely over an unsecured network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 850-851

QUESTION 279
Which conceptual approach to intrusion detection system is the MOST common?

A. Behavior-based intrusion detection
B. Knowledge-based intrusion detection
C. Statistical anomaly-based intrusion detection
D. Host-based intrusion detection

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
An IDS can detect malicious behavior using two common methods. One way is to use knowledge-based detection which is more frequently used. The second detection type is behavior-based detection.

Incorrect Answers:
A: behavior-based detection is less common compared to knowledge-based detection.
C: A Statistical anomaly-based IDS is a behavioral-based system.

D: Host-based intrusion detection is not a conceptual iDS approach. The two conventional approaches are knowledge-based detection and behavior-based detection.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 280
Which of the following is most affected by denial-of-service (DoS) attacks?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Denial-of-service (DoS) attacks are attacks that prevent a system from processing or responding to legitimate traffic or requests for resources and objects. This type of attack makes the system unavailable.

Incorrect Answers:
A: Denial-of-service (DoS) attack main effect is not confidentiality, it is availability.
B: Denial-of-service (DoS) attack main effect is not integrity, it is availability.
C: Denial-of-service (DoS) attack main effect is not integrity, it is accountability.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 64

QUESTION 281
In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the BEST choice below.

A. Network Address Translation
B. Network Address Hijacking
C. Network Address Supernetting

D. Network Address Sniffing

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network address hijacking allows an attacker to reroute data traffic from a network device to a personal computer.

Also referred to as session hijacking, network address hijacking enables an attacker to capture and analyze the data addressed to a target system. This allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization.

Session hijacking involves assuming control of an existing connection after the user has successfully created an authenticated session. Session hijacking is the act of unauthorized insertion of packets into a data stream. It is normally based on sequence number attacks, where sequence numbers are either guessed or intercepted.

Incorrect Answers:
A: Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. This is not what is described in the question.
C: Network Address Supernetting is forming an Internet Protocol (IP) network from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing (CIDR) prefix. The new routing prefix for the combined network aggregates the prefixes of the constituent networks. This is not what is described in the question.
D: Network Address Sniffing: This is another bogus choice that sounds good but does not even exist. However, sniffing is a common attack to capture cleartext passwords and information unencrypted over the network. Sniffing is accomplished using a sniffer also called a Protocol Analyzer. A network sniffer monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it.

References:
http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm
http://wiki.answers.com/Q/What_is_network_address_hijacking
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p.

239

QUESTION 282
The Loki attack exploits a covert channel using which network protocol?

A. TCP
B. PPP

C. ICMP
D. SMTP

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The ICMP protocol was developed to send status messages, not to hold or transmit user data. But someone figured out how to insert some data inside of an ICMP packet, which can be used to communicate to an already compromised system. Loki is actually a client/server program used by hackers to set up back doors on systems. The attacker targets a computer and installs the server portion of the Loki software. This server portion "listens" on a port, which is the back door an attacker can use to access the system. To gain access and open a remote shell to this computer, an attacker sends commands inside of ICMP packets. This is usually successful, because most routers and firewalls are configured to allow ICMP traffic to come and go out of the network, based on the assumption that this is safe because ICMP was developed to not hold any data or a payload.

Incorrect Answers:
A: A Loki attack uses ICMP, not TCP.
B: A Loki attack uses ICMP, not PPP.
D: A Loki attack uses ICMP, not SMTP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 585

QUESTION 283
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SSL and TLS both support server authentication (mandatory) and client authentication (optional).

Incorrect Answers:
A: Peer-to-peer authentication is not support by SSL/TLS.
B: Server authentication (optional) is not a supported SSL/TLS authentication mode.
D: Role based authentication is not supported by SSL/TLS.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 3rd Edition, Wiley & Sons, Indianapolis, 2005, p. 353

QUESTION 284
At which layer of ISO/OSI does the fiber optics work?

A. Network layer
B. Transport layer
C. Data link layer
D. Physical layer

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The physical layer consists of the basic networking hardware transmission technologies, such as fiber optics, of a network.

Incorrect Answers:
A: The network layer is responsible for packet forwarding including routing through intermediate routers.
B: The transport layer provide host-to-host communication services for applications. It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.
C: The data link layer is responsible for media access control, flow control and error checking.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 530

QUESTION 285
Which of the following is TRUE of network security?

A. A firewall is a not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.

D. A black firewall is a necessity in today's connected world.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Firewalls are used to restrict access to one network from another network. Most companies use firewalls to restrict access to their networks from the Internet. Using a firewall is today mandatory.

Incorrect Answers:
A: Today, as almost all computers are interconnected through the Internet, usage of firewall is necessary.
C: Whitewall is not a concept used in the IT security domain.
D: Black firewall is not a concept used in the IT security domain.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 286
Which of the following is NOT a correct notation for an IPv6 address?

A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:
C. ABCD:EF01:2345:6789::1
D. 2001:DB8::8:800::417A

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as 4 hexadecimal digits and the groups are separated by colons (:).Consecutive sections of zeroes are replaced with a double colon (::).The double colon may only be used once in an address, as multiple use would render the address indeterminate. The address 2001:DB8::8:800::417A uses double colon twice, which is illegal.

Incorrect Answers:
A: 2001:0db8:0:0:0:0:1428:57ab is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers.

B: ABCD:EF01:2345:6789:1 is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers.
C: ABCD:EF01:2345:6789::1 is a well-formed IPv6 address with 8 groups of 16-bit hexadecimal numbers, and only one double colon.

References:
https://en.wikipedia.org/wiki/IPv6

QUESTION 287
Which layer deals with Media Access Control (MAC) addresses?

A. Data link layer
B. Physical layer
C. Transport layer
D. Network layer

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The data link layer is divided into two functional sublayers: the Logical Link Control (LLC) and the Media Access Control (MAC).

Incorrect Answers:
B: Media Access Control layer is part of the Data Link Layer, not the Physical layer.
C: Media Access Control layer is part of the Data Link Layer, not the Transport layer.
D: Media Access Control layer is part of the Data Link Layer, not the Network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 288
What is a decrease in amplitude as a signal propagates along a transmission medium BEST known as?

A. Crosstalk
B. Noise
C. Delay distortion
D. Attenuation

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Attenuation is the loss of signal strength (amplitude) as it travels. The longer a cable, the more attenuation occurs, which causes the signal carrying the data to deteriorate. This

Incorrect Answers:
A: Crosstalk is not decrease in amplitude. Crosstalk is a phenomenon that occurs when electrical signals of one wire spill over to the signals of another wire. B: Loss in signal strength is called attenuation. Noise does not affect signal strength. C: Delay distortion does not affect signal strength.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 561

QUESTION 289
Which device acting as a translator is used to connect two networks or applications from Layer 4 up to Layer 7 of the ISO/OSI Model?

A. Bridge
B. Repeater
C. Router
D. Gateway

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A gateway works at OSI Application layer, where it connects different types of networks; performs protocol and format translations.

Incorrect Answers:
A: A bridge works at the data link layer, not the application layer.
B: A repeater works at the physical layer, not the application layer.
C: A router works at the transport layer, not the application layer.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 623

QUESTION 290

In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?

A. Transport layer
B. Application layer
C. Physical layerD. Network layer

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
When two computers are going to communicate through a connection-oriented Protocol, such as TCP/IP, they will first agree on how much information each computer will send at a time, how to verify the integrity of the data once received, and how to determine whether a packet was lost along the way. The two computers agree on these parameters through a handshaking process at the transport layer, layer 4.

Incorrect Answers:
B: Connection-oriented protocols are located at transport layer, not at the Application layer.
C: Connection-oriented protocols are located at transport layer, not at the Physical layer.
D: Connection-oriented protocols are located at transport layer, not at the Network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 525

QUESTION 291
Which of the following transmission media would NOT be affected by cross talk or interference?

A. Copper cable
B. Radio System
C. Satellite radiolink
D. Fiber optic cables

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

Fiber-optic cable uses a type of glass that carries light waves, which represent the data being transmitted. Light waves are not affected by cross talk or interference.

Incorrect Answers:
A: Copper cables suffer from cross talk and interference.
B: Radio Systems suffer from cross talk and interference.
C: Satellite radiolink suffers from cross talk and interference.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 559

QUESTION 292
What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

A. SYN Flood attack
B. Smurf attack
C. Ping of Death attack
D. Denial of Service (DoS) attack

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In a Smurf attack the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim’s network broadcast address. This means that each system on the victim’s subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets—which is the victim’s address.

Incorrect Answers:
A: A Syn flood attack does not involve spoofing and ICMP ECHO broadcasts. A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. C: A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. It could cause a buffer overflow, but it does not involve ICMP ECHO broadcast packets
D: A DoS attack does not use spoofing or ICMP ECHO broadcasts. In a DoS attack the attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 587

QUESTION 293
This OSI layer has a service that negotiates transfer syntax and translates data to and from the transfer syntax for users, which may represent data using different syntaxes. At which of the following layers would you find such service?

A. Session
B. Transport
C. Presentation
D. Application

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The presentation layer is not concerned with the meaning of data, but with the syntax and format of the data. It works as a translator, translating the format an application is using to a standard format used for passing messages over a network.

Incorrect Answers:
A: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications.
B: The transport layer provide host-to-host communication services for applications. It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.
D: The application layer as the user interface responsible for displaying received information to the user.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 522

QUESTION 294
The International Organization for Standardization / Open Systems Interconnection (ISO/OSI) Layer 7 does NOT include which of the following?

A. SMTP (Simple Mail Transfer Protocol)
B. TCP (Transmission Control Protocol)
C. SNMP (Simple Network Management Protocol
D. HTTP (Hypertext Transfer Protocol)

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TCP is an OSI layer 4 (transport layer) protocol.
Some examples of the protocols working at OSI layer 7, the application layer, are the Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), Line Printer Daemon (LPD),File Transfer Protocol (FTP), Telnet, and Trivial File Transfer Protocol (TFTP).

Incorrect Answers:
A: SMTP is an OSI Layer 7 protocol.
C: SNMP is an OSI Layer 7 protocol.
D: HTTP is an OSI Layer 7 protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 521

QUESTION 295
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?

A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The OSI/ISO Layers are not designed for monitoring network devices.

Incorrect Answers:
A: The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology.
C: The goal of the OSI model goal is the interoperability of diverse communication systems with standard protocols.
D: The original version of the OSI model defined seven protocol layers, defining a protocol stack.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 296
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers 6 is which of the following?

A. Application Layer
B. Presentation Layer
C. Data Link Layer
D. Network Layer

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Presentation Layer is layer 6 in the OSI model.

Incorrect Answers:
A: The Application Layer is layer 7 in the OSI model.
C: The Data Link Layer is layer 2 in the OSI model.
D: The Network Layer is layer 3 in the OSI model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 522

QUESTION 297

In telephony different types of connections are being used. The connection from the phone company's branch office to local customers is referred to as which of the following choices?

A. new loop
B. local loop
C. loopback
D. indigenous loop

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In telephony, the local loop is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the common carrier or telecommunications service provider's network.

Incorrect Answers:
A: New loop is not a type of connection.
C: A loopback interface is a serial communications transceiver can use loopback for testing its functionality.
D: Indigenous loop is not a type of connection.

References:
https://en.wikipedia.org/wiki/Local_loop

QUESTION 298
Communications and network security relates to transmission of which of the following?

A. voice
B. voice and multimedia
C. data and multimedia
D. voice, data and multimedia

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

Security applies to all types of transmitted data whether it is voice, data or multimedia.

Incorrect Answers:
A: Not only voice transfer must be secure. Data and multimedia transmission must be secure as well.
B: Not only voice and multimedia transfers must be secure. Data transmission must be secure as well.
C: Not only data and multimedia transfers must be secure. Voice transmission must be secure as well.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 515

QUESTION 299
One of the following assertions is NOT a characteristic of Internet Protocol Security (IPSec)

A. Data cannot be read by unauthorized parties
B. The identity of all IPsec endpoints are confirmed by other endpoints
C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec uses the IP protocol to deliver packets. IP treats every packet independently, and the packets can arrive out of order.

Incorrect Answers:
A: The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. IPSec data cannot be read by unauthorized parties.
B: IPSec, through the use of IKE (Internet Key Exchange), ensures the identity of each endpoint is confirmed by the other endpoints.
D: An ESP packet, used by IPSec to transfer data, includes a Sequence Number which counts the packets that have been transmitted.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 860

QUESTION 300
Tim is a network administrator of Acme Inc. He is responsible for configuring the network devices. John the new security manager reviews the configuration of the Firewall configured by Tim and identifies an issue.

This specific firewall is configured in failover mode with another firewall. A sniffer on a PC connected to the same switch as the firewalls can decipher the credentials, used by Tim while configuring the firewalls.

Which of the following should be used by Tim to ensure that no one can eavesdrop on the communication?

A. SSH
B. SFTP
C. SCP
D. RSH

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network devices are often configured by a command line interface such as Telnet. Telnet, however is insecure in that the data including login credentials is unencrypted as it passes over the network. A secure alternative is to use Secure Shell (SSH).
Secure Shell (SSH) functions as a type of tunneling mechanism that provides terminal-like access to remote computers. SSH is a program and a protocol that can be used to log into another computer over a network.
SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, which provide the same type of functionality SSH offers but in a much less secure manner. SSH is a program and a set of protocols that work together to provide a secure tunnel between two computers. The two computers go through a handshaking process and exchange (via Diffie-Hellman) a session key that will be used during the session to encrypt and protect the data sent.

Incorrect Answers:
B: SFTP (Secure File Transfer Protocol) is FTP over SSH. SFTP is secure but it is not used to configure network devices.
C: SCP (Secure Copy) is an application used to copy files over a network using an SSH connection. SCP is secure but it is not used to configure network devices.
D: RSH (Remote Shell) offers remote command line functionality. However, like Telnet, RSH is insecure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 859-860 http://www.novell.com/documentation/suse91/suselinux-adminguide/html/ch19s02html http://en.wikipedia.org/wiki/Remote_Shell http://en.wikipedia.org/wiki/Secure_copy

QUESTION 301
One of the following statements about the differences between PPTP and L2TP is NOT true

A. PPTP can run only on top of IP networks.
B. PPTP is an encryption protocol and L2TP is not.

C. L2TP works well with all firewalls and network devices that perform NAT.
D. L2TP supports AAA servers

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
L2TP is not compatible with NAT.
Incorrect Answers:
A: PPTP was designed to provide a way to tunnel PPP connections through an IP network.
B: PPTP uses PPP data packets that encrypted using Microsoft Point to Point Encryption (MPPE), while L2TP on the other hand does not provide any encryption or confidentiality by itself.
D: Radius AAA servers can be configured to use L2TP tunnels.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 702-703

QUESTION 302
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network availability can be defined as an area of the of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability.

Incorrect Answers:
A: Netware is a protocol family from the Novell Corporation, and not an area within the Network Security domain.
C: Network acceptability is not an area in the Telecommunications and Network Security domain.

D: Network accountability is not an area in the Telecommunications and Network Security domain.

QUESTION 303
Which of the following are well known ports assigned by the IANA?

A. Ports 0 to 255
B. Ports 0 to 1024
C. Ports 0 to 1023
D. Ports 0 to 127

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The port numbers in the range from 0 to 1023 are the well-known ports or system ports.

Incorrect Answers:
A: The range of the well-known ports is from 0 to 1023, not from 0 to 255.
B: The range of the well-known ports is from 0 to 1023, not from 0 to 1024.
D: The range of the well-known ports is from 0 to 1023, not from 0 to 127.

References:
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 304
What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?

A. 80 meters
B. 100 metersC. 185 meters
D. 500 meters

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

The maximum length of a Category 5 10Base-T cable is 100 meters.

Incorrect Answers:
A: The maximum length is 100 meters, not 80 meters.
C: The maximum length is 100 meters, not 185 meters.
D: The maximum length is 100 meters, not 500 meters.

References:
https://en.wikipedia.org/wiki/Ethernet_over_twisted_pair

QUESTION 305
Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?
A. Web transactions.
B. EDI transactions.
C. Telnet transactions.
D. Electronic Payment transactions.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Secure Sockets Layer (SSL) protects mainly web-based traffic.

Incorrect Answers:
B: The Secure Sockets Layer (SSL) does not protect EDI transactions. It protects Web transactions.
C: The Secure Sockets Layer (SSL) protects Web transactions, not Telnet transactions.
D: The Secure Sockets Layer (SSL) protects Web transactions, not Electronic Payment transactions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 708

QUESTION 306
Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the:

A. Transport Layer Security (TLS) Internet Protocol.
B. Transport Layer Security (TLS) Data Protocol.
C. Transport Layer Security (TLS) Link Protocol.

D. Transport Layer Security (TLS) Handshake Protocol.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The TLS protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

Incorrect Answers:
A: TLS Internet Protocol is not part of the Transport Layer Security (TLS) protocol.
B: TLS Data Protocol is not part of the Transport Layer Security (TLS) protocol.
C: TLS Link Protocol is not part of the Transport Layer Security (TLS) protocol.

References:
https://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 307
Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:

A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Peer authentication is an integral part of the SSL protocol. Peer authentication relies on the availability of trust anchors and authentication keys.

Incorrect Answers:
B: Peer authentication, not peer identification, is part of the SSL protocol.
C: SSL uses Peer authentication, not Server Authentication, for encrypting data that is sent over a session.
D: SSL uses Peer authentication, not Name Resolution, for encrypting data that is sent over a session.

QUESTION 308
Which of the following is TRUE related to network sniffing?

A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C. Sniffers take over network connections.
D. Sniffers send IP fragments to a system that overlap with each other.

Correct Answer: A
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
Packet sniffing is the process of intercepting data as it is transmitted over a network.
A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

Incorrect Answers:
B: Sniffers do not alter the source address of a computer to disguise and exploit weak authentication methods. This describes IP spoofing.
C: Sniffers do not take over network connections. Session Hijacking tools allow an attacker to take over network connections, kicking off the legitimate user or sharing a login.
D: Sniffers do not send IP fragments to a system that overlap with each other. This describes a Malformed Packet attack. Malformed Packet attacks are a type of DoS attack that involves one or two packets that are formatted in an unexpected way. Many vendor product implementations do not take into account all variations of user entries or packet types. If software handles such errors poorly, the system may crash when it receives such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other (the fragment offset values are incorrectly set. Some unpatched Windows and Linux systems will crash when the encounter such packets.

References:
http://www.techopedia.com/definition/4113/sniffer

QUESTION 309
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?

A. Fiber Optic cable
B. Coaxial cable

C. Twisted Pair cable
D. Axial cable

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Because fiber-optic cable passes electrically non-conducting photons through a glass medium, it is immune to electromagnetic interference.

Incorrect Answers:
B: As an electromagnetic field carries the signal in the Coaxial cable, the signal can be affected by external inference.
C: As an electromagnetic field carries the signal in the Twisted Pair cable, the signal can be affected by external inference.
D: An axial cable is a coaxial cable with only one conductor instead of two conductors. Compared to a coaxial cable the axial cable is more vulnerable to electromagnetic interference.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 100

QUESTION 310
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Alternative routing provides two different cables from the local exchange to your site, so you can protect against cable failure as your service will be maintained on the alternative route.

Incorrect Answers:

B: With diverse routing, you can protect not only against cable failure but also against local exchange failure as there are two separate routes from two exchanges to your site.
C: Lang-haul refers to circuits that span large distances, not between your site and the local exchange, such as interstate or international.
D: Last mile circuit protection does not provide an extra connection.

References:
https://en.wikipedia.org/wiki/Routing_in_the_PSTN

QUESTION 311
Which service usually runs on port 25?

A. File Transfer Protocol (FTP)
B. Telnet
C. Simple Mail Transfer Protocol (SMTP)
D. Domain Name Service (DNS)

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SMTP uses port 25.

Incorrect Answers:
A: FTP uses port 21.
B: Telnet uses port 23.
D: DNS uses port 53.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1289

QUESTION 312
Which port does the Post Office Protocol Version 3 (POP3) make use of?

A. 110
B. 109
C. 139
D. 119

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
POP3 uses port 110.

Incorrect Answers:
B: Port 109 is used by POP2.
C: Port 139 is used by the NetBIOS Session Service.
D: Port 119 is used by NNTP.

References:
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 313
Behavioral-based systems are also known as?

A. Profile-based systems
B. Pattern matching systems
C. Misuse detective systems
D. Rule-based IDS

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Behavioral-based IDSs are also known as profile-based systems.

Incorrect Answers:
B: A pattern matching IDS does not work in the same way as a Behavioral-based IDS.
C: There is no Intrusion Detection System type called Misuse detective systems.
D: A Rule-based IDS does not work in the same way as a Behavioral-based IDS.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 260

QUESTION 314
Which type of attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number?

A. IP spoofing attack
B. SYN flood attack
C. TCP sequence number attack
D. Smurf attack

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A TCP sequence prediction attack is an attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets.

Incorrect Answers:
A: IP spoofing attacks do not use TCP sequence numbers. IP spoofing is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity.
B: Syn flood attacks do not use TCP sequence numbers. A SYN flood DoS attack where an attacker sends a succession of SYN packets with the goal of overwhelming the victim system so that it is unresponsive to legitimate traffic.
D: A Smurf attack does not use TCP sequence numbers. In a smurf attack the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address.

References:
https://en.wikipedia.org/wiki/TCP_sequence_prediction_attack

QUESTION 315
Which of the following media is MOST resistant to EMI interference?

A. microwave
B. fiber optic
C. twisted pair
D. coaxial cable

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Because fiber-optic cable passes electrically non-conducting photons through a glass medium, it is resistant to Electromagnetic interference (EMI).

Incorrect Answers:
A: Microwaves are vulnerable to Electromagnetic interference (EMI).
C: Twisted pair cables are vulnerable to Electromagnetic interference (EMI).
D: Coaxial cables are vulnerable to Electromagnetic interference (EMI).

QUESTION 316
Which OSI/ISO layer defines how to address the physical devices on the network?

A. Session layer
B. Data Link layer
C. Application layer
D. Transport layer

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The data link layer is responsible for proper communication within the network components and for changing the data into the necessary format (electrical voltage) for the physical layer.

Incorrect Answers:
A: The session layer protocols set up connections between applications; maintain dialog control; and negotiate, establish, maintain, and tear down the communication channel.
C: The protocols at the application layer handle file transfer, virtual terminals, network management, and fulfilling networking requests of applications.
D: The protocols at the transport layer handle end-to-end transmission and segmentation of a data stream.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 317

Which layer defines how packets are routed between end systems?

A. Session layer
B. Transport layer
C. Network layer
D. Data link layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The responsibilities of the network layer protocols include internetworking service, addressing, and routing.

Incorrect Answers:
A: The session layer protocols set up connections between applications; maintain dialog control; and negotiate, establish, maintain, and tear down the communication channel.
B: The protocols at the transport layer handle end-to-end transmission and segmentation of a data stream.
D: The data link layer is responsible for proper communication within the network components and for changing the data into the necessary format (electrical voltage) for the physical layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 531

QUESTION 318
At which of the OSI/ISO model layer is IP implemented?

A. Session layer
B. Transport layer
C. Network layer
D. Data link layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Internet Protocol (IP) is implemented at the Network layer.

Incorrect Answers:
A: The session layer implements protocols such as NFS and NetBIOS, but not the IP protocol.
B: The transport layer implements protocols such as TCP and UDP, but not the IP protocol.
D: The Data link layer implements protocols such as ARP and ATM, but not the IP protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 531

QUESTION 319
Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The data link layer is responsible for proper communication within the network devices and for changing the data into the necessary format (electrical voltage) for the physical link or channel.

Incorrect Answers:
A: The protocols at the transport layer handle end-to-end transmission and segmentation of a data stream.
B: The responsibilities of the network layer protocols include internetworking service, addressing, and routing.
D: The physical layer include network interface cards and drivers that convert bits into electrical signals and control the physical aspects of data transmission

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 531

QUESTION 320
Which OSI/ISO layer is the Media Access Control (MAC) sublayer part of?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Data link layer is divided into the Logical Link Control (LLC) and the Media Access Control (MAC) sublayers.

Incorrect Answers:
A: The MAC sublayer is part of the data link layer, not the transport layer.
B: The MAC sublayer is part of the data link layer, not the network layer.
D: The MAC sublayer is part of the data link layer, not the physical layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 531

QUESTION 321
Which OSI/OSI layer defines the X.24, V.35, X.21 and HSSI standard interfaces?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
X.25, V.35, X21 and HSSI all work at the physical layer in the OSI model.
X.25 is an older WAN protocol that defines how devices and networks establish and maintain connections.
V.35 is the interface standard used by most routers and DSUs that connect to T-1 carriers.
X21 is a physical and electrical interface.
High-Speed Serial Interface (HSSI) is a short-distance communications interface.

Incorrect Answers:
A: X.25, V.35, X21 and HSSI all work at the physical layer, not the transport layer.
B: X.25, V.35, X21 and HSSI all work at the physical layer, not the network layer.
C: X.25, V.35, X21 and HSSI all work at the physical layer, not the data link layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 679

QUESTION 322
How many layers are defined within the US Department of Defense (DoD) TCP/IP Model?

A. 7
B. 5
C. 4
D. 3
Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The TCP/IP model includes the following four layers: application, host-to-host, Internet, and Network access.

Incorrect Answers:
A: The OSI have seven layers, while the TCP/IP model only has four layers.
B: The TCP/IP model has four layers, not five.
D: The TCP/IP model has four layers, not three.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 323
Which layer of the TCP/IP protocol model defines the IP datagram and handles the routing of data across networks?

A. Application layer
B. Host-to-host transport layer
C. Internet layer
D. Network access layer

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
The Internet layer of the TCP/IP protocol handles the IP packets, the IP datagrams, and routes them through the network.

Incorrect Answers:
A: The application layer includes protocols that support the applications. The application layer includes protocols such as SMTP, HTTP, and FTP, but not the IP protocol.
B: The Host-to-host transport layer includes the TCP protocol, but not the IP protocol. The transport layer provides end-to-end data transport services and establishes the logical connection between two communicating computers.
D: The Network Access Layer defines how to use the network to transmit an IP datagram, but it does not define or route the IP datagrams.
The Network Access Layer is the lowest layer of the TCP/IP protocol hierarchy. The protocols in this layer provide the means for the system to deliver data to the other devices on a directly attached network.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 324
Which layer of the TCP/IP protocol model would BEST correspond to the OSI/ISO model's network layer?

A. Network access layer
B. Application layer
C. Host-to-host transport layer
D. Internet layer

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The OSI model Network layer corresponds to the TCP/IP model Internet layer.

Incorrect Answers:
A: The Network access layer corresponds to the data link and physical layers of the OSI model.
B: The Application layer corresponds to the Application, Presentation, and the Session layers of the OSI model.
C: The Host-to-host transport layer corresponds to the Transport layer of the OSI model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 325
Which layer of the DoD TCP/IP model controls the communication flow between hosts?

A. Internet layer
B. Host-to-host transport layer
C. Application layer
D. Network access layer

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Host-to-host transport layer provides end-to-end data transport services and establishes the logical connection between two communicating hosts.

Incorrect Answers:
A: The internet layer has the responsibility of sending packets across potentially multiple networks. This process is called routing.
C: The application layer includes the protocols used by most applications for providing user services or exchanging application data over the network connections established by the lower level protocols.
D: The link layer (network access layer) is used to move packets between the Internet layer interfaces of two different hosts on the same link.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 525

QUESTION 326
How many bits compose an IPv6 address?

A. 32 bits B.
64 bits
C. 96 bits
D. 128 bits

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPv6 uses 128 bits for its addresses.

Incorrect Answers:
A: IPv4 uses 32 bits for its addresses, while IPv6 uses 128 bits.
B: IPv6 uses 128 bits, not 64 bits, for its addresses.
C: IPv6 uses 128 bits, not 96 bits, for its addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 541

QUESTION 327
What protocol is used on the Local Area Network (LAN) to obtain an IP address from its known MAC address?

A. Reverse address resolution protocol (RARP)
B. Address resolution protocol (ARP)
C. Data link layer
D. Network address translation (NAT)

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
RARP translates a MAC address into an IP address.

Incorrect Answers:
B: ARP translates the IP address into a MAC address, not the other way around.
C: Network address translation (NAT) is a methodology of remapping one IP address space into another IP address space. NAT does handle MAC addresses. D: The data link layer does not use IP addresses. It transfers data between adjacent network nodes in a wide area network (WAN) or between nodes on the same local area network (LAN) segment.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 740

QUESTION 328
Which of the following security-focused protocols has confidentiality services operating at a layer different from the others?

A. Secure HTTP (S-HTTP)
B. FTP Secure (FTPS)
C. Secure socket layer (SSL)
D. Sequenced Packet Exchange (SPX)

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
S-HTTP provides application layer security, while the other protocols provide transport layer security.

Incorrect Answers:
B: FTPS can use SSL.
FTPS (also known as FTPES, FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.
C: SSL can be used by FTPS. SSL provides transport layer security.
D: SPX is a transport layer protocol (layer 4 of the OSI Model).

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 856

QUESTION 329
Packet Filtering Firewalls can also enable access for:

A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering is a firewall technology that makes access decisions based upon network-level protocol header values. The filters can make access decisions based upon the following basic criteria:
▪ Source and destination port numbers (such as an application port or a service number) ▪
Protocol types
▪ Source and destination IP addresses
▪ Inbound and outbound traffic direction

Incorrect Answers:
B: Only authorized ports or service numbers, not unauthorized, would be granted access through the firewall.
C: Packet Filtering Firewalls do not grant access through ex-service numbers. They use service numbers.
D: Packet Filtering Firewalls do not grant access through service integers. A service has a number, not an integer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 330
Which of the following is NOT a VPN communications protocol standard?

A. Point-to-point tunneling protocol (PPTP)
B. Challenge Handshake Authentication Protocol (CHAP)
C. Layer 2 tunneling protocol (L2TP)
D. IP Security

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Challenge Handshake Authentication Protocol (CHAP) is used for authentication only. It is not a VPN communications protocol.

Incorrect Answers:
A: The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks.
C: Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).
D: IP Security, Internet Protocol Security (IPsec), can be used to setup secure VPN connections.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 683

QUESTION 331
What layer of the OSI/ISO model does Point-to-point tunneling protocol (PPTP) work at?

A. Data link layer
B. Transport layer
C. Session layer
D. Network layer

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
PPTP works at the data link layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 708

QUESTION 332
Which of the following statements pertaining to VPN protocol standards is false?

A. L2TP is a combination of PPTP and L2F.
B. L2TP and PPTP were designed for single point-to-point client to server communication.
C. L2TP operates at the network layer.
D. PPTP uses native PPP authentication and encryption services.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
L2TP works at the data link layer, not at the network layer.

Incorrect Answers:
A: L2TP is a hybrid of PPTP and L2F
B: Both L2TP and PPTP are designed for single point-to-point connections.
D: PPTP extends and protects PPP connections.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 708

QUESTION 333
Which IPSec operational mode encrypts the entire data packet (including header and data) into an IPSec packet?

A. Authentication mode
B. Tunnel mode
C. Transport modeD. Safe mode

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected.
Incorrect Answers:
A: IPsec does not have an Authentication mode
C: In tunnel mode only the payload is protected.
D: IPsec does not have a Safe mode.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 861

QUESTION 334
Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?

A. Category 5e UTP
B. Category 2 UTP
C. Category 3 UTP
D. Category 1e UTP

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Category 5 UTP cable provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet). Category 5 was superseded by the category 5e (enhanced) specification.

Incorrect Answers:
B: The maximum frequency suitable for transmission over Category 2 UTP cable is 4 MHz, and the maximum bandwidth is 4Mbit/s.
C: Category 3 UTP was widely used in computer networking in the early 1990s for 10BASE-T Ethernet (and to a lesser extent for 100BaseVG Ethernet, token ring and 100BASE-T4), but from the early 2000s new structured cable installations were almost invariably built with the higher performing Cat 5e or Cat 6 cable required by 100BASE-TX.
D: The maximum frequency suitable for transmission over Category 1 UTP cable is 1 MHz, but Category 1 is not considered adequate for data transmission.

References:
https://en.wikipedia.org/wiki/Category_5_cable

QUESTION 335
In which LAN transmission method is a source packet copied and sent to specific multiple destinations but not ALL of the destinations on the network?

A. Overcast
B. Unicast
C. Multicast D. Broadcast

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:

Explanation:
If the packet needs to go to a specific group of systems, the sending system uses the multicast method.

Incorrect Answers:
A: There is no LAN transmission method called Overcast.
B: Unicast is a one-to-one transmission.
D: If a system wants all computers on its subnet to receive a message, it will use the broadcast method.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 579

QUESTION 336
Which of the following can prevent hijacking of a web session?

A. RSA
B. SET
C. SSL
D. PPP

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
One method to prevent web session hijacking is to encrypt the data traffic passed between the parties by using SSL/TLS.

Incorrect Answers:
A: RSA cannot be used to prevent web session hijacking.
B: SET cannot be used to prevent web session hijacking.
D: PPP cannot be used to prevent web session hijacking.
References:
https://en.wikipedia.org/wiki/Session_hijacking

QUESTION 337
What is defined as the rules for communicating between computers on a Local Area Network (LAN)?

A. LAN Media Access methods
B. LAN topologies

C. LAN transmission methods
D. Contention Access Control

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Media access technologies deal with how these systems communicate over the network media. LAN access technologies set up the rules of how computers will communicate on the Local Area Network.

Incorrect Answers:
B: Network topology is not defined by rules of communication. It is the arrangement of the various elements (links, nodes, etc.) of a computer network.
C: The communications rules on a LAN is called Media Access rules, not transmissions methods.
D: Contention Access Control is just used to avoid collisions. To communicate LAN Media Access methods are used.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 565

QUESTION 338
Which of the following is a LAN transmission method?

A. Broadcast
B. Carrier-sense multiple access with collision detection (CSMA/CD)
C. Token ring
D. Fiber Distributed Data Interface (FDDI)

Correct Answer: A
Section: Communication and Network Security
Explanation
Explanation/Reference:
Explanation:
Broadcast, unicast, and multicast are all LAN transmissions methods.

Incorrect Answers:
B: CSMA/CD is a media access method, not a LAN transmission method.
C: Token ring is a media access methodology, not a LAN transmission method.
D: FDDI is a media access methodology, not a LAN transmission method.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 579

QUESTION 339
In what LAN topology do all the transmissions of the network travel the full length of cable and are received by all other stations?

A. Bus topology
B. Ring topology
C. Star topology
D. FDDI topology

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In a bus topology a linear, single cable for all computers attached is used. All traffic travels the full cable and can be viewed by all other computers.

Incorrect Answers:
B: In a ring topology all computers are connected by a unidirectional transmission link, and the cable is in a closed loop.
C: In a star topology all computers are connected to a central device, which provides more resilience for the network.
D: FDDI is a media access methodology, not a LAN topology.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 566

QUESTION 340
Which of the following IEEE standards defines the token ring media access method?

A. 802.3
B. 802.11
C. 802.5
D. 802.2

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Token Ring technology is defined by the IEEE 802.5 standard.

Incorrect Answers:
A: IEEE 802.3 is the IEEE standard defining the physical layer and data link layer's media access control (MAC) of wired Ethernet.
B: IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication.
D: IEEE 802.2 is the original name of the standard which defines Logical Link Control (LLC) as the upper portion of the data link layer of the OSI Model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 570

QUESTION 341
Which of the following LAN devices only operates at the physical layer of the OSI/ISO model?

A. Switch
B. Bridge
C. Hub
D. Router

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A hub is a multiport repeater. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance.

Incorrect Answers:
A: Basic switches work at the data link layer. Layer 3, layer 4, and other layer switches have more enhanced functionality than layer 2 switches.
B: A bridge is a LAN device used to connect LAN segments. It works at the data link layer.
D: Routers work at the network layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 612

QUESTION 342
Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

A. ISDN
B. SLIP
C. xDSL
D. T1

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Serial Line Internet Protocol (SLIP) is an older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial - up.

Incorrect Answers:
A: ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is digital, not serial.
C: xDSL is a digital technology. xDSL is the term for the Broadband Access technologies based on Digital Subscriber Line (DSL) technology
D: The T1 carrier is the most commonly used digital, not serial, transmission service.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 138

QUESTION 343
Which xDSL flavor, appropriate for home or small offices, delivers more bandwidth downstream than upstream and over longer distance?

A. VDSL B.
SDSL
C. ADSL
D. HDSL

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

Asymmetric DSL (ADSL) provides data travel downstream faster than upstream. Upstream speeds are 128 Kbps to 384 Kbps, and downstream speeds can be as fast as 768 Kbps. Generally used by residential users. ADSL is appropriate for small offices.

Incorrect Answers:
A: VDSL is basically ADSL at much higher data rates (13 Mbps downstream and 2 Mbps upstream).
B: Symmetric DSL (SDSL) provides data travel upstream and downstream at the same rate.
D: High-Bit-Rate DSL (HDSL) provides T1 (1.544 Mbps) speeds over regular copper phone wire without the use of repeaters.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 699

QUESTION 344
Another name for a VPN is a:

A. tunnel
B. one-time password
C. pipeline
D. bypass

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A virtual private network (VPN) is a secure, private connection through an untrusted network. VPN technology requires a tunnel to work and it assumes encryption.

Incorrect Answers:
B: A one-time password is not the same as a VPN.
C: Tunnel, not pipeline, can be used as a name for a VPN.
D: Tunnel, not bypass, can be used as a name for a VPN.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 702

QUESTION 345
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?

A. DS-0
B. DS-1
C. DS-2
D. DS-3

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Digital Signal Level 1 (DS - 1) provides 1.544 Mbps over a T1 line.

Incorrect Answers:
A: Digital Signal Level 0 (DS - 0) provides from 64 Kbps up to 1.544 Mbps on a Partial T1 line.
C: There is no framing specification named DS-2.
D: Digital Signal Level 3 (DS - 3) is a specification for T3, not for T1.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 165

QUESTION 346
Which of the following is the BIGGEST concern with firewall security?

A. Internal hackers
B. Complex configuration rules leading to misconfiguration
C. Buffer overflows
D. Distributed denial of service (DDoS) attacks

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Firewalls filter traffic based on a defined set of rules. The rules must be configured correctly for the firewall to provide the intended security.
Incorrect Answers:

A: Firewalls main duty is to defend against external, not internal, threats.
C: Firewalls do not product from buffer overflows attacks.
D: Firewalls can help in defending from DDoS attacks, but the main concern with firewall is to configure them correctly.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 25

QUESTION 347
Which of the following is the SIMPLEST type of firewall?

A. Stateful packet filtering firewall
B. Packet filtering firewall
C. Dual-homed host firewall
D. Application gateway

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering was the first generation of firewalls and it is the most rudimentary type of all of the firewall technologies.

Incorrect Answers:
A: A stateful packet filtering firewall is more complicated compared to the Packet filtering firewall, since the latter is stateless.
C: Dual-homed is a firewall architecture, not a firewall type.
A Dual-homed firewall refers to a device that has two interfaces: one facing the external network and the other facing the internal network.
D: Application -level gateways are known as second generation firewalls, while packet filtering is a first generation firewall

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 348
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?

A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)

D. Wan switch

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
An electronic multiplexer makes it possible for several signals to share one device or resource. A multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line.

Incorrect Answers:
A: A router forwards data packets. A router does not handle signals.
C: A CSU/DSU is a digital-interface device used to connect a data terminal equipment (DTE), such as a router, to a digital circuit, such as a Digital Signal 1 (T1) line.
D: A switch forwards traffic at the data link layer of the OSI model. It does operate with multiple signals.

References:
https://en.wikipedia.org/wiki/Multiplexer

QUESTION 349
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized

Correct Answer: A

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Event logging is available in both TACACS and TACACS+.

Incorrect Answers:
B: TACACS+ is XTACACS with extended two-factor user authentication.
C: TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection.
D: TACACS+ features security tokes, which is not included in TACACS.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 234

QUESTION 350
Which of the following remote access authentication systems is the MOST robust?

A. TACACS+
B. RADIUS
C. PAP
D. TACACS

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
TACACS+ is more secure compared to TACACS, RADIUS, and PAP.

Incorrect Answers:
B: TACACS+ encrypts all of this data between the client and server and thus does not have the vulnerabilities inherent in the RADIUS protocol.
C: PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure.
D: TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection. TACACS+ is XTACACS with extended two-factor user authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 234

QUESTION 351
Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?

A. LLC and MAC; IEEE 802.2 and 802.3
B. LLC and MAC; IEEE 802.1 and 802.3
C. Network and MAC; IEEE 802.1 and 802.3
D. LLC and MAC; IEEE 802.2 and 802.3

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:

QUESTION 352
Which of the following protects Kerberos against replay attacks?

A. Tokens
B. Passwords
C. Cryptography
D. Time stamps

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
To protect against replay attacks, the Kerberos authentication protocol uses the concept of an authenticator. The authenticator includes the user identification information, a sequence number, and a timestamp. The timestamp is used to help fight against replay attacks.

Incorrect Answers:
A: Kerberos uses time stamps, not tokens, to defend against replay attacks.
B: Kerberos uses time stamps, not passwords, to defend against replay attacks.
C: Kerberos uses time stamps, not cryptography, to defend against replay attacks.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 212

QUESTION 353
Which of the following offers security to wireless communications?

A. S-WAP
B. WTLS
C. WSP D. WDP

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Wireless Transport Layer Security (WTLS) provides security connectivity services similar to those of SSL or TLS.

Incorrect Answers:
A: There is no protocol named S-WAP
C: Wireless Session Protocol (WSP) does not provide security.
D: Wireless Datagram Protocol (WDP) does not provide security.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 103

QUESTION 354
Which of the following is a Wide Area Network that was originally funded by the Department of Defense, which uses TCP/IP for data interchange?

A. The Internet.
B. The Intranet.
C. The extranet.
D. The Ethernet.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:

Explanation:
The Advanced Research Projects Agency Network (ARPANET), funded by the Department of Defense, was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

Incorrect Answers:
B: Intranets can use other protocols than TCP/IP. Intranet is not standard that was developed by the Department of Defense.
C: Intranet can use other protocols than TCP/IP. Extranet is not standard that was developed by the Department of Defense.
D: Ethernet can use other protocols than TCP/IP. Ethernet is not standard that was developed by the Department of Defense.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 549

QUESTION 355
An intranet is an Internet-like logical network that uses:

A. a firm's internal, physical network infrastructure.
B. a firm's external, physical network infrastructure.
C. a firm's external, physical netBIOS infrastructure.
D. a firm's internal, physical netBIOS infrastructure.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
When a company uses web-based technologies inside its networks, it is using an intranet, a private network. The company's internal physical network structure is used.

Incorrect Answers:
B: The internal, not the external, network structure is used.
C: The internal, not the external, network structure is used.
D: The physical structure, not the NetBIOS structure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 661

QUESTION 356
An intranet provides more security and control than which of the following:

A. private posting on the Internet. B.
public posting on the Ethernet.
C. public posting on the Internet.
D. public posting on the Extranet.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A public posting on the internet is not secure. Compared to the internet, an intranet provides more control.

Incorrect Answers:
A: A private posting provides high security and control.
B: Ethernet is a link layer protocol in the TCP/IP stack. An Intranet is defined on the physical layer. The data link layer provides more control compared to the physical layer.
D: An extranet is a website that allows controlled access to partners, vendors and suppliers or an authorized set of customers - normally to a subset of the information accessible from an organization's intranet. As an extranet is a subset of an intranet is provides more security and control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 661

QUESTION 357
Which of the following Common Data Network Services is used to share data files and subdirectories on file servers?

A. File services.
B. Mail services.
C. Print services.
D. Client/Server services.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Files services, which are part of the Common Data Network Services, provides sharing of data files and subdirectories on file servers.

Incorrect Answers:
B: Mail services only provide sending and receiving email internally or externally through an email gateway device.
C: Print services only provide printing documents to a shared printer or a print queue/spooler.
D: Client/server services provide allocating computing power resources among workstations with some shared resources centralized in a file server.

References:
The CISSP and CAP Prep Guide: Mastering CISSP and CA (2007), page 138

QUESTION 358
Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?

A. File services.
B. Mail services.
C. Print services.
D. Client/Server services.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Mail services, which are part of the Common Data Network Services, sends and receives email internally or externally through an email gateway device.

Incorrect Answers:
A: Files services provide sharing of data files and subdirectories on file servers.
C: Print services only prints documents to a shared printer or a print queue/spooler.
D: Client/server services allocate computing power resources among workstations with some shared resources centralized in a file server.

QUESTION 359
Asynchronous Communication transfers data by sending:

A. bits of data sequentially
B. bits of data sequentially in irregular timing patterns
C. bits of data in sync with a heartbeat or clock
D. bits of data simultaneously

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Asynchronous communication is the transmission sequencing technology that uses start and stop bits or similar encoding mechanism. Used in environments that transmits a variable amount of data in a periodic fashion.

Incorrect Answers:
A: Both asynchronous and synchronous communication sends bits of data sequentially.
C: Data bits transferred in sync with a heartbeat or clock is called synchronous communication.
D: Asynchronous Communication transfers one bit at a time, not multiple bits of data simultaneously.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 566

QUESTION 360
Communications devices must operate:

A. at different speeds to communicate. B.
at the same speed to communicate.
C. at varying speeds to interact.
D. at high speed to interact.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
It is preferable that both devices have the same speed when they are going to interoperate.

Incorrect Answers:
A: It is preferable that the devices have the same speed to interoperate well.
C: Communication is easier if the speeds of the devices do not change.
D: High speed is not a necessity for devices to be able to interact.

QUESTION 361
The basic language of modems and dial-up remote access systems is:

A. Asynchronous Communication.
B. Synchronous Communication.
C. Asynchronous Interaction.
D. Synchronous Interaction.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Asynchronous start-stop is the physical layer used to connect computers to modems for many dial-up Internet access applications, using a data link framing protocol.

Incorrect Answers:
B: Dial-up modems use Asynchronous, not synchronous, communication.
C: Dial-up modems connect to a remote system using communication, not interaction.
D: Dial-up modems connect to a remote system using communication, not interaction.

References:
https://en.wikipedia.org/wiki/Asynchronous_serial_communication

QUESTION 362
Which of the following Common Data Network Services is used to print documents to a shared printer or a print queue/spooler?

A. Mail services.
B. Print services.
C. Client/Server services.
D. Domain Name Service.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Print services, which are part of the Common Data Network Services, prints documents to a shared printer or a print queue/spooler.

Incorrect Answers:
A: Mail services only send and receive email internally or externally through an email gateway device.
C: Client/server services allocate computing power resources among workstations with some shared resources centralized in a file server.
D: Domain Name Service translates domain names into IP addresses.

QUESTION 363
Which of the following Common Data Network Services allocates computing power resources among workstations with some shared resources centralized on a server?

A. Print services
B. File services
C. Client/Server services
D. Domain Name Service

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Client/server services, which belongs to the Common Data Network Services, allocates computing power resources among workstations with some shared resources centralized in a file server.

Incorrect Answers:
A: Print services only print documents to a shared printer or a print queue/spooler.
B: Files services provide sharing of data files and subdirectories on file servers.
D: Domain Name Service translates domain names into IP addresses.

QUESTION 364
Domain Name Service is a distributed database system that is used to map:

A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.
D. IP addresses to MAC Addresses.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Domain Name Service translates domain names into IP addresses.

Incorrect Answers:
B: DNS is not used to map MAC addresses to domain names. DNS maps domain names into IP addresses.
C: The RARP protocol translates MAC Address to IP addresses.
D: The ARP protocol translates IP addresses to MAC Addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 365
The Domain Name System (DNS) is a global network of:
A. servers that provide these Domain Name Services.
B. clients that provide these Domain Name Services.
C. hosts that provide these Domain Name Services.
D. workstations that provide these Domain Name Services.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The Domain Name System is lists of domain names and IP addresses that are distributed on Domain Name System (DNS) Servers throughout the Internet in a hierarchy of authority.

Incorrect Answers:
B: The global Domain Name System (DNS) system consists of DNS servers, not DNS clients.
C: The global Domain Name System (DNS) system consists of DNS servers, not DNS hosts.
D: The global Domain Name System (DNS) system consists of DNS servers, not DNS workstations.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 591

QUESTION 366
The communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together refers to:

A. Netware Architecture.
B. Network Architecture.
C. WAN Architecture.
D. Multiprotocol Architecture.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network architecture is the design of a communication network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, including protocols and access methods, as well as data formats used in its operation.
Incorrect Answers:
A: Novell Netware is specific to the vendor Novell.
C: WAN Architecture is not used for the various components of a network. It used for components that enables different local network to communicate with other networks.
D: The physical components must be included as well, not just the protocols.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 246

QUESTION 367
Unshielded Twisted Pair cabling is a:

A. four-pair wire medium that is used in a variety of networks.
B. three-pair wire medium that is used in a variety of networks.
C. two-pair wire medium that is used in a variety of networks.
D. one-pair wire medium that is used in a variety of networks.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Unshielded Twisted Pair cabling consists of an outer jacket and four pairs of twisted wire medium.

Incorrect Answers:
B: There are four pairs, not three.
C: There are four pairs, not two.
D: There are four pairs, not one.

References:
https://en.wikipedia.org/wiki/Twisted_pair#Unshielded_twisted_pair_.28UTP.29

QUESTION 368
In the UTP category rating, the tighter the wind:

A. the higher the rating and its resistance against interference and crosstalk.
B. the slower the rating and its resistance against interference and attenuation.
C. the shorter the rating and its resistance against interference and attenuation.
D. the longer the rating and its resistance against interference and attenuation.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
With Increased UTP category the better the signal is transmitted, that is the cable is more resistance against interference and crosstalk.
The lowest category is 1 and the highest is 8.2.

Incorrect Answers:
B: The UTP categories are just numbers from 1 to 8.2. They do not represent speed.
C: The UTP categories are just numbers. They do not represent length.
D: The UTP categories are just numbers. They do not represent speed.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 559

QUESTION 369
What works as an E-mail message transfer agent?

A. SMTP
B. SNMP
C. S-RPC
D. S/MIME

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.

Incorrect Answers:
B: SNMP is used for monitoring the network, not for sending email messages.
C: S-RPC is used for remote procedure not calls, and not for sending email messages.
D: S/MIME is a standard for email encryption. It is not used to send email messages.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 370
Which of the following statements pertaining to packet switching is NOT true?

A. Most data sent today uses digital signals over network employing packet switching.
B. Messages are divided into packets.
C. All packets from a message travel through the same route.
D. Each network node or point examines each packet for routing.

Correct Answer: C

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet switching does not set up a dedicated virtual link, and packets from one connection can pass through a number of different individual devices, instead of all of them following one another through the same devices.

Incorrect Answers:
A: Most traffic over the Internet uses packet switching and the Internet is basically a connectionless network.
B: In a packet-switching network, the data are broken up into packets containing frame check sequence numbers.
D: The packet switching packets go through different network nodes, and their paths can be dynamically altered by a router or switch that determines a better route for a specific packet to take.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 674

QUESTION 371
All hosts on an IP network have a logical ID called a(n):

A. IP address.

B. MAC address.
C. TCP address.
D. Datagram address.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Each node on an IP network must have a unique IP address.

Incorrect Answers:
B: IP hosts use IP addresses, not MAC addresses.
C: There is no such thing as a TCP address in the TCP/IP model.
D: There is no such thing as a datagram address in the TCP/IP model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 541

QUESTION 372
An Ethernet address is composed of how many bits?

A. 48-bit address B.
32-bit address.
C. 64-bit address
D. 128-bit address

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Ethernet is a common LAN media access technology standardized by IEEE 802.3. Ethernet uses 48-bit MAC addressing, works in contention-based networks, and has extended outside of just LAN environments.

Incorrect Answers:
B: An Ethernet address has 48 bits, not 32 bits.
C: An Ethernet address has 48 bits, not 64 bits.
D: An Ethernet address has 48 bits, not 128 bits.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 578

QUESTION 373
Address Resolution Protocol (ARP) interrogates the network by sending out a?

A. broadcast.
B. multicast.
C. unicast.
D. semicast.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it. The computer that has the destination IP address responds with its MAC address.

Incorrect Answers:
B: The ARP protocol uses broadcasts, not multicasts.
C: The ARP protocol uses broadcasts, not unicast.
D: The ARP protocol uses broadcasts, not semicast.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 581

QUESTION 374
When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The RARP protocol translates MAC (Ethernet) Address to IP addresses.

Incorrect Answers:
A: The ARP protocol translates IP addresses to MAC Addresses. It is the wrong direction.
C: ICMP is not an address resolution protocol.
D: UDP is not an address resolution protocol. It is a transport protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 584

QUESTION 375

Which protocol's primary function is to facilitate file and directory transfer between two machines?

A. Telnet.
B. File Transfer Protocol (FTP).
C. Trivial File Transfer Protocol (TFTP).
D. Simple Mail Transfer Protocol (SMTP)

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
FTP is a network application that supports an exchange of files between computers, and that requires anonymous or specific authentication.

Incorrect Answers:
A: Through Telnet users can access someone else's computer remotely.
C: TFTP is less capable compared to FTP. TFTP is used where user authentication and directory visibility are not required.
D: SMTP is used only for sending email messages.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 125

QUESTION 376
What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP
B. Due to the inherent security risks
C. It does not offer high level encryption like FTP
D. It cannot support the Lightweight Directory Access Protocol (LDAP)

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

TFTP is a network application that supports an exchange of fi les that does not require authentication. TFTP is not secure.

Incorrect Answers:
A: FTP is too insure, not too complex.
C: The difference between FTP and TFTP is that TFTP does not offer authentication.
D: Both FTP and TFTP support LDAP.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1276

QUESTION 377
Which protocol is used to send email?

A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.
Incorrect Answers:
A: FTP is a network application that supports an exchange of files between computers.
B: The Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve, not to send, e-mail from a remote server over a TCP/IP connection.
C: The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update file on a remote computer as though they were on the user's own computer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 378
Which of the following best describes the Secure Electronic Transaction (SET) protocol?

A. Originated by VISA and MasterCard as an Internet credit card protocol using Message Authentication Code.
B. Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
C. Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
D. Originated by VISA and American Express as an Internet credit card protocol using SSL.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. With SET an entity verifies a digital signature of the sender and digitally signs the information before it is sent to the next entity involved in the process.

Incorrect Answers:
A: SET uses digital signatures, not Message Authentication Codes.
C: SET uses digital signatures, not transport layer security.
D: Visa and Mastercard, not American Express, has proposed the SET protocol. The current security solution in use for credit cards transfers use SSL, but SET uses digital signatures.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 857

QUESTION 379
Which of the following protocols is designed to send individual messages securely?

A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:

S-HTTP provides protection for each message sent between two computers, but not the actual link.

Incorrect Answers:
A: Kerberos is a network authentication protocol. It is not used to secure messages.
B: SET is designed to provide secure credit card transactions, not to provide secure transfer of messages.
C: HTTPS protects the communication channel, not each individual message separately. HTTPS is HTTP that uses SSL for security purposes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 873

QUESTION 380
Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

A. Application Layer.
B. Transport Layer.
C. Session Layer.
D. Network Layer.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Both SET and S-HTTP provides application layer security.

Incorrect Answers:
B: SET and S-HTTP work at the application layer, not at the transportation layer.
C: SET and S-HTTP work at the session layer, not at the transportation layer.
D: SET and S-HTTP work at the network layer, not at the transportation layer.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 856

QUESTION 381
Why does fiber optic communication technology have significant security advantage over other transmission technology?

A. Higher data rates can be transmitted.
B. Interception of data traffic is more difficult.

C. Traffic analysis is prevented by multiplexing.
D. Single and double-bit errors are correctable.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Because fiber-optic cable passes electrically non-conducting photons through a glass medium, it is very hard to intercept or wiretap.

Incorrect Answers:
A: High data rates are an advantage of fiber options, but speed in itself does not significantly increase speed.
C: Multiplexing would not prevent traffic analysis. It would just make it harder.
D: Correctable bits are not an advantage of fiber optic communication.

QUESTION 382
Which of the following statements pertaining to IPSec is NOT true?

A. IPSec can help in protecting networks from some of the IP network attacks.
B. IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.
C. IPSec protects against man-in-the-middle attacks.
D. IPSec protects against spoofing.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec works at the network layer, not at the transport layer.

Incorrect Answers:
A: IPSec protects networks by authenticating and encrypting each IP packet of a communication session.
C: IPSec protects against man-in-the-middle attacks by combining mutual authentication with shared, cryptography-based keys.
D: IPSec uses cryptography-based keys, shared only by the sending and receiving computers, to create a cryptographic checksum for each IP packet. The cryptographic checksum ensures that only the computers that have knowledge of the keys could have sent each packet. This products against spoofing.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1360

QUESTION 383
Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?

A. The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network. B. They don't protect against IP or DNS address spoofing.
C. They do not support strong user authentication.
D. They are appropriate for medium-risk environment.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering was the first generation of firewalls and it is the most rudimentary type of all of the firewall technologies. Packet filtering gateways/firewalls would be insufficient for a medium-risk environment.

Incorrect Answers:
A: Packet filtering gateways can make access decisions based upon the following basic criteria: ▪
Source and destination IP addresses
▪ Source and destination port numbers
▪ Protocol types
▪ Inbound and outbound traffic direction
B: Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa). On the other hand packet filtering gateways would not be able to protect against DNS spoofing. A stateful firewall is needed to protect against DNS spoofing C: Packet filter gateways cannot ensure strong user authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 384
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

A. Screened subnets
B. Digital certificates
C. An encrypted Virtual Private Network

D. Encryption

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A virtual private network (VPN) is a secure, private connection through an untrusted Network. It is a private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit.

Incorrect Answers:
A: The main purpose of a screened subnet it to set up a demilitarized zone, not to protect connections over an insecure network.
B: A digital certificate provides identifying information. It is not used to protect connections over an insecure network.
D: Encryption can be used to protect connections over an insecure network, but it cannot protect the integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 701

QUESTION 385
Which of the following protocols does not operate at the data link layer (layer 2)?

A. PPP
B. RARP
C. L2F
D. ICMP

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
ICMP works at the network layer of the OSI model.

Incorrect Answers:
A: RARP is a data link layer protocol.
B: L2F is a data link layer protocol.
C: ICMP is a data link layer protocol.

References:
https://en.wikipedia.org/wiki/Network_layer

QUESTION 386
Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LPD
D. SPX

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Remote procedure call (RPC) works at the session layer of the OSI model.

Incorrect Answers:
B: ICMP works at the network layer of the OSI model.
C: LPD (Line Printer Daemon Protocol) is an application layer protocol.
D: SPX is a transport layer protocol.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 524

QUESTION 387
Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The network layer of the OSI model corresponds to the Internet layer of the TCP/IP model.

Incorrect Answers:
A: The host-to-host layer of the TCP/IP model corresponds to the Transport layer of the OSI model.
C: The host-to-host layer of the TCP/IP model corresponds to the Data link layer of the OSI model.
D: The TCP/IP model does not have any session layer.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 518

QUESTION 388
Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?

A. Physical
B. Data link
C. Network
D. Session

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The data link layer is responsible for proper communication within the network components and for changing the data into the necessary format (electrical voltage) for the physical layer. It is concerned with local delivery of frames between devices on the same LAN.

Incorrect Answers:
A: The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes.
C: The session layer protocols set up connections between applications; maintain dialog control; and negotiate, establish, maintain, and tear down the communication channel.
D: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 389
The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer.
B. The Reference monitor.
C. The Transport layer of the TCP/IP stack model.
D. Change management control.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
The ISO/OSI data link layer is divided into two functional sublayers: the Logical Link Control (LLC) and the Media Access Control (MAC).

Incorrect Answers:
B: Logical Link Control is a sublayer of the Data link layer, and not part of the Reference monitor.
C: Logical Link Control is a sublayer of the Data link layer, and not part of the Transport layer.
D: Logical Link Control is a sublayer of the Data link layer, and not part of the Change management control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 528

QUESTION 390
Which of the following services relies on UDP?

A. FTP
B. Telnet

C. DNS
D. SMTP

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
DNS primarily uses User Datagram Protocol (UDP) on port number 53 to serve requests. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.

Incorrect Answers:
A: FTP uses the TCP protocol.
B: Telnet uses the TCP protocol.
C: SMTP uses the TCP protocol.

References:
https://en.wikipedia.org/wiki/Domain_Name_System

QUESTION 391
Which of the following is NOT a common weakness of packet filtering firewalls?

A. Vulnerability to denial-of-service and related attacks.
B. Vulnerability to IP spoofing.
C. Limited logging functionality.
D. No support for advanced user authentication schemes.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).

Incorrect Answers:

A: Packet filtering firewalls, as they are stateless, are vulnerable to denial-of-service attacks. A stateful firewall would be able to handle these attacks better.
C: Logging is no problem when using packet filtering firewalls.
D: Packet filter gateways cannot ensure strong user authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 630

QUESTION 392
Which Network Address Translation (NAT) is the MOST convenient and secure solution?

A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Port Address Translation (PAT) maps one internal IP address to an external IP address and port number combination. Thus, PAT can theoretically support 65,536 (2 16) simultaneous communications from internal clients over a single external leased IP address. A company can save a lot of money by using PAT, because the company needs to buy only a few public IP addresses, which are used by all systems in the network.

Incorrect Answers:
A: NAT maps one internal IP address to one external IP address. Compared to PAT this is pretty bad.
C: There is no NAT implementation called Dedicated Address Translation.
D: Static Address Translation is not convenient as it must be configured manually.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 393
What is the primary difference between FTP and TFTP?

A. Speed of negotiation
B. Authentication
C. Ability to automate

D. TFTP is used to transfer configuration files to and from network equipment.

Correct Answer: B

Section: Communication and Network Security

Explanation

Explanation/Reference:

Explanation:

TFTP is less capable compared to FTP. TFTP is used where user authentication and directory visibility are not required.

Incorrect Answers:

A: Both FTP and TFTP have ability to negotiate speedC:

There is ability to automate both FTP and TFTP.

D: TFTP can be used to transfer any files, not just configuration files between network equipment.

References:

Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 125

QUESTION 394

Which of the following cable types is limited in length to 185 meters?

A. 10BaseT

B. RG8

C. RG58

D. 10Base5

Correct Answer: C

Section: Communication and Network Security

Explanation

Explanation/Reference:

Explanation:

RG-58 was once widely used in "thin" Ethernet (10BASE2), where it provides a maximum segment length of 185 meters.

Incorrect Answers:

A: 10BaseT has a maximal distance of 100 meters.

B: RG-8 has a maximal distance of 500 meters.

D: 10Base5 has a maximal distance of 500 meters.

References:
https://en.wikipedia.org/wiki/RG-58

QUESTION 395
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
HTTP Secure (HTTPS) is HTTP running over SSL. The client browser generates a session key and encrypts it with the server's public key.

Incorrect Answers:
A: Only the client generates the key.
C: The client, not the server, generates the key.
D: The client, not a certification server, generates the key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 855

QUESTION 396
Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is NOT true?

A. PPTP allows the tunneling of any protocols that can be carried within PPP.
B. PPTP does not provide strong encryption.
C. PPTP does not support any token-based authentication method for users.
D. PPTP is derived from L2TP.

Correct Answer: D

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server. While PPTP depends on IP to establish its connection. As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks.
PPTP does have some limitations: It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users. L2TP is derived from L2F and PPTP, not the opposite.

Incorrect Answers:
A: PPTP relies on the Point-to-Point Protocol (PPP) being tunneled to implement security functionality.
B: PPTP uses PPP for encryption. The PPP protocol has only the capability to encrypt data with 128-bit so it ensures low security.
C: The PPTP specification does not include authentication. In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, MSCHAP v1/v2 , but not with any token-based authentication scheme.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 708

QUESTION 397
During the initial stage of configuration of your firewall, which of the following rules appearing in an Internet firewall policy is inappropriate?

A. The firewall software shall run on a dedicated computer.
B. Appropriate firewall documentation and a copy of the rulebase shall be maintained on offline storage at all times.
C. The firewall shall be configured to deny all services not expressly permitted.
D. The firewall should be tested online first to validate proper configuration.

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
For security reasons, the firewall should be tested offline.

Incorrect Answers:

A: A firewall may take the form of either software installed on a regular computer using a regular operating system or a dedicated hardware appliance that has its own operating system. The second choice is usually more secure.
B: It is important to make a backup of the configuration of the firewall.
C: All unneeded ports should be closed, and all unneeded services should be denied.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 643

QUESTION 398
SMTP can best be described as:

A. a host-to-host email protocol.
B. an email retrieval protocol.
C. a web-based e-mail reading protocol.
D. a standard defining the format of e-mail messages.

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In e-mail clients SMTP works as a message transfer agent and moves the message from the user's computer to the mail server when the user sends the e-mail message.

Incorrect Answers:
B: SMTP is used only for sending, not retrieving, email messages.
C: SMTP is used only for sending, not reading, email messages.
D: SMTP is not a format of email messages. It is a protocol for sending email messages.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 599

QUESTION 399
Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

A. SSL
B. FTP

C. SSH
D. S/MIME

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
SSL is primarily used to protect HTTP traffic. SSL capabilities are already embedded into most web browsers.
Incorrect Answers:
B: FTP is used to transfer files, not to secure data that are transferred.
C: S/MIME is not to protect data sent in web applications. S/MIME, more specifically, is used to secure email messages.
D: SSH is not used in a web based application. SSH allows remote login and other network services to operate securely over an unsecured network.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 846

QUESTION 400
What attack involves the perpetrator sending spoofed packet(s) which contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

A. Boink attack
B. Land attack
C. Teardrop attack
D. Smurf attack

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
A land (Local Area Network Denial) attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. This causes the machine to reply to itself continuously.

Incorrect Answers:

A: The Boink attack manipulates a field in TCP/IP packets, called a fragment offset. This field tells a computer how to reconstruct a packet that was broken up (fragmented) because it was too big to transmit in a whole piece. By manipulating this number, the Boink attack causes the target machine to reassemble a packet that is much too big to be reassembled. This causes the target computer to crash.
C: A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine.
D: The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 257

QUESTION 401
If an organization were to deploy only one Intrusion Detection System (IDS) sensor to protect its information system from the Internet:
A. It should be host-based and installed on the most critical system in the DMZ, between the external router and the firewall.
B. It should be network-based and installed in the DMZ, between the external router and the firewall.
C. It should be network-based and installed between the firewall to the DMZ and the intranet.
D. It should be host-based and installed between the external router and the Internet.

Correct Answer: B
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Network Intrusion Detection Systems (NIDS) are placed at a strategic point, such as between the internet-facing router and the firewall, within the network to monitor traffic to and from all devices on the network.

Incorrect Answers:
A: A host-based IDS is an IDS that is installed on a single computer and can monitor the activities on that computer only.
C: It is better to place the IDS between the DMZ and the internet.
D: A host-based IDS is an IDS that is installed on a single computer and can monitor the activities on that computer only.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 402
Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?

A. Because infrared eavesdropping requires more sophisticated equipment.
B. Because infrared operates only over short distances.

C. Because infrared requires direct line-of-sight paths.
D. Because infrared operates at extra-low frequencies (ELF).

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Infrared communications require line-of-sight transmission. This makes infrared relative secure from electronic eavesdropping.

Incorrect Answers:
A: Infrared eavesdropping does not require more advanced transmissions.
B: Infrared operates over short distances, but this is not the main reason it is hard to eavesdrop. Compared to multidirectional radio transmission a direct line of sight is necessary.
D: Infrared operates at high frequencies around 430 THz.

QUESTION 403
Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:

A. Authentication
B. Integrity
C. Replay resistance and non-repudiations
D. Confidentiality

Correct Answer: D
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Integrity and authentication for IP datagrams are provided by AH, but AH does not provide Confidentiality.

Incorrect Answers:
A: Authentication is provided by AH.
B: Integrity is provided by AH.
C: Authentication Headers (AH) might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. With nonrepudiations comes replay resistance.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 862

QUESTION 404
In IPSec, if the communication is to be gateway-to-gateway or host-to-gateway:

A. Tunnel mode of operation is required
B. Only transport mode can be used
C. Encapsulating Security Payload (ESP) authentication must be used
D. Both tunnel and transport mode can be used

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
In IPSec tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications.

Incorrect Answers:
B: Tunnel mode, not transport mode, must be used.
C: Tunnel mode, not ESP authentication, must be used.
D: Only tunnel mode can be used.

References:
https://en.wikipedia.org/wiki/IPsec#Tunnel_mode

QUESTION 405
Which of the following is NOT true about IPSec Tunnel mode?

A. Fundamentally an IP tunnel with encryption and authentication
B. Works at the Transport layer of the OSI model
C. Have two sets of IP headers
D. Established for gateway service

Correct Answer: B

Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
IPSec Tunnel mode works at the Internet layer, not at the Transport layer.

Incorrect Answers:
A: In IPSec tunnel mode, the entire IP packet is encrypted and/or authenticated.
C: In tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. That is, in tunnel mode, there are two sets of IP headers.
D: Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access or for gateway services) and host-to-host communications.

References:
https://en.wikipedia.org/wiki/IPsec#Tunnel_mode

QUESTION 406
Which of the following statements is NOT true of IPSec Transport mode?

A. It is required for gateways providing access to internal systems
B. Set-up when end-point is host or communications terminates at end-points
C. If used in gateway-to-host communication, gateway must act as host
D. When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet

Correct Answer: A
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Tunnel mode, not transport mode, is required for gateway services.

Incorrect Answers:
B: Transport mode is allowed between two end hosts only.
C: As Transport mode only is allowed between two end hosts, the gateway must act as a host.
D: ESP operates directly on top of IP. The encryption is only applied to the upper layer protocols contained in the packet.

References:

https://tools.ietf.org/html/rfc3884

QUESTION 407
Which of the following statements pertaining to firewalls is NOT true?

A. Firewalls create bottlenecks between the internal and external network.
B. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C. Firewalls protect a network at all layers of the OSI models.
D. Firewalls are used to create security checkpoints at the boundaries of private networks.

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Packet filtering firewalls work at the network level of the OSI model.
If you filter specific ports, you can say you're filtering at layer 4.
If your firewall inspects specific protocol states or data, you can say it operates at layer 7.
Firewalls do not work at layer 1, layer 2, or layer 3 of the OSI model.

Incorrect Answers:
A: Firewalls can create bottlenecks between the internal and external network.
B: Firewalls can be administered from a central location.
D: Firewall are most often placed at the boundaries of the private networks to implement a security checkpoint to restrict access from the Internet.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 628

QUESTION 408
Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?

A. IP Spoofing
B. IP subnetting
C. Port address translation
D. IP Distribution

Correct Answer: C
Section: Communication and Network Security
Explanation

Explanation/Reference:
Explanation:
Port address translation (PAT) is an implementation of Network Address Translation. PAT is a mechanism for converting the internal private IP addresses found in packet headers into public IP addresses and port numbers for transmission over the Internet. PAT supports a many-to-one mapping of internal to external IP addresses by using ports.

Incorrect Answers:
A: IP Spoofing does not involve mapping of IP addresses. IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system B: IP subnetting is the practice of dividing a network into two or more networks. D: The distribution of IP addresses does not involve mapping of IP addresses.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 606

QUESTION 409
Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is TRUE?

A. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Controls can be administrative, logical or technical, and physical.
- Administrative controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

- Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists, and transmission protocols.
- Physical controls incorporate guards and building security in general, such as the locking of doors, securing of server rooms or laptops, the protection of cables, the separation of duties, and the backing up of files.

Incorrect Answers:
A: The controls listed in this answer are all administrative controls (including a review of vacation history).
B: Technical controls DO include encryption, smart cards, access lists, and transmission protocols.
D: The controls listed in this answer are all administrative controls.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 47

QUESTION 410
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

A. through access control mechanisms that require identification and authentication and through the audit function.
B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Incorrect Answers:
B: This answer does not describe how accountability is accomplished.
C: This answer does not describe how accountability is accomplished.
D: This answer does not describe how accountability is accomplished.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 47

QUESTION 411

In the Bell-LaPadula model, the *-property (Star-property) is also called:

A. The simple security property
B. The confidentiality property
C. The confinement property
D. The tranquility property

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The *-property ("star"-property) states that a subject in a specified security level cannot write information to a lower security level. This property is also known as the Confinement property.

Incorrect Answers:
A: The simple security property is only known as the simple security property.
B: The *-property ("star"-property) is also known as the Confinement property, not the confidentiality property.
D: The *-property ("star"-property) is also known as the Confinement property, not the tranquility property.
References:
http://cse.yeditepe.edu.tr/~odemir/fall2010/cse439/lecture11.pdf
http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control
http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model http://en.wikipedia.org/wiki/Brewer_and_Nash_model

QUESTION 412
In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

A. The society's role in the organization
B. The individual's role in the organization
C. The group-dynamics as they relate to the individual's role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization

Correct Answer: B

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
With Non-Discretionary Access Control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization (role-based access control) or the subject's responsibilities and duties (task-based access control). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual's role or title within the organization. These access controls do not need to be changed whenever a new person takes over that role.

Incorrect Answers:
A: In RBAC, the access controls are based on the individual's role in the organization, not the society's role in the organization.
C: In RBAC, the access controls are based on the individual's role in the organization, not the group-dynamics as they relate to the individual's role in the organization.
D: In RBAC, the access controls are based on the individual's role in the organization, not the group-dynamics as they relate to the master-slave role in the organization.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 48

QUESTION 413
In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

A. people need not use discretion
B. the access controls are based on the individual's role or title within the organization.
C. the access controls are not based on the individual's role or title within the organization
D. the access controls are often based on the individual's role or title within the organization

Correct Answer: B

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
With Non-Discretionary Access Control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization (role-based access control) or the subject's responsibilities and duties (task-based access control). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual's role or title within the organization. These access controls do not need to be changed whenever a new person takes over that role.

Incorrect Answers:
A: People not needing to use discretion is not the reason RBAC is useful in an organization where there are frequent personnel changes.
C: With RBAC, the access controls ARE based on the individual's role or title within the organization.
D: With RBAC, the access controls are ALWAYS based on the individual's role or title within the organization.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 48
http://csrc.nist.gov/groups/SNS/rbac/

QUESTION 414
Which of the following are additional access control objectives?

A. Consistency and utility
B. Reliability and utility
C. Usefulness and utility
D. Convenience and utility

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity, and availability. Confidentiality assures that the information is not disclosed to unauthorized persons or processes. Integrity ensures the consistency of data. Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility.

Incorrect Answers:
A: Consistency is not one of the defined additional access control objectives.

C: Usefulness is not one of the defined additional access control objectives.
D: Convenience is not one of the defined additional access control objectives.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 46

QUESTION 415
Which of the following access control techniques BEST gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

A. Access control lists
B. Discretionary access control
C. Role-based access control
D. Non-mandatory access control

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Role-based access control (RBAC) is a model where access to resources is determines by job role rather than by user account.
Hierarchical RBAC allows the administrator to set up an organizational RBAC model that maps to the organizational structures and functional delineations required in a specific environment. This is very useful since businesses are already set up in a personnel hierarchical structure. In most cases, the higher you are in the chain of command, the more access you will most likely have.
Role relation defines user membership and privilege inheritance. For example, the nurse role can access a certain amount of files, and the lab technician role can access another set of files. The doctor role inherits the permissions and access rights of these two roles and has more elevated rights already assigned to the doctor role. So hierarchical is an accumulation of rights and permissions of other roles.
Reflects organizational structures and functional delineations.

Incorrect Answers:
A: Access control lists form the basis of access control; they determine who can access what. However, “access control lists” on its own is not a model that maps to the organizational structures and functional delineations required in a specific environment.
B: Discretionary access control is a model where the subjects must have the discretion to specify what resources certain users are permitted to access. This is not a model that maps to the organizational structures and functional delineations required in a specific environment.
D: Non-mandatory access control is not a defined access control model. It would imply any access model that is not mandatory access control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 224-226

QUESTION 416
Which access control model was proposed for enforcing access control in government and military applications?

A. Bell-LaPadula model
B. Biba model
C. Sutherland model
D. Brewer-Nash model

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The Bell–LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

Incorrect Answers:
B: The Biba Model describes a set of access control rules designed to ensure data integrity. It is not used for enforcing access control in government and military applications.
C: The Sutherland model is an information flow model. It is not used for enforcing access control in government and military applications.
D: The Brewer and Nash Model deals with conflict of interest. It is not used for enforcing access control in government and military applications.

References:
https://en.wikipedia.org/wiki/Bell–LaPadula_model

QUESTION 417
Which access control model achieves data integrity through well-formed transactions and separation of duties?

A. Clark-Wilson model
B. Biba model
C. Non-interference model
D. Sutherland model

Correct Answer: A

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The Clark-Wilson model enforces the three goals of integrity by using access triple (subject, software [TP], object), separation of duties, and auditing. This model enforces integrity by using well-formed transactions (through access triple) and separation of duties.
When an application uses the Clark-Wilson model, it separates data into one subset that needs to be highly protected, which is referred to as a constrained data item (CDI), and another subset that does not require a high level of protection, which is called an unconstrained data item (UDI). Users cannot modify critical data (CDI) directly. Instead, the subject (user) must be authenticated to a piece of software, and the software procedures (TPs) will carry out the operations on behalf of the user. For example, when Kathy needs to update information held within her company's database, she will not be allowed to do so without a piece of software controlling these activities. First, Kathy must authenticate to a program, which is acting as a front end for the database, and then the program will control what Kathy can and cannot do to the information in the database.
This is referred to as access triple: subject (user), program (TP), and object (CDI). A user cannot modify CDI without using a TP.
The Clark-Wilson security model uses division of operations into different parts and requires different users to perform each part. This is known as Separation of Duties.
The Clark-Wilson model outlines how to incorporate separation of duties into the architecture of an application. If a customer needs to withdraw over $10,000, the application may require a supervisor to log in and authenticate this transaction. This is a countermeasure against potential fraudulent activities. The model provides the rules that the developers must follow to properly implement and enforce separation of duties through software procedures.

Incorrect Answers:
B: The Biba Model describes a set of access control rules designed to ensure data integrity. However, it does not achieve data integrity through well-formed transactions and separation of duties.
C: The Non-interference model is not an integrity model.
D: The Sutherland model is not an integrity model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 370-377

QUESTION 418
Which of the following statements pertaining to access control is FALSE?
A. Users should only access data on a need-to-know basis.
B. If access is not explicitly denied, it should be implicitly allowed.
C. Access rights should be granted based on the level of trust a company has on a subject.
D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
This answer is false as access control mechanisms should default to no access. The correct statement is that if access is not explicitly allowed, it should be implicitly denied.

Incorrect Answers:
A, C: Access rights should be granted to users based on their level of trust and their need-to-know.
D: Using roles is an effective method of assigning rights to a certain user who executes a specific task.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 203-206

QUESTION 419
The steps of an access control model should follow which logical flow:

A. Authorization, Identification, authentication
B. Identification, accountability, authorization
C. Identification, authentication, authorization
D. Authentication, Authorization, Identification

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting.
Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token. These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet. Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

Incorrect Answers:
A: A user (or other entity) must be must be identified and authentication before he can be authorized.

B: This answer does not include authentication which is key to access control.
D: A user (or other entity) must be must be identified before he can be authenticated and then authorized.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 160

QUESTION 420
What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?

A. Mandatory model
B. Discretionary model
C. Lattice model
D. Rule model

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A lattice is a mathematical construct that is built upon the notion of a group. The most common definition of the lattice model is “a structure consisting of a finite partially ordered set together with least upper and greatest lower bound operators on the set.” Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching: - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Incorrect Answers:
A: The model described in the question is a type of mandatory access control. However, the Lattice Model is specifically described in the question.
B: A discretionary model is not what is described in the question.
D: A rule model is not what is described in the question.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 381
https://en.wikipedia.org/wiki/Computer_access_control

QUESTION 421
Which access control model is also called Non-Discretionary Access Control (NDAC)?

A. Lattice based access control
B. Mandatory access control
C. Role-based access control
D. Label-based access control

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network. This type of access control can be role based or rule based, as both of these prevents users from making access decisions based upon their own discretion.

Incorrect Answers:
A: Lattice-based Access control is known as a label-based access control, or rule-based access control restriction.
B: Mandatory Access control is based on a security label system
D: Label-based access control uses one or more security labels to control who has read access or write access to individual rows and columns in a table

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228
https://en.wikipedia.org/wiki/Lattice-based_access_control
http://www.drdobbs.com/understanding-label-based-access-control/199201852

QUESTION 422
Which access model is most appropriate for companies with a high employee turnover?

A. Role-based access control
B. Mandatory access control
C. Lattice-based access control
D. Discretionary access control

Correct Answer: A

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Role-based access control (RBAC) model is the BEST system for a company whose staff renewal rate is high. For example, if an employee who is mapped to a certain role leaves the company, then his replacement can be easily mapped to this role. This results in the administrator not having to continually change the ACLs on the individual objects.

Incorrect Answers:
B: Mandatory Access control is considered nondiscretionary and is based on a security label system
C: Lattice-based Access control is known as a label-based access control, or rule-based access control restriction.
D: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228 https://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 423
Which of the following is NOT part of the Kerberos authentication protocol?

A. Symmetric key cryptography
B. Authentication service (AS)
C. Principals
D. Public Key

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is based on symmetric key cryptography, not asymmetric key cryptography, which is also called public and private keys.

Incorrect Answers:
A: Kerberos is based on symmetric key cryptography.
B: The authentication service is the part of the KDC that authenticates a principal
C: Principals can be users, applications, or network services that receive security services from the KDC.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213, 782

QUESTION 424
What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

A. A capability table
B. An access control list
C. An access control matrix
D. A role-based matrix

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Access control lists defines subjects that are authorized to access a specific object, and includes the level of authorization that subjects are granted.

Incorrect Answers:
A: A capability table stipulates the access rights that a specified subject has in relation to detailed objects.
C: An access control matrix is a table of subjects and objects that specifies the actions individual subjects can take upon individual objects.
D: A role-based matrix is not a valid answer with regards to this question.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 229-231

QUESTION 425
What is the difference between Access Control Lists (ACLs) and Capability Tables?

A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
C. Capability tables are used for objects whereas access control lists are used for users.
D. They are basically the same.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A capability table stipulates the access rights that a specified subject has in relation to detailed objects.
Access control lists defines subjects that are authorized to access a specific object, and includes the level of authorization that subjects are granted.
Therefore, the difference between the two is that the subject is bound to the capability table, while the object is bound to the ACL.

Incorrect Answers:
A: This is incorrect as access control lists are related/attached to an object, and capability tables are related/attached to a subject.
C: This is incorrect as access control lists are used for objects, and capability tables are for subjects.
D: access control lists and capability tables are not basically the same because one is bound to objects, and the other is bound to subjects.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 229-231

QUESTION 426
What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?

A. A capacity table
B. An access control list
C. An access control matrix
D. A capability table

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
An access control matrix is a table of subjects and objects that specifies the actions individual subjects can take upon individual objects.

Incorrect Answers:
A: A capacity table is not valid with regards to the context of this question.
B: Access control lists define subjects that are authorized to access a specific object, and includes the level of authorization that subjects are granted.
D: A capability table stipulates the access rights that a specified subject has in relation to detailed objects.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 229-231

QUESTION 427

Which access control model is BEST suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

A. DAC
B. MAC
C. Access control matrix
D. TACACS

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
MAC systems are generally very specialized and are used to protect highly classified data. Users require the correct security clearance to access a specific classification of data.

Incorrect Answers:
A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: An access control matrix is a table of subjects and objects indicating the actions individual subjects are allowed to take on individual objects.
D: TACACS is a remote access protocol, not an access control model.

References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 220-237

QUESTION 428
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:

Explanation:
Rule-based access control makes use of explicit rules that specify what can and cannot happen between a subject and an object.
Incorrect Answers:
B: An access control matrix is a table of subjects and objects specifying the actions individual subjects can take upon individual objects. C: Identification is a mechanism that falls under the Technical controls banner. D: Access terminal refers to the workstation that allows access.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 28, 227-229

QUESTION 429
Which access control model provides upper and lower bounds of access capabilities for a subject?

A. Role-based access control
B. Lattice-based access control
C. Biba access control
D. Content-dependent access control

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Lattice-based access control is a mathematical model that allows a system to easily represent the different security levels and control access attempts based on those levels. Every pair of elements has a highest lower bound and a lowest upper bound of access rights.

Incorrect Answers:
A: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
C: Biba is a security model, rather than an access control model. It centers on preventing information from flowing from a low integrity level to a high integrity level
D: Content-dependent access control is when the access decisions depend upon the value of an attribute of the object itself.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 224, 377, G-9
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.5365

QUESTION 430
What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The pattern of light receptors at the back of the eye
D. The pattern of blood vessels at the back of the eye

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A retinal scan is a biometric technique that uses the unique patterns on a person's retina blood vessels.
The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is not entirely genetically determined and thus even identical twins do not share a similar pattern.
Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric, aside from DNA. The National Center for State Courts estimate that retinal scanning has an error rate of one in ten million.
A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Because retinal blood vessels absorb light more readily than the surrounding tissue, the amount of reflection varies during the scan. The pattern of variations is digitized and stored in a database.

Incorrect Answers:
A: A retinal scan does not measure the amount of light reaching the retina. Therefore, this answer is incorrect.
B: A retinal scan does not measure the amount of light reflected by the retina. Therefore, this answer is incorrect.
C: A retinal scan does not measure the pattern of light receptors at the back of the eye. Therefore, this answer is incorrect.

References:
https://en.wikipedia.org/wiki/Retinal_scan

QUESTION 431
What is the main concern with single sign-on?

A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase. C. The users' password would be too hard to remember.
D. User access rights would be increased.

Correct Answer: A

Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.

Incorrect Answers:
B: Since the security administrator would not be responsible for maintaining multiple user accounts just the one, the security administrator's workload would decrease and not increase.
C: Since users would only have one password to remember, it would not be hard.
D: User access rights would not be any different than if they had to log into systems manually.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 207-209

QUESTION 432
In the context of access control, locks, gates, guards are examples of which of the following?

A. Administrative controls
B. Technical controls
C. Physical controls
D. Logical controls

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Physical controls are items put into place to protect facility, personnel, and resources. These include guards, locks, fencing, and lighting.

Incorrect Answers:
A: Administrative controls include Security policy, Monitoring and Supervising, Separation of duties, Job rotation, Information Classification, Personnel Procedures, Testing, and Security-awareness training.
B, D: Technical controls, which are also known as logical controls, are software or hardware components such as firewalls, IDS, encryption, identification and authentication mechanisms.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 32, 33

QUESTION 433
Access Control techniques do NOT include which of the following?

A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Relevant Access Controls is not a valid Access Control model.

Incorrect Answers:
B: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: Mandatory Access control is considered nondiscretionary and is based on a security label system.
D: Lattice-based Access control is known as a label-based access control, or rule-based access control restriction.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228
https://en.wikipedia.org/wiki/Lattice-based_access_control
https://en.wikipedia.org/wiki/Computer_access_control

QUESTION 434
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network.

Incorrect Answers:
A: Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.
B: Discretionary access control (DAC) is an access control model and policy that restricts access to objects according to the identity of the subjects and the groups to which those subjects belong.
D: Rule-based access control makes use of explicit rules that specify what can and cannot happen between a subject and an object.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 435
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/ software units. Such controls, also known as logical controls, represent which pairing?

A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Technical controls, which are also known as logical controls, are software or hardware components, such as firewalls, IDS, encryption, identification and authentication mechanisms. Preventive/Technical controls include the following:
▪ Passwords, biometrics, smart cards
▪ Encryption, secure protocols, call-back systems, database views, constrained user interfaces ▪
Antimalware software, access control lists, firewalls, intrusion prevention

Incorrect Answers:
A: Technical controls are also known as logical controls, not Administrative controls.
C: Technical controls are also known as logical controls, not Physical controls.
D: Detective/Technical controls include Audit logs and IDS.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 28-33

QUESTION 436
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control?

A. Discretionary Access Control (DAC)
B. Mandatory Access control (MAC)
C. Non-Discretionary Access Control (NDAC)
D. Lattice-based Access control

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Rule-based access control is considered nondiscretionary because the users cannot make access decisions based upon their own discretion.

Incorrect Answers:
A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
B: Mandatory Access control is considered nondiscretionary and is based on a security label system
D: Lattice-based Access control is known as a label-based access control, or rule-based access control restriction.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228 https://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 437
The type of discretionary access control (DAC) that is based on an individual's identity is also called:

A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.

Incorrect Answers:
B: Rule-based Access control is based on rules.
C: Non-Discretionary Access Control does not allow access based on discretion.
D: Lattice-based Access control is a type of label-based mandatory access control model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228 https://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 438
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?

A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control

Correct Answer: C

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Non-discretionary access control is when the system administrator or a single management body within an organization centrally controls access to all resources for everybody on a network. This type of access control can be role based or rule based, as both of these prevents users from making access decisions based upon their own discretion.

Incorrect Answers:
A: Mandatory Access Control is based on a security label system.
B: Discretionary Access control is based on identity.
D: Rule Based Access Control is based on rules.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228
http://www.answers.com/Q/What_is_Non_discretionary_access_control
https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Non_Discretionary_or_Role_Based_Access_Control

QUESTION 439
A periodic review of user account management should NOT determine:

A. conformity with the concept of least privilege.
B. whether active accounts are still being used.
C. strength of user-chosen passwords.
D. whether management authorizations are up-to-date.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/ database through either a dictionary or brute-force attack in order to check the strength of passwords.

Incorrect Answers:
A: A periodic review of user account management should determine conformity with the concept of least privilege.
B: A periodic review of user account management should determine whether active accounts are still being used.
D: A periodic review of user account management should determine whether management authorizations are up-to-date.

QUESTION 440
Which of the following access control models requires security clearance for subjects?

A. Identity-based access control
B. Role-based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Mandatory access control (MAC) is an access policy that restricts access to objects based on the security clearance of a subject and the classification of an object.

Incorrect Answers:
A: Identity-based access control is a type of DAC system that allows or prevents access based on the identity of the subject.
B: Role-based access control (RBAC) provides access to resources according to the role the user holds within the company or the tasks that the user has been assigned.
C: Access in a DAC model is restricted based on the authorization granted to the users.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 220-228

QUESTION 441
Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos uses public key cryptography.
B. Kerberos uses X.509 certificates.
C. Kerberos is a credential-based authentication system.

D. Kerberos was developed by Microsoft.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos uses symmetric key cryptography and provides end-to-end security. Although it allows the use of passwords for authentication, it was designed specifically to eliminate the need to transmit passwords over the network. Most Kerberos implementations work with shared secret keys.
Kerberos uses a credential-based mechanism as the basis for identification and authentication. Kerberos credentials are referred to as tickets.

Incorrect Answers:
A: Kerberos does not use public key cryptography (asymmetric); it uses symmetric key cryptography.
B: Kerberos does not use X.509 certificates. X.509 certificates are used in public key cryptography.
D: Kerberos was not developed by Microsoft; it was developed in the mid-1980s as part of MIT's Project Athena.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 209

QUESTION 442
Which of the following statements pertaining to using Kerberos without any extension is FALSE?

A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.
Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Kerberos does not use public key cryptography (asymmetric); it uses symmetric key cryptography.

Incorrect Answers:

A: It is true that a client can be impersonated by password-guessing.
B: It is true that Kerberos is mostly a third-party authentication protocol.
D: It is true that Kerberos provides robust authentication.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 64
http://www.ietf.org/rfc/rfc4556txt

QUESTION 443
Which of the following services is provided by S-RPC?

A. Availability
B. Accountability
C. Integrity
D. Authentication

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Secure Remote Procedure Call (S- RPC) is an authentication service and is simply a means to prevent unauthorized execution of code on remote systems.

Incorrect Answers:
A: S-RPC provides authentication, not availability.
B: S-RPC provides authentication, not accountability.
C: S-RPC provides authentication, not integrity.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 1419

QUESTION 444
A smart Card that has two chips with the Capability of utilizing both Contact and Contactless formats is called:

A. Contact Smart Cards
B. Contactless Smart Cards
C. Hybrid Cards
D. Combi Cards

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A smart Card that has two chips with the ability of utilizing both Contact and Contactless formats is called a combi card.

Incorrect Answers:
A: Contact Smart Cards are not configured for the Contactless format.
B: Contactless Smart Cards are not configured for the Contact format
C: The hybrid card makes use of two CPU chips for processing and includes both contact-oriented and contactless components.
D: The combi-card is similar to the hybrid card, but it only uses a single CPU chip for the processing.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, Sebastopol, p. 82
http://www.smartcardalliance.org/pages/smart-cards-intro-primer

QUESTION 445
The BEST technique to authenticate to a system is to:

A. establish biometric access through a secured server or Web site.
B. ensure the person is authenticated by something he knows and something he has.
C. maintain correct and accurate ACLs (access control lists) to allow access to applications.
D. allow access only through user ID and password.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
This is a tricky question. Normally, biometrics is the preferred answer as it is a more secure means of authentication than even multi-factor authentication. However, you would not establish biometric access through a secured server or Web site. Therefore, the answer must be "Ensure the person is authenticated by something he knows and something he has". This is an example of two-factor authentication.

Incorrect Answers:
A: You would not establish biometric access through a secured server or Web site.
C: Maintain correct and accurate ACLs is always a good idea. However, this provides no authentication solution as required by the question.

D: A user ID and password is single-factor authentication. The user ID and the password are both “something you

QUESTION 446
Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

A. Palm Scan
B. Hand Geometry
C. Fingerprint
D. Retina scan

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A system that reads a person’s retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously. Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person’s health, such as diabetes or high blood pressure.

Incorrect Answers:
A: While requiring contact with a surface shared by others, a palm scan is generally considered more acceptable than sharing a surface with other parts of the anatomy. Therefore, this answer is incorrect.
B: A Hand Geometry scan is less accurate and more acceptable than a retina scan. Therefore, this answer is incorrect.
C: A fingerprint scan is more acceptable to users than a retina scan. Users are much more likely to prefer placing their fingers on a fingerprint scanner than looking into a retina scanner. Therefore, this answer is incorrect.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191

QUESTION 447
Identity Management solutions include such technologies as Directories services, Single Sign-On and Web Access management. There are many reasons for management to choose an identity management solution.

Which of the following is a key management challenge regarding identity management solutions?

A. Increasing the number of points of failures.
B. Users will no longer be able to “recycle” their password for different applications.
C. Costs increase as identity management technologies require significant resources.
D. It must be able to scale to support high volumes of data and peak transaction rates.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identity management is the combination of business process and technology used to manage data on IT systems and applications about users. Managed data includes user objects, identity attributes, security entitlements and authentication factors.
Enterprises manage identity data about two broad kinds of users:
▪ Insiders: including employees and contractors. They often access multiple internal systems and their identity profiles are relatively complex. ▪
Outsiders: including customers, partners and vendors. There are normally many more outsiders than insiders.

One of the challenges presented by Identity management is scalability.
Enterprises manage user profile data for large numbers of people. There may be tens of thousands of insiders and hundreds of thousands of outsiders.
Any identity management system used in this environment must scale to support the data volumes and peak transaction rates produced by large user populations.

Incorrect Answers:
A: Increasing the number of points of failures is not key management challenge regarding identity management solutions. There should be no single points of failure but this would be more of a concern for the IT department than management.
B: Users not being able to “recycle” their password for different applications is not a concern for management.
C: A working scalable identity management system is more important to management than the cost. The resource requirement for identity management technologies is not that much when compared to the cost of other systems.

References:
http://hitachi-id.com/password-manager/docs/defining-enterprise-identity-management.html

QUESTION 448
When submitting a passphrase for authentication, the passphrase is converted into:

A. a virtual password by the system.
B. a new passphrase by the system.
C. a new passphrase by the encryption technology
D. a real password by the system which can be used forever.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A passphrase is a sequence of characters that is longer than a password. The user enters this phrase into an application, and the application transforms the value into a virtual password, making the passphrase the length and format that is required by the application. (For example, an application may require your virtual password to be 128 bits to be used as a key with the AES algorithm.) If a user wants to authenticate to an application, such as Pretty Good Privacy (PGP), he types in a passphrase, let's say StickWithMeKidAndYouWillWearDiamonds. The application converts this phrase into a virtual password that is used for the actual authentication.
A passphrase is more secure than a password because it is longer, and thus harder to obtain by an attacker. In many cases, the user is more likely to remember a passphrase than a password.

Incorrect Answers:
B: The passphrase is not converted into a new passphrase by the system.
C: The passphrase is not converted into a new passphrase by the encryption technology.
D: The passphrase is not converted into a real password by the system which can be used forever.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 199
http://www.itl.nist.gov/fipspubs/fip112htm

QUESTION 449
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication ProtocolC. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Extensible Authentication Protocol (EAP) is defined as:

A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

Incorrect Answers:
B: The definition in the question does not describe Challenge Handshake Authentication Protocol.
C: The definition in the question does not describe Remote Authentication Dial-In User Service.
D: The definition in the question does not describe Multilevel Authentication Protocol.

References:
http://www.sans.org/security-resources/glossary-of-terms/?pass=e
http://searchsecurity.techtarget.com/definition/Extensible-Authentication-Protocol-EAP

QUESTION 450
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

A. 100 subjects per minute.
B. 25 subjects per minute.
C. 10 subjects per minute.
D. 50 subjects per minute.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute.

Incorrect Answers:
A: 100 subjects per minute is just over half a second per user. This is way faster than is necessary.
B: 25 subjects per minute is less than 3 seconds per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.

D: 50 subjects per minute is just over one second per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59

QUESTION 451
Which of the following biometric parameters are better suited for authentication use over a long period of time?

A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Of the answers given, the iris is the least likely to change over a long period of time which makes the iris pattern better suited for authentication use over a long period of time.
The iris is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information gathered during the enrollment phase. Of the biometric systems, iris scans are the most accurate. The iris remains constant through adulthood, which reduces the type of errors that can happen during the authentication process.

Incorrect Answers:
B: A person's voice pattern is less suited for authentication use over a long period of time because the voice pattern can change over time.
C: A person's signature is less suited for authentication use over a long period of time because the signature can change over time.
D: A person's retina pattern is less suited for authentication use over a long period of time because the retina pattern can change over time and can be changed by illnesses such as Diabetes.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191

QUESTION 452
Which of the following is NOT a disadvantage of Single Sign On (SSO)?

A. Support for all major operating system environment is difficult
B. The cost associated with SSO development can be significant

C. SSO could be single point of failure and total compromise of an organization asset
D. SSO improves an administrator's ability to manage user's account and authorization to all associated system

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single sign-on (SSO) gives the administrator the ability to streamline user accounts and better control access rights. It, therefore, improves an administrator's ability to manage users and user configurations to all associated systems.

Incorrect Answers:
A: A disadvantage of SSO is that insufficient software solutions accommodate all major operating system environments. A mix of solutions must, therefore, be adapted to the enterprise's IT architecture and strategic direction.
B: A disadvantage of SSO is that considerable interface development and maintenance may be required, which could be costly.
C: SSO could be single point of failure and total compromise of an organization asset. This means that that if an attacker uncovers a credential set, the attacker would have access to every resource within the environment that the compromised account has access to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 207-209

QUESTION 453
Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?
A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
B. The pair of elements is the subject and object, and the subject has an upper bound lower than the upper bound of the object being accessed.
C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A lattice is a mathematical construct that is built upon the notion of a group. The most common definition of the lattice model is “a structure consisting of a finite partially ordered set together with least upper and greatest lower bound operators on the set.” Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching: - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Incorrect Answers:
B: The subject's upper bound must be equal or higher, not lower than the upper bound of the object being accessed.
C: The subject must have an upper bound.
D: The subject must have access rights determined by an upper bound.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 381
https://en.wikipedia.org/wiki/Computer_access_control http://en.wikipedia.org/wiki/Lattice-based_access_control

QUESTION 454
In the context of Biometric authentication, there is a quick way to compare the accuracy of devices. In general, the devices that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used
Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three main performance measures in biometrics. These measures are as follows:
- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected.
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted.
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase. Thus, to have a valid measure of the system performance, the CER is used.

Incorrect Answers:
B: FRR is the percentage of valid subjects that are falsely rejected. It is not used to compare accuracy of biometric devices.
C: FAR is the percentage of invalid subjects that are falsely accepted. It is not used to compare accuracy of biometric devices.
D: FER is not used to compare accuracy of biometric devices.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59
https://en.wikipedia.org/wiki/Biometrics

QUESTION 455
Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan
B. Fingerprint scan
C. Hand geometry
D. Signature recognition

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
Incorrect Answers:
A: While requiring contact with a surface shared by others, a fingerprint scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
B: While requiring contact with a surface shared by others, a hand geometry scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
C: A signature does not involve contact with a surface shared by others and is therefore more acceptable than other biometric methods.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 191
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

QUESTION 456

Which of the following would be an example of the BEST password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The following four rules apply to what can be contained in a password. The more rules that are met by a password, the stronger the password is.
Passwords should contain uppercase characters
Passwords should contain lowercase characters
Passwords should contain base 10 digits (0 through 9)
Passwords should contain nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
Further to the list above, passwords should be at least eight characters long and not include names, usernames or dictionary words.

The password T1me4g0lF meets three of the above rules. It contains uppercase characters, numeric characters and lowercase characters. This is the strongest password of the options given.

Incorrect Answers:
A: golf001 meets only two of the password rules. It contains lowercase and numeric characters. This is not the strongest password.
B: Elizabeth meets only two of the password rules. It contains lowercase and numeric characters. Furthermore, the password is a name which makes it easier to guess. This is not the strongest password.
D: 'password' is a very weak password. It meets only one password rule (it contains lowercase letters). It is also one of the most easily guessed passwords there is.

References:
http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password

QUESTION 457
Which of the following does NOT apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Passwords that are generated by a system or a password generation tool are robust passwords in that they will contain a mix of uppercase characters, lowercase characters, numbers and non-alphanumeric characters.
One of the benefits of system-generated passwords is that they are LESS (not more) vulnerable to brute force and dictionary attacks.

Incorrect Answers:
A: It is true that system-generated passwords are harder to remember for users. This is due to the complexity of the password.
B: It is true that if the password-generating algorithm gets to be known, the entire system is in jeopardy. This is because it would be possible to crack the passwords by using the algorithm used to create the passwords.
D: It is true that system-generated passwords are harder to guess for attackers. This is due to the complexity of the password.

QUESTION 458
What is the MOST critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements
C. Accuracy D. Scalability

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics are based on the Type 3 authentication mechanism — something you are. Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
The most critical characteristic of a biometric identifying system (or any other identification and authentication system) is the accuracy of the system. The system needs to ensure that the identification of the person is correct.

Incorrect Answers:
A: The perceived intrusiveness of a biometric system is an important consideration. Users will not be happy to use a system which is perceived to be too intrusive. However, this is not as critical as the accuracy of the system.
B: The storage requirement of a biometric system is not an important consideration. Storage is cheap nowadays and biometric data does not require much storage space.
D: The scalability of a biometric system could be an important consideration if the company intends to expand in the future although most biometric systems are easily scalable. However, this is not as critical as the accuracy of the system.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 58

QUESTION 459
What is considered the MOST important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II Error occurs when the system accepts impostors who should be rejected. This type of error is the most dangerous type, and therefore the most important to avoid.

Incorrect Answers:
A: A Type I Error is when a biometric system rejects an authorized individual. It is not as dangerous as a Type II Error, and therefore not the most important to avoid.
C: Combined Error Rate is not a valid type of biometric error.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate. It is the most important measurement when determining the system's accuracy.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 188

QUESTION 460
How can an individual/person BEST be identified or authenticated to prevent local masquerading attacks?

A. User Id and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Masquerading is the term used when one user pretends to be another user. Strong authentication is the best defense against this. Authentication is based on the following three factor types: ▪ Type 1. Something you know, such as a PIN or password
▪ Type 2. Something you have, such as an ATM card or smart card
▪ Type 3. Something you are (physically), such as a fingerprint or retina scan

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.
A biometric authentication such as a fingerprint cannot be imitated which makes biometrics the best defense against masquerading attacks.

Incorrect Answers:
A: A user Id and password can be guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.
B: A smart card can be stolen and the PIN guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.

C: Two-factor authentication is more secure than other methods but still less secure than biometrics. Two-factor authentication could comprise of “something you have” and “something you know”. The “something you have” such as a smart card could be stolen by an attacker and the “something you know” such as a PIN could be guessed. This is not the best identification and authentication method to prevent local masquerading attacks.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 187

QUESTION 461
What are cognitive passwords?

A. Passwords that can be used only once.
B. Fact or opinion-based information used to verify an individual's identity.
C. Password generators that use a challenge response scheme.
D. Passphrases.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Cognitive passwords refer to fact-based or opinion-based information used to verify the identity of an individual. The cognitive password enrollment process requires the answering of some questions based on the user’s life experiences.

Incorrect Answers:
A: Passwords that can be used only once are known as one-time passwords (OTPs).
C: Password generators that use a challenge response scheme are known as asynchronous token devices.
D: A passphrase is a sequence of characters that is longer than a password.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 195-199

QUESTION 462
Which of the following biometrics devices has the highest Crossover Error Rate (CER)?

A. Iris scan
B. Hand geometry
C. Voice pattern

D. Fingerprints
Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three main performance measures in biometrics. These measures are as follows:
- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected.
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted.
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.

Voice pattern biometrics have the highest Crossover Error Rate (CER). This is because voice patterns tend to change with the individual's mood and health. The common cold or flu, for instance, would alter the tone and pitch of a person's voice.

Incorrect Answers:
A: Iris scan biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of an iris scan and the fact that the iris rarely changes. B: Hand geometry biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of a hand geometry scan the fact that the hand rarely changes.
D: Fingerprint biometric devices do not have the highest Crossover Error Rate (CER) due to the accuracy of fingerprint scan the fact that the fingerprint rarely changes.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 59

QUESTION 463
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various users' accesses.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

A protected string of characters, known as a password, is used to authenticate an individual.

Incorrect Answers:
A: The primary use of a password is not to allow access to files, it is to authenticate an individual.
B: The primary use of a password is not to identify an individual, it is to authenticate an individual.
D: The primary use of a password is not to divide various user's accesses, it is to authenticate an individual.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 192

QUESTION 464
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

A. you need.
B. you read.
C. you are.
D. you do.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three common factors that can be used for authentication:
- Something a person knows.
- Something a person has.
- Something a person is.

Incorrect Answers:
A, B, D: These answers are not valid classic authentication factors.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 162

QUESTION 465
An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

A. Discretionary Access

B. Least Privilege
C. Mandatory Access
D. Separation of Duties

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more.

Incorrect Answers:
A: A: Discretionary Access Control (DAC) allows data owners to dictate what subjects have access to the files and resources they own.
C: Mandatory Access control is based on a security label system
D: Separation of Duties is a preventive administrative control that is used to make sure one person is unable to carry out a critical task alone.

References:
https://en.wikipedia.org/wiki/Principle_of_least_privilege
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 126, 220-228

QUESTION 466
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these items listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

A. Multi-party authentication
B. Two-factor authentication
C. Mandatory authentication
D. Discretionary authentication

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication provides identification of users via the combination of two different components, which could be something that the user knows, something that the user possesses or something that is inseparable from the user.

Incorrect Answers:

A: Multi-party authentication is not a valid term.
C: Mandatory authentication is not a valid term.
D: Discretionary authentication is not a valid term.

References:
https://en.wikipedia.org/wiki/Two-factor_authentication

QUESTION 467
Legacy single sign on (SSO) is:

A. Technology to allow users to authenticate to every application by entering the same user ID and password each time, thus having to remember only a single password.
B. Technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals.
C. A mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
D. Another way of referring to SESAME and KryptoKnight, now that Kerberos is the de-facto industry standard single sign on mechanism.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Legacy single sign on (SSO) is a mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
An SSO solution may provide a bottleneck or single point of failure. If the SSO server goes down, users are unable to access network resources. This is why it's a good idea to have some type of redundancy or fail-over technology in place.

Incorrect Answers:
A: Legacy single sign on (SSO) enables users to sign on once; they do not have to sign on to every application.
B: Legacy single sign on (SSO) is not technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals. This can be done with password synchronization.
D: Legacy single sign on (SSO) is not another way of referring to SESAME and KryptoKnight.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 177

QUESTION 468
Which type of password token involves time synchronization?

A. Static password tokens
B. Synchronous dynamic password tokens
C. Asynchronous dynamic password tokens
D. Challenge-response tokens

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Synchronous dynamic tokens make use of time or counters to synchronize a displayed token code with the code expected by the authentication server. Hence, the codes are synchronized.

Incorrect Answers:
A: Static passwords are reusable passwords that may or may not expire, and are normally user generated.
C: Asynchronous dynamic tokens are not synchronized with a central server.
D: Challenge-response tokens are asynchronous dynamic password tokens.

References:

Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 30-36

QUESTION 469
Which of the following would describe a type of biometric error refers to as FASLE rejection rate?

A. Type I error
B. Type II error
C. Type III error
D. CER error

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.

Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93
https://pciguru.wordpress.com/2010/05/01/one-two-and-three-factor-authentication/

QUESTION 470
Which of the following statements pertaining to biometrics is FALSE?

A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Type 2 authentication is based on something you have, like a token. Biometrics for part of Type 3 authentication, which is based on something you are. Something you are refers to an individual's physical traits.

Incorrect Answers:
A, B, C: These options are all TRUE with regards to biometrics.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 35-37
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187-189

QUESTION 471
Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos does not address availability
B. Kerberos does not address integrity

C. Kerberos does not make use of Symmetric Keys
D. Kerberos cannot address confidentiality of information

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not address availability.

Incorrect Answers:
B: Kerberos does address integrity.
C: Kerberos does make use of Symmetric Keys.
D: Kerberos does address confidentiality of information.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 472
Which of the following BEST ensures accountability of users for the actions taken within a system or domain?

A. Identification
B. Authentication
C. Authorization
D. Credentials

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.

To 'ensure' accountability, the user must prove that they are who they say they are. This is the function of authentication. Therefore, authentication best ensures accountability of users for the actions taken within a system or domain.

Incorrect Answers:
A: Identification is the user saying who they are. However, to ensure accountability, you need authentication to prove that they are who they say they are.
C: Authorization is the rights and permissions granted to an individual which enable access to a computer resource. This does not ensure accountability because it does not ensure that the user accessing the system is who they say they are.
D: Credentials are the user's username and password combination. However, authentication is the process of validating the credentials. Credentials alone (without validation/authentication) do not ensure that the user accessing the system is who they say they are.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 473
Which of the following statements pertaining to biometrics is FALSE?

A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics is based on "what you are" or "what you do". It is not based on what you know.

Incorrect Answers:
A: Behavioral (what you do), is one of the two categories that biometrics are divided into.
B: The physiological biometric category refers to traits that are physical attributes unique to a specific individual.
D: When determining a biometric system's accuracy, the CER metric is the most important measurement.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187, 188

QUESTION 474
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
According to the SANS Institute, an Iris scan has a lower CER than keystroke dynamics, voice verification, and fingerprint.

Incorrect Answers:
A, B, D: According to the SANS Institute, keystroke dynamics, voice verification, and fingerprint has a higher CER than iris scan.

References:
https://www.sans.org/reading-room/whitepapers/authentication/biometric-selection-body-parts-online-139

QUESTION 475
Which of the following is the WEAKEST authentication mechanism?

A. Passphrases
B. Passwords
C. One-time passwords
D. Token devices

Correct Answer: B

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Passwords are considered one of the weakest security mechanisms available, because users generally select passwords that are easy to guess.

Incorrect Answers:
A: Because a passphrase is longer, it is said to be more secure than a password.
C: Once a one-time password is used, it is no longer valid. It is, therefore, more secure than a normal password.
D: Token devices generate a One-time password, which is more secure than a normal password.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 192, 196, 197, 199

QUESTION 476
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?
A. Type I error
B. Type II error
C. Type III error
D. Crossover error

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.

Incorrect Answers:
A: A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93

QUESTION 477
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?

A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single Sign-On (SSO) allows a user to enter credentials once to gain access to all resources in primary and secondary network domains. Thereby, minimizing the amount of time users spend authenticating to resources and enabling the administrator to streamline user accounts and better control access rights. Furthermore, security is improved by reducing the likelihood that users will record passwords and also lessens the administrator's time spent on adding and removing user accounts and modifying access permissions. Because SSO requires a user to remember only one password, a but one of the goals is that if a user only has to remember one password, a more complicated and secure password policy can be enforced.

Incorrect Answers:
A: Smart cards are used for authentication purposes in access control. Although it can provide extra protection in an SSO environment, it does not provide the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access.
C: Symmetric Ciphers are used for encryption and decryption. It does not provide the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access.
D: Public Key Infrastructure allows for people who are widely dispersed to communicate securely and predictably.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 200, 207, 208, 833 https://en.wikipedia.org/wiki/Symmetric-key_algorithm#Cryptographic_primitives_based_on_symmetric_ciphers

QUESTION 478
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.

C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A security issue to consider in an SSO environment is that If an attacker uncovers a credential set, the attacker would have access to every resource within the environment that the compromised account has access to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 207, 2078

QUESTION 479
Which of the following is implemented through scripts or smart agents that replay the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single Sign-On (SSO) addresses the cumbersome situation of logging on multiple times to access different resources. In SSO, a user provides one ID and password per work session and is automatically logged-on to all the required applications. SSO can be implemented by using scripts that replay the users' multiple log-ins, or by using authentication servers to verify a user's identity and encrypted authentication tickets to permit access to system services.

Incorrect Answers:
B: Dynamic Sign-On is not the correct term to describe an authentication system that can be implemented through scripts or smart agents that replay the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services.
C: Smart cards provide static or dynamic passwords or certificates to authenticate a user. The authentication happens every time the smart card is presented and the login. This is not what is described in the question.

D: Kerberos can be used to implement Single-Sign on. However, “single sign-on” is the term described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 40

QUESTION 480
Which of the following protects a password from eavesdroppers and supports the encryption of communication?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP) C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
One approach to remote access security is the Challenge Handshake Authentication Protocol (CHAP). CHAP protects the password from eavesdroppers and supports the encryption of communication.
Challenge Handshake Authentication Protocol (CHAP) addresses some of the vulnerabilities found in PAP. It uses a challenge/response mechanism to authenticate the user instead of sending a password. When a user wants to establish a PPP connection and both ends have agreed that CHAP will be used for authentication purposes, the user’s computer sends the authentication server a logon request. The server sends the user a challenge (nonce), which is a random value. This challenge is encrypted with the use of a predefined password as an encryption key, and the encrypted challenge value is returned to the server. The authentication server also uses the predefined password as an encryption key and decrypts the challenge value, comparing it to the original value sent. If the two results are the same, the authentication server deduces that the user must have entered the correct password, and authentication is granted.

Incorrect Answers:
B: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Identification Protocol (CHIP).
C: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Encryption Protocol (CHEP).
D: The correct name for the protocol is Challenge Handshake Authentication Protocol (CHAP), not Challenge Handshake Substitution Protocol (CHSP).

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 66
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 710

QUESTION 481
The act of requiring two of the three factors to be used in the authentication process refers to:

A. Two-Factor Authentication
B. One-Factor Authentication
C. Bi-Factor Authentication
D. Double Authentication

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Two-Factor Authentication, also known as strong authentication, must include two out of the three authentication types.

Incorrect Answers:
B: One-Factor Authentication would only include a single authentication type.
C: Bi-Factor Authentication is not a valid authentication term.
D: Double Authentication is not a valid authentication term.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 163

QUESTION 482
Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token B.
The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Static password token is a device that contains a password which is physically hidden, but which is transmitted for each authentication. The token authenticates the identity of the owner to the information system.

Incorrect Answers:

B: Static password tokens will authenticate the identity of the owner to the information system.
C: Static password tokens do not allow the owner to authenticate himself to the system. It authenticates the identity of the owner to the information system.
D: Static password tokens authenticate the identity of the owner to the information system, not the system.

References:
https://en.wikipedia.org/wiki/Security_token
http://www.informit.com/guides/content.aspx?g=security&seqNum=146

QUESTION 483
In Synchronous dynamic password tokens:

A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
C. The unique password is not entered into a system or workstation along with an owner's PIN.
D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Synchronous dynamic password tokens generate new passwords at specific time intervals that are synched with the main system. Passwords are only valid for a specific time period.

Incorrect Answers:
B: With synchronous dynamic password tokens, a timer is used to rotate through various combinations produced by a cryptographic algorithm. Therefore the password will be unique.
C: With synchronous dynamic password tokens, the user enters the generated value and a user ID (this could be a PIN) into the computer, which then passes them to the server running the authentication service.
D: This is incorrect as the time value on the token device and a secret key is used to create the one-time password, which the authentication service decrypts and compares to the value it expected.

References:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
https://en.wikipedia.org/wiki/Security_token
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 196

QUESTION 484
In biometrics, "one-to-many" search against database of stored biometric images is done in:

A. Authentication
B. Identification
C. Identities
D. Identity-based access control

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A biometric system executes a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown user in identification mode. If the comparison of the biometric sample to a template in the database falls within a threshold previously set, identifying the individual will succeed.

Incorrect Answers:
A: In authentication mode, the biometric system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to confirm the individual is the person they claim to be.
C: Identities refer to who users are, not a mode used in biometrics.
D: An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.

References:
https://en.wikipedia.org/wiki/Biometrics

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 220

QUESTION 485
Which of the following is true of biometrics?

A. It is used for identification in physical controls and it is not used in logical controls.
B. It is used for authentication in physical controls and for identification in logical controls.
C. It is used for identification in physical controls and for authentication in logical controls.
D. Biometrics has no role in logical controls.

Correct Answer: C

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics is used for identification in physical controls and for authentication in logical controls. Physical controls are items put into place to protect facility, personnel, and resources. As a physical control, biometrics provides protection by identifying a person to see if that person is authorized to access a facility. When a user is identified and granted physical access to a facility, biometrics can be used for authentication in logical controls to provide access to resources.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:
A: Biometrics is used in logical controls.
B: Biometrics is used for identification in physical controls and for authentication in logical controls, not the other way round. Biometrics is used first as a physical control to identify a person to grant access to a facility, and then as a logical control to authenticate the user to provide access to resources.
D: Biometrics does have a role in logical controls.

References:

What is the percentage of valid subjects that are falsely rejected by a Biometric Authentication system called?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.

Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.
D: The true reject rate refers to the percentage of times a system correctly rejects a false claim of identity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=93

QUESTION 487
What is the percentage of invalid subjects that are falsely accepted by a Biometric authentication system called?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Acceptance Rate (TAR) or Type III Error

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.

Incorrect Answers:
A: A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.
C: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.
D: The true accept rate is the percentage of times a system correctly verifies a true claim of identity.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 188
http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=92

QUESTION 488
Which of the following is NOT a security characteristic we need to consider while choosing a biometric identification system?

A. data acquisition process

B. cost
C. enrollment process
D. speed and user interface

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
The cost of the biometric identification system is a financial consideration, not a security consideration.

The data acquisition process refers to how a user's biometric data will be acquired. Will you use a fingerprint scan, a retina scan, a palm scan etc. This is an obvious security characteristic to be considered while choosing a biometric identification system.
The enrollment process refers to how the user's biometric data will be initially acquired and the data stored as a template for comparison for future identifications. This is also a security characteristic to be considered while choosing a biometric identification system.
The speed and user interface are security characteristics to be considered while choosing a biometric identification system. You need a biometric identification system that does not keep the user waiting before being identified and authenticated. The user interface for a biometric identification system should include instructional and feedback aspects that would enable users to use the system effectively without assistance.

Incorrect Answers:
A: The data acquisition process refers to how a user's biometric data will be acquired. This is a security characteristic to be considered while choosing a biometric identification system.
C: The enrollment process is a security characteristic to be considered while choosing a biometric identification system.
D: The speed and user interface are security characteristics to be considered while choosing a biometric identification system.

QUESTION 489
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person.

This raised the necessity of answering two questions: A. What was the sex of a person and his age?

B. What part of body to be used and how to accomplish identification that is viable?
C. What was the age of a person and his income level?
D. What was the tone of the voice of a person and his habits?

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:

Explanation:
When it became apparent that truly positive identification could only be based on physical attributes of a person, two questions had to be answered. First, what part of body could be used? Second, how could identification be accomplished with sufficient accuracy, reliability and speed so as to be viable?
Because most identity authentication requirements take place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are the hands, face and eyes.

Incorrect Answers:
A: The sex of a person and his age are not considered in biometric identification systems.
C: The age of a person and his income level are not considered in biometric identification systems.
D: The tone of the voice of a person and his habits are not considered in biometric identification systems.

References:
Tipton, Harold F. and Micki Krause, *Information Security Management Handbook*, 5th Edition, Auerbach Publications, Boca Raton, 2006, p. 62

QUESTION 490
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A smart card, which includes the ability to process data stored on it, is also able to deliver a two-factor authentication method as the user may have to enter a PIN to unlock the smart card. The authentication can be completed by using an OTP, by utilizing a challenge/response value, or by presenting the user's private key if it is used within a PKI environment. The fact that the memory of a smart card is not readable until the correct PIN is entered, as well as the complexity of the smart token makes these cards resistant to reverse-engineering and tampering methods.

Incorrect Answers:
A: Transparent renewal of user keys is not the primary role of smartcards in a PKI.
B: Easy distribution of the certificates between the users is not the primary role of smartcards in a PKI.
C: Fast hardware encryption of the raw data is not the primary role of smartcards in a PKI.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 200, 201
http://en.wikipedia.org/wiki/Tamper_resistance

QUESTION 491
In biometric identification systems, the parts of the body conveniently available for identification are:

A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Most identity authentication takes place when people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.

Incorrect Answers:
A: The neck is not convenient as it can be covered.
C: The feet normally have shoes on, and therefore not convenient.
D: The neck is not convenient as it can be covered.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 187-192

QUESTION 492
Which of the following is TRUE of two-factor authentication?

A. It uses the RSA public-key signature based on integers with large prime factors.
B. It requires two measurements of hand geometry.
C. It does not use single sign-on technology.
D. It relies on two independent proofs of identity.

Correct Answer: D

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three general factors that are used for authentication:
- Something a person knows.
- Something a person has.
- Something a person is.

Two-factor authentication requires two of the three factors to be part of authentication process.

Incorrect Answers:
A: RSA encryption uses integers with exactly two prime factors, but the term "two-factor authentication" is not used in that context.
B: Measuring hand geometry twice only provides one factor.
C: Single sign-on (SSO) technology allows a user to enter their credentials once to gain access to multiple systems. Two-factor authentication could be used for SSO, not the other way around.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 162, 163, 207, 815

QUESTION 493
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

Incorrect Answers:
B: In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use.
C: A root certificate is an unsigned or a self-signed public key certificate that identifies the Root Certificate Authority (CA).
D: Code signing digitally signs executables and scripts to verify the software author and guarantee that the code has not been changed or tainted since it was signed by use of a cryptographic hash.

References:
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate
https://en.wikipedia.org/wiki/Root_certificate
https://en.wikipedia.org/wiki/Code_signing

QUESTION 494
Single Sign-on (SSO) is characterized by which of the following advantages?

A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Single sign-on allows users to type their passwords only once when they first log in to access all the network resources. This makes SSO convenient.
Single Sign-on allows a single administrator to add and delete accounts across the entire network from one user interface, providing centralized administration.

Incorrect Answers:
A: Single Sign-on does offer convenience, but it also offers centralized administration, making option B a more suitable answer.
C: Centralized data administration is not an advantage of Single Sign-on.
D: Centralized network administration is not an advantage of Single Sign-on.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 42
QUESTION 495
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

A. Authentication
B. Identification
C. Authorization
D. Confidentiality

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification involves a user supplying identification information using a username, user ID, or account number.

Incorrect Answers:
A: Authentication involves verifying a user's identification information using a passphrase, PIN value, biometric, one-time password, or password.
C: Authorization is when a system establishes whether the user is authorized to access the particular resource and what actions he is permitted to perform on that resource.
D: Confidentiality is used to make sure that the required level of secrecy is imposed at every junction of data processing and prevents unauthorized disclosure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 24, 166, 203

QUESTION 496
What is the verification that the user's claimed identity is valid called and is usually implemented through a user password at log-on time?

A. Authentication
B. Identification
C. Integrity
D. Confidentiality

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Authentication involves verifying a user's identification information using a passphrase, PIN value, biometric, one-time password, or password.

Incorrect Answers:
B: Identification involves a user supplying identification information using a username, user ID, or account number.
C: Integrity is a security principle that ensures information and systems are not maliciously or accidentally modified.
D: Confidentiality is used to make sure that the required level of secrecy is imposed at every junction of data processing and prevents unauthorized disclosure.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 23, 24, 166

QUESTION 497
Which of the following is TRUE about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos makes use of symmetric key cryptography and offers end-to-end security. The majority Kerberos implementations works with shared secret keys.

Incorrect Answers:
A: Kerberos makes use of symmetric key cryptography, which does not include the use of public keys.
B: Kerberos was specifically designed to remove the need to transmit passwords over the network.
D: Kerberos is a trusted third-party service.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 782
https://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 498
A confidential number used as an authentication factor to verify a user's identity is called a:

A. PIN
B. User ID
C. Password D. Challenge

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Personal Identification Number (PIN) is a numeric password shared between a user and a system, which can be used to authenticate the user to the system.

Incorrect Answers:
B: User ID is used for identification, not authentication.
C: A password is a word or string of characters used for user authentication.
D: Challenge-response authentication involves one party presenting a question ("challenge") and another party providing a valid answer ("response") to be authenticated. It does not specifically be a number sequence.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 162
https://en.wikipedia.org/wiki/Personal_identification_number
https://en.wikipedia.org/wiki/Password https://en.wikipedia.org/wiki/Challenge-response_authentication#Cryptographic_techniques

QUESTION 499
Which type of password provides maximum security because a new password is required for each new log-on?

A. One-time or dynamic password
B. Cognitive password
C. Static password
D. Passphrase

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A one-time or dynamic password is no longer valid and, if obtained by a hacker, cannot be reused after it has been used. A one-time or dynamic password is used in environments where a higher level of security than static passwords is required.
Incorrect Answers:
B: After a user is enrolled by answering several questions based on her life experiences, the user can answer the questions asked of her to be authenticated instead of having to remember a password. The questions do not change from log-on to log-on.

C: Static passwords are passwords that can be reused, but may or may not expire.
D: Passphrases are long static passwords, which is made up of words in a phrase or sentence.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 195, 196
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 30

QUESTION 500
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality
C. authentication
D. authorization

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a third-party authentication service that can be used to support SSO.

Incorrect Answers:
A: Non-repudiation provides assurance that a specific user performed a specific transaction that did not change. It is not, however, the primary service provided by Kerberos.
B: Confidentiality strives to prevent unauthorized read access to data. It is not, however, the primary service provided by Kerberos.
D: Authorization refers to the actions you are allowed to carry out on a system after identification and authentication has taken place. It is not, however, the primary service provided by Kerberos.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 12, 14, 15, 43

QUESTION 501
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos uses shared secret keys and tickets for the initial authentication, not a public key algorithm.

Incorrect Answers:
A: Kerberos is an example of a single sign-on system for distributed environments, and therefore only requires a single login per session.
C: the foundation of Kerberos security is trust that clients and services have in the integrity of the KDC.
D: Kerberos provides mutual authentication in that both the user and the server verify each other's identity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213
https://en.wikipedia.org/wiki/Kerberos_(protocol)

QUESTION 502
The authenticator within Kerberos provides a requested service to the client after validating which of the following?

A. timestamp
B. client public key

C. client private key
D. server public key

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In Kerberos implementations where the use of an authenticator is configured, the user sends their identification information and a timestamp and sequence number encrypted with the shared session key to the requested service, which then decrypts this information and compares it with the identification data the KDC sent to it about this requesting user. If the data matches, the user is allowed access to the requested service.

Incorrect Answers:
B: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a client public key.
C: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a client private key.
D: A requested service is provided to the client after validating a user's identification information and a timestamp and encrypted sequence number, not a server public key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 209-213

QUESTION 503
Which of the following is addressed by Kerberos?

A. Confidentiality and Integrity
B. Authentication and Availability
C. Validation and Integrity
D. Auditability and Integrity

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:

Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability and attacks such as frequency analysis.

Incorrect Answers:
B: Kerberos an authentication protocol. However, it does not address availability.
C: Kerberos does address integrity but it does not address validation.
D: Kerberos does address integrity but it does not address auditability.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 504
Kerberos is vulnerable to replay in which of the following circumstances?

A. When a private key is compromised within an allotted time window.
B. When a public key is compromised within an allotted time window.
C. When a ticket is compromised within an allotted time window.
D. When the KSD is compromised within an allotted time window.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability and attacks such as frequency analysis. Furthermore, because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code. Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window. Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

Incorrect Answers:
A: Kerberos does not use a private key like an asymmetric key cryptography system does. It uses symmetric key cryptography (shared key).
B: Kerberos does not use a public key like an asymmetric key cryptography system does. It uses symmetric key cryptography (shared key).
D: KSD being compromised is not a vulnerability of Kerberos.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 78

QUESTION 505
Like the Kerberos protocol, SESAME is also subject to which of the following?

A. timeslot replay
B. password guessing
C. symmetric key guessing
D. asymmetric key guessing

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Just like Kerberos, SESAME depends on the initial user authentication. For that reason, SESAME has the same weakness to attacks on the user's password as Kerberos does.

Incorrect Answers:
A: SESAME is not susceptible to timeslot replay attacks.
C: Symmetric key guessing is not a weakness of Kerberos.
D: Asymmetric key guessing is not a weakness of Kerberos.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, Sebastopol, p. 101
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 46

QUESTION 506
RADIUS incorporates which of the following services?

A. Authentication server and PIN codes.
B. Authentication of clients and static passwords generation.
C. Authentication of clients and dynamic passwords generation.
D. Authentication server as well as support for Static and Dynamic passwords.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:

Explanation:
A central authentication service for dial-up users is the standard Remote Authentication and Dial-In User Service (RADIUS). RADIUS incorporates an authentication server and dynamic passwords. The RADIUS protocol is an open lightweight, UDP-based protocol that can be modified to work with a variety of security systems. It provides authentication, authorization and accounting services to routers, modem servers, and wireless applications. RADIUS is described in RFC 2865.

Incorrect Answers:
A: RADIUS does not incorporate PIN codes.
B: Authentication of clients is provided by the authentication server which is incorporated into RADIUS. RADIUS does not incorporate static passwords 'generation'.
C: Authentication of clients is provided by the authentication server which is incorporated into RADIUS. RADIUS does not incorporate dynamic passwords 'generation'.
References:
Cole, Eric, *Network Security Bible*, Wiley Publishing, Indianapolis, 2009, p. 124

QUESTION 507
Which of the following would constitute the BEST example of a password to use for access to a system by a network administrator?

A. holiday
B. Christmas12
C. JennyD. GyN19Za!

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A generally accepted minimum standard for password complexity is a minimum of eight characters, one uppercase alpha character, one lowercase alpha character, one number character, and one symbol character. Therefore, "**GyN19Za!**" is the best example.

Incorrect Answers:
A: This option does not satisfy the minimum complexity as it only has lowercase characters.
B: This option does not satisfy minimum complexity as there are no alpha or symbol characters.
C: This option does not satisfy the minimum complexity as it is less than eight characters, and has no alpha, number, or symbol characters.

References:
Miller, David R, *CISSP Training Kit*, O'Reilly Media, 2013, California, p. 77

QUESTION 508
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls

Correct Answer: C
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Incorrect Answers:
A: Controls are administrative, logical/technical or physical. Accountability controls are not a defined control type and do not ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
B: Mandatory access controls are an access control type. They do not ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
D: Administrative controls are a group of controls that include policies and procedures. However, assurance procedures are the specific name for the set of procedures that ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 47

QUESTION 509
Smart cards are an example of which type of control?

A. Detective control
B. Administrative control
C. Technical control
D. Physical control

Correct Answer: C

Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Smart cards are an example of a Preventive/Technical control.

Incorrect Answers:
A: Detective controls include Motion detectors, Closed-circuit TVs, Monitoring and Supervising, Job rotation, Investigations, Audit logs, and IDS.
B: Administrative controls include Security policy, Monitoring and Supervising, Separation of duties, Job rotation, Information Classification, Personnel Procedures, Testing, and Security-awareness training.
D: Physical controls include Fences, Locks, Badge system, Security guard, Biometric system, Mantrap doors, Lighting, Motion detectors, and Closed-circuit TVs.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 32, 33

QUESTION 510
Which of the following is NOT a two-factor authentication mechanism?

A. Something you have and something you know.
B. Something you do and a password.
C. A smartcard and something you are.
D. Something you know and a password.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Two-factor authentication includes two of the following three factors:
- Something you know - Password
- Something you have - Token
- Something you are - Biometrics

A password is something you know, and cannot be used together for two-factor authentication.

Incorrect Answers:
A, B, C: This answer satisfies the requirements for two-factor authentication.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 163

QUESTION 511
Which of following is NOT a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Correct Answer: B
Section: Identity and Access Management
Explanation
Explanation/Reference:
Explanation:
The AAA term refers to authentication, authorization, and accounting/audit. Administration is not one of the options, therefore, the correct answer.

Incorrect Answers:
A, C, D: Authentication, Accounting, and Authorization are what the AAA term refers to.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 236

QUESTION 512
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:

Explanation:
TACACS has been through three generations: TACACS, Extended TACACS (XTACACS), and TACACS+. TACACS combines its authentication and authorization processes; XTACACS separates authentication, authorization, and auditing processes; and TACACS+ is XTACACS with extended two-factor user authentication. TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection. The original TACACS was developed during the days of ARPANET which is the basis for the Internet. TACACS uses UDP as its communication protocol. TACACS + uses TCP as its communication protocol.

Incorrect Answers:
A: TACACS uses UDP as its communication protocol, not TCP.
B: TACACS uses UDP as its communication protocol, not SSL.
D: TACACS uses UDP as its communication protocol, not SSH.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 234
Jacobs, Josh, et al., *SSCP Systems Security Certified Practitioner Study Guide and DVD Training System*, Syngress, Rockland, 2003, p. 450
http://en.wikipedia.org/wiki/TACACS

QUESTION 513
What is Kerberos?

A. A three-headed dog from the Egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial-in user server.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a third-party authentication service that can be used to support SSO.
Kerberos (or Cerberus) was the name of the three-headed dog that guarded the entrance to Hades in Greek mythology.

Incorrect Answers:
A: Kerberos (or Cerberus) was the name of the three-headed dog that guarded the entrance to Hades in Greek mythology. We are, however, dealing with information systems, not mythology.
C: Kerberos is an authentication protocol, not just a security model.
D: A remote authentication dial in user server refers to RADIUS, not Kerberos.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 22, 43

QUESTION 514
Which of the following can BEST eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5
D. Only attaching modems to non-networked hosts.

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
As client computers used to have built-in modems to allow for Internet connectivity, organizations commonly had a pool of modems to allow for remote access into and out of their networks. In some cases the modems were installed on individual servers here and there throughout the network or they were centrally located and managed. Most companies did not properly enforce access control through these modem connections, and they served as easy entry points for attackers. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall can best eliminate dial-up access through a Remote Access Server as a hacking vector. This solution would mean that even if an attacker gained access to the Remote Access Server, the firewall would provide another layer of protection.

Incorrect Answers:
A: Using a TACACS+ server does provide a good remote access authentication and authorization solution. However, to best eliminate dial-up access through a Remote Access Server as a hacking vector, you should place the remote access server outside the firewall.
C: Setting modem ring count to at least 5 may deter wardialers but it does not eliminate dial-up access through a Remote Access Server as a hacking vector.
D: Only attaching modems to non-networked hosts do not eliminate dial-up access through a Remote Access Server as a hacking vector. Besides being impractical, the non-network hosts would be vulnerable to attack.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 695

QUESTION 515
Which authentication technique BEST protects against hijacking?

A. Static authentication
B. Continuous authentication

C. Robust authentication
D. Strong authentication

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. These can be compromised by session hijacking. Continuous authentication prevents session hijacking.
Continuous Authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect.
Incorrect Answers:
A: Static authentication only provides protection against attacks in which an imposter cannot see, insert or alter the information passed between the claimant and the verifier during an authentication exchange and subsequent session. Static authentication does not protect against hijacking.
C: Robust Authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and verifier. Robust or dynamic authentication does not protect against hijacking.
D: Strong authentication is not a specific authentication type; it is another term for multi-factor authentication.

References:
http://www.windowsecurity.com/whitepapers/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Sample_Policy_Areas.html

QUESTION 516
Which of the following is NOT a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources
D. Automated login for remote users

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Protection of confidential data is one of the most important security aspects of any business.
Providing remote access to a network and its computer systems brings new risks. Is the person logging in remotely who he claims to be? Is someone physically or electronically looking over his shoulder, or tapping the communication line? Is the client device from which he is performing the remote access in a secure configuration, or has it been compromised by spyware, Trojan horses, and other malicious code?
When providing remote access to your network, you need reliable authentication of users and systems. You also need to be able to control access to the systems and network resources.
Automated login for remote users is not a security goal for remote access. Logins should not be automated for remote users. Automated logins do not improve the security of the network or systems.

Incorrect Answers:
A: Reliable authentication of users and systems is a security goal for remote access.
B: Protection of confidential data is a security goal for remote access.
C: Easy to manage access control to systems and network resources is a security goal for remote access.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1250

QUESTION 517
During an IS audit, one of your auditors has observed that some of the critical servers in your organization can be accessed ONLY by using a shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

A. Password sharing
B. Accountability
C. Shared account management
D. Difficulty in auditing shared account

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
Audit trails list the actions performed by the user account used to perform the actions. However, if all the users are using the same user account, you have no way of knowing which person performed which action. Therefore, you have no "accountability".

Incorrect Answers:
A: Password sharing is not the primary concern in this case. The only password shared is the password for the shared account.
C: Shared account management is not a concern. The fact that the account is shared is the concern.
D: Difficulty in auditing shared account is not the primary concern. Auditing a single account is not a problem. The problem is that you do not know which person is using the account at any given time.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 57

QUESTION 518
During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

A. Eavesdropping
B. Traffic analysis
C. Masquerading
D. Race Condition

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A race condition happens when two different processes need to carry out their tasks on the same resource.

Incorrect Answers:
A: Sniffing or eavesdropping involves the capturing and recording of all frames traveling across the network media. B: Traffic analysis is used for discovering information by watching traffic patterns on a network. C: Masquerading occurs by impersonating another user to gain unauthorized access to a system

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 410, 411, 1060, 1294
Miller, David R, CISSP Training Kit, O'Reilly Media, 2013, Sebastopol, p. 508

QUESTION 519
Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of its internals?

A. Black-box testing

B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Black box testing examines the functionality of an application without peering into its internal structures or workings. Black box testing provides the tester with no internal details; the software is treated as a black box that receives inputs.

Incorrect Answers:
B: Parallel Testing is the process of entering the same inputs in two different versions of the application and reporting the anomalies.
C: Regression Testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
D: Pilot Testing is a preliminary test that focuses on specific and predefined aspect of a system.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1105 https://en.wikipedia.org/wiki/Black-box_testing
http://www.tutorialspoint.com/software_testing_dictionary/parallel_testing.htm http://soft-engineering.blogspot.co.za/2010/12/what-is-difference-between-pilot-and.html

QUESTION 520
Which of the following is NOT a technique used to perform a penetration test?

A. traffic padding
B. scanning and probing
C. war dialing
D. sniffing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:

Explanation:
Traffic padding is a countermeasure to traffic analysis.
Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organizing a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.
Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner.

Incorrect Answers:
B: Scanning and probing is a technique used in Penetration Testing. Various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports.
C: War dialing is a technique used in Penetration Testing. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers to hack in to.
D: Sniffing (packet sniffing) is a technique used in Penetration Testing. Packet sniffing is the process of intercepting data as it is transmitted over a network.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, pp. 233, 238.
https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_analysis

QUESTION 521
Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

A. They are more cost-effective
B. They offer a lack of corporate bias
C. They use highly talented ex-hackers
D. They ensure a more complete reporting

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Two points are important to consider when it comes to ethical hacking: integrity and independence.

By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not cost-effective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques.

External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps.

Incorrect Answers:
A: External penetration service firms are more cost-effective than using corporate resources for penetration testing. This is a valid reason to use external penetration service firms.
B: External penetration service firms do offer a lack of corporate bias compared to corporate resources. This is a valid reason to use external penetration service firms.
D: External penetration service firms do tend to ensure more complete reporting than corporate resources. This is a valid reason to use external penetration service firms.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 517

QUESTION 522
Which of the following statements pertaining to ethical hacking is NOT true?

A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely to simulate external threats.
C. Ethical hacking should not involve writing to or modifying the target systems negatively.
D. Ethical hackers never use tools that have the potential of affecting servers or services.

Correct Answer: D
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Ethical hackers should use tools that have the potential of affecting servers or services to provide a valid security test. These are the tools that a malicious hacker would use.
The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understands that some of the tests could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.

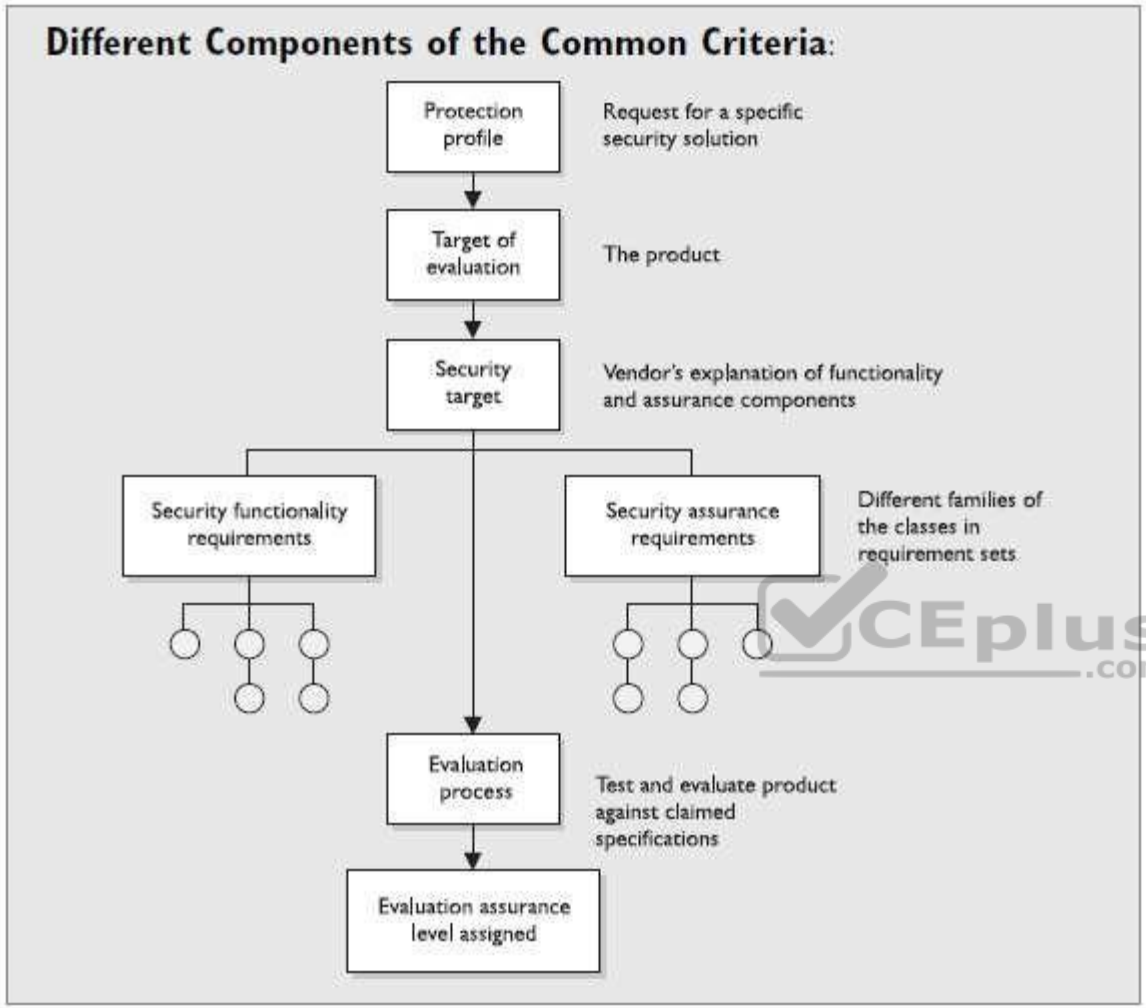
Incorrect Answers:
A: An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions at the same time as doing testing for the same client.
B: Testing should be done remotely to simulate external threats. Testing simulating a cracker from the Internet is often one of the first tests being done. This is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.
C: Ethical hacking should not involve writing to or modifying the target systems negatively. Proving the ability to write to or modify the target systems (without causing harm) is enough to demonstrate the existence of a vulnerability.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 520

QUESTION 523
Common Criteria 15408 generally outlines assurance and functional requirements through a security evaluation process concept of _____, _____, _____ for Evaluated Assurance Levels (EALs) to certify a product or system.

A. EAL, Security Target, Target of Evaluation
B. SFR, Protection Profile, Security Target
C. Protection Profile, Target of Evaluation, Security Target
D. SFR, Security Target, Target of Evaluation

Correct Answer: C
Section: Security Assessment and Testing
Explanation
Explanation/Reference:
Explanation:
Under the Common Criteria model, an evaluation is carried out on a product and it is assigned an Evaluation Assurance Level (EAL). The thorough and stringent testing increases in detailed-oriented tasks as the assurance levels increase. The Common Criteria has seven assurance levels. The range is from EAL1, where functionality testing takes place, to EAL7, where thorough testing is performed and the system design is verified. The different components are shown in the exhibit below:



Incorrect Answers:
A: Evaluated Assurance Levels (EALs) determine the levels of evaluation required. EAL is not a common criteria security evaluation process concept. B: Security functional requirements (SFRs) are individual security functions which must be provided by a product. An SFR is not a common criteria security evaluation process concept.
D: Security functional requirements (SFRs) are individual security functions which must be provided by a product. An SFR is not a common criteria security evaluation process concept.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 403-405

QUESTION 524
You are a security consultant who is required to perform penetration testing on a client's network. During penetration testing, you are required to use a compromised system to attack other systems on the network to avoid network restrictions like firewalls.

Which method would you use in this scenario:

A. Black box Method
B. Pivoting methodC. White Box Method.
D. Grey Box Method

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Pivoting is a method that makes use of the compromised system to attack other systems on the same network to avoid restrictions that might prohibit direct access to all machines.

Incorrect Answers:
A: Black box testing examines the functionality of an application without peering into its internal structures or workings.
C: With white box testing, the testers are provided with complete knowledge of the infrastructure being tested.
D: With gray-box pen testing, the tester is provided with partial knowledge of the infrastructure being tested.

References:
https://en.wikipedia.org/wiki/Exploit_(computer_security)#Pivoting
https://en.wikipedia.org/wiki/Black-box_testing
http://www.redsphereglobal.com/content/penetration-testing

QUESTION 525
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.

D. Production environment using sanitized live workloads data.

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
You should perform stress tests in a test environment. It is best to use live workload data as the stress test would be more realistic.
Stress testing (sometimes called torture testing) is a form of deliberately intense or thorough testing used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

Incorrect Answers:
A: It would be better to use live workload data.
C: You should not perform stress tests in the product environment.
D: You should not perform stress tests in the product environment.

References:
https://en.wikipedia.org/wiki/Stress_testing

QUESTION 526
Which of the following are required for Life-Cycle Assurance?

A. System Architecture and Design specification
B. Security Testing and Covert Channel Analysis
C. Security Testing and Trusted distribution
D. Configuration Management and Trusted Facility Management

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.

The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces the requirements. By extension, assurance must include a guarantee that the trusted portion of the system works only as intended. To accomplish these objectives, two types of assurance are needed with their respective elements:
Operational Assurance: System Architecture, System Integrity, Covert Channel Analysis, Trusted Facility Management and Trusted Recovery **Life-cycle Assurance:** Security Testing, Design Specification and Verification, Configuration Management and Trusted System Distribution

Incorrect Answers:
A: System Architecture is not required for Life-Cycle Assurance. System Architecture is part of Operational Assurance.
B: Covert Channel Analysis is not required for Life-Cycle Assurance. Covert Channel Analysis is part of Operational Assurance.
D: Trusted Facility Management is not required for Life-Cycle Assurance. Trusted Facility Management is part of Operational Assurance.

References:
https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

QUESTION 527
What is the most effective means of determining that controls are functioning properly within an operating system?

A. Interview with computer operator
B. Review of software control features and/or parameters
C. Review of operating system manual
D. Interview with product vendor

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Various operating system software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments. The reviewing of software control features and/or parameters is the most effective means of determining how controls are functioning within an operating system and of assessing and operating system's integrity.
The review of software control features and/or parameters would be part of your security audit. A security audit is typically performed by an independent third party to the management of the system. The audit determines the degree with which the required controls are implemented.

A security review is conducted by the system maintenance or security personnel to discover vulnerabilities within the system. A vulnerability occurs when policies are not followed, misconfigurations are present, or flaws exist in the hardware or software of the system. System reviews are sometimes referred to as a vulnerability assessment.

Incorrect Answers:
A: An interview with the computer operator is not an effective means of determining that controls are functioning properly within an operating system because the computer operator will not necessarily be aware of the detailed settings of the parameters.
C: The operating system manual should provide information as to what settings can be used but will not give any hint as to how parameters are actually set.
D: An interview with the product vendor is not an effective means of determining that controls are functioning properly within an operating system because the product vendor will not be aware of the detailed settings of the parameters.

QUESTION 528
Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
You should always separate test and development environments.
When testing a system, you need to isolate the system to ensure the test system is controlled and stable. This will ensure the system is tested in a realistic environment that mirrors the live environment as closely as possible.
Access control methods can be used to easily separate the test and development environments.

Incorrect Answers:
A: Restricting access to systems under test is not the best reason for separating the test and development environments. Preventing instability in a development environment from affecting the test environment is a better answer.
C: Segregate user and development staff is not the best reason for separating the test and development environments.
D: Securing access to systems under development is not the best reason for separating the test and development environments. Securing access to systems under development would not be achieved by separating the test and development environments.

QUESTION 529
Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security

requirements? A. Validation

B. Verification C.
Assessment

D. Accuracy

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Verification is the process of determining whether the product accurately represents and meets the design specifications given to the developers.

Incorrect Answers:
A: Validation is the process of determining whether the product provides the necessary solution for the real-world problem that is was created to solve.
C: Assessments are performed to determine the potential risks to a system. It does not test a system's compliance with design specifications and security requirements.
D: Accuracy is related to the integrity of information and systems. The integrity of information and systems requires that the information and systems remain accurate and reliable. This is ensured by preventing any unauthorized modification to the information or systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 23-24, 74-74, 1106
https://en.wikipedia.org/wiki/Verification_and_validation

QUESTION 530
Which of the following is a not a preventative control?

A. Deny programmer access to production data.
B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
To run a source comparison does not prevent any specific action from occurring.

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

To help review or design security controls, they can be classified by several criteria, for example according to the time that they act, relative to a security incident: ▪ Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders;
- During the event, detective controls are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;
- After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

Incorrect Answers:
A: Denying a programmer access to production data is an example of preventive control as it prevents the programmer from accessing the data.
B: To make a change request to include extra information would prevent unauthorized changes from being made.
D: By establishing procedure for emergency changes unauthorized changes could be prevented.

References:
https://en.wikipedia.org/wiki/Security_controls

QUESTION 531
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.
C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
An Intrusion Detection System (IDS) typically follows a two-step process. First procedures include inspection of the configuration files of a system to detect inadvisable settings; inspection of the password files to detect inadvisable passwords; and inspection of other system areas to detect policy violations.
In a second step, procedures are network-based and considered an active component; mechanisms are set in place to reenact known methods of attack and to record system responses.

Incorrect Answers:
B: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a routing vulnerability assessment.
C: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a host-based vulnerability assessment.
D: A network-based vulnerability assessment is referred to as an active vulnerability assessment, not a passive vulnerability assessment.
QUESTION 532

Which of the following answers best describes the type of penetration testing where the analyst has full knowledge of the network on which he is going to perform his test?

A. White-Box Penetration Testing
B. Black-Box Pen Testing
C. Penetration Testing
D. Gray-Box Pen Testing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
In general there are three ways a pen tester can test a target system.
▪ White-Box: The tester has full access and is testing from inside the system.
▪ Gray-Box: The tester has some knowledge of the system he's testing. ▪ Black-Box: The tester has no knowledge of the system.

Each of these forms of testing has different benefits and can test different aspects of the system from different approaches.

Incorrect Answers:
B: Black-Box Pen Testing: This is where no prior knowledge is given about the target network. Only a domain name or business name may be given to the analyst. This is not what is described in the question.
C: The term “Penetration Testing” does not specify what type of penetration testing is being performed.
D: With Gray-Box testing, the tester has some knowledge of the system he's testing. This is not what is described in the question.

QUESTION 533
Which one of the following is NOT one of the outcomes of a vulnerability assessment?

A. Quantative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Formal approval of BCP scope is not part of the vulnerability assessment. A vulnerability assessment identifies a wide range of vulnerabilities in the environment. Vulnerability assessments just find the vulnerabilities (the holes). A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Incorrect Answers:
A: Quantifying losses is part of the vulnerability assessment.
B: Prioritizing (qualifying) losses is part of the vulnerability assessment.
D: Identifying critical vulnerabilities is part of the vulnerability assessment.

References:
https://en.wikipedia.org/wiki/Vulnerability_assessment

QUESTION 534
Which of the following testing method examines internal structure or working of an application?

A. White-box testing
B. Parallel Test
C. Regression Testing
D. Pilot Testing

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
White-box testing is a method of testing software that tests internal structures or workings of an application, versus its functionality. White-box testing allows access to program source code, data structures, variables, etc.

Incorrect Answers:
B: Parallel Testing is the process of entering the same inputs in two different versions of the application and reporting the anomalies.
C: Regression Testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors.
D: Pilot Testing is a preliminary test that focuses on specific and predefined aspect of a system.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1105 https://en.wikipedia.org/wiki/White-box_testing

http://www.tutorialspoint.com/software_testing_dictionary/parallel_testing.htm http://soft-engineering.blogspot.co.za/2010/12/what-is-difference-between-pilot-and.html **QUESTION 535**
What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program.
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
C. A standalone workstation on which the password database is copied and processed by the cracking program.
D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.

Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.

Out of the four choice presented above this is the best choice.
However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choices presented.

Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.

Incorrect Answers:
A: The password cracking program should not be on a networked computer. This is a security risk as someone could access the computer over the network. Furthermore, you should not run the password cracking program on the live password database.
B: The password cracking program should not be on a networked computer. This is a security risk as someone could access the computer over the network.
D: Whether or not a password-cracking program is unethical depends on why you are cracking the passwords. Cracking passwords as a test of password strength is a valid security test.

QUESTION 536
Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.
B. Black-box testing uses the bottom-up approach.
C. White-box testing examines the program internal logical structure.
D. Black-box testing involves the business units

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
White box software testing gives the tester access to program source code, data structures, variables, etc.
White box testing gives the tester access to the internal logical structure of the program, while black box testing gives the tester no internal details: The software is treated as a black box that receives inputs.

Incorrect Answers:
A: White-box testing can be performed by any programmer who has access the source code.
B: Black-box testing just hides the internal details of the program. Black-box testing does not use either a bottom-up, or top down approach.
D: Black-box testing is blind to business units, as it has not access to any internal details of the program.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 194

QUESTION 537
Who should measure the effectiveness of Information System security related controls in an organization?

A. The local security specialist
B. The business manager
C. The systems auditor

D. The central security manager

Correct Answer: C
Section: Security Assessment and Testing
Explanation
Explanation/Reference:
Explanation:
The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met.
CobiT is a model that most information security auditors follow when evaluating a security program. The Control Objectives for Information and related Technology (CobiT) is a framework and set of control objectives developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and to ensure that IT maps to business needs.

Incorrect Answers:
A: A local security specialist could be hired to measure the effectiveness of Information System security related controls in an organization. However, in doing so, the local security specialist would be performing the role of systems auditor.
B: The business manager does not measure the effectiveness of Information System security related controls in an organization.
D: The central security manager could measure the effectiveness of Information System security related controls in an organization. However, in doing so, central security manager would be performing the role of systems auditor.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 55, 125

QUESTION 538
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:

Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives. Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible.
For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization. Senior management needs to define the scope of security and identify and decide what must be protected and to what extent.

Incorrect Answers:
A: IS security specialists may be the ones who implement the security measures; however, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.
C: Senior security analysts may be the ones who determine how to implement the security measures; however, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.
D: Systems Auditors ensure the appropriate security controls are in place. However, they do not bear the primary responsibility for determining the level of protection needed for information systems resources.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 101

QUESTION 539
Common Criteria has assurance level from EAL 1 to EAL 7 regarding the depth of design and testing. Which of following assure the Target of Evaluation (or TOE) is methodically designed, tested and reviewed?

A. EAL 3
B. EAL 4
C. EAL 5
D. EAL 6

Correct Answer: B
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Under the Common Criteria model, an evaluation is carried out on a product and it is assigned an *Evaluation Assurance Level (EAL).* The thorough and stringent testing increases in detailed-oriented tasks as the assurance levels increase. The Common Criteria has seven assurance levels. The range is from EAL1, where functionality testing takes place, to EAL7, where thorough testing is performed and the system design is verified. The different EAL packages are listed next: ▪ EAL1 Functionally tested
▪ EAL2 Structurally tested
▪ EAL3 Methodically tested and checked
▪ EAL4 Methodically designed, tested, and reviewed

- EAL5 Semi-formally designed and tested
- EAL6 Semi-formally verified design and tested
- EAL7 Formally verified design and tested

Incorrect Answers:
A: EAL3 is 'methodically tested and checked', not 'methodically designed, tested, and reviewed'.
C: EAL5 is 'semi-formally designed and tested, not 'methodically designed, tested, and reviewed'.
D: EAL6 is 'semi-formally verified design and tested, not 'methodically designed, tested, and reviewed'.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 402

QUESTION 540
Which Orange Book evaluation level is described as "Verified Design"?

A. A1.
B. B3.
C. B2.
D. B1.

Correct Answer: A
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Level A1 is "Verified Design".
A1: Verified Design: The architecture and protection features are not much different from systems that achieve a B3 rating, but the assurance of an A1 system is higher than a B3 system because of the formality in the way the A1 system was designed, the way the specifications were developed, and the level of detail in the verification techniques. Formal techniques are used to prove the equivalence between the TCB specifications and the security policy model. A more stringent change configuration is put in place with the development of an A1 system, and the overall design can be verified. In many cases, even the way in which the system is delivered to the customer is under scrutiny to ensure there is no way of compromising the system before it reaches its destination.
The type of environment that would require A1 systems is the most secure of secured environments. This type of environment deals with top-secret information and cannot adequately trust anyone using the systems without strict authentication, restrictions, and auditing.

Incorrect Answers:
B: Level B3 is "Security Domains", not "Verified Design".
C: Level B2 is "Structured Protection", not "Verified Design".
D: Level B1 is "Labeled Security", not "Verified Design".

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-397

QUESTION 541
Which Orange Book evaluation level is described as "Structured Protection"?

A. A1 B.
B3
C. B2
D. B1

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Level B2 is described as “Structured Protection”.
B2: Structured Protection The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
A: Level A1 is “Verified Design”, not “Structured Protection”.
B: Level B3 is “Security Domains”, not “Structured Protection”.
D: Level B1 is “Labeled Security”, not “Structured Protection”.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 395-397

QUESTION 542
What can be BEST defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence

Correct Answer: C
Section: Security Assessment and Testing
Explanation

Explanation/Reference:
Explanation:
Threat analysis is defined as the examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

Incorrect Answers:
A: Risk management is defined the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.
B: Risk analysis is defined as a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards.
D: Due diligence is the act of gathering the necessary information so the best decision-making activities can take place.

QUESTION 543
Operations Security seeks to PRIMARILY protect against which of the following?

A. object reuse
B. facility disaster
C. compromising emanations
D. asset threats

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Operations Security refers to the act of understanding the threats to and vulnerabilities of computer operations in order to routinely support operational activities that enable computer systems to function correctly. It also refers to the implementation of security controls for normal transaction processing, system administration

tasks, and critical external support operations. These controls can include resolving software or hardware problems along with the proper maintenance of auditing and monitoring processes.
Like the other domains, the Operations Security domain is concerned with triples — threats, vulnerabilities, and assets.

- A threat in the Operations Security domain can be defined as an event that could cause harm by violating the security. An example of an operations threat would be an operator's abuse of privileges, thereby violating confidentiality.
- A vulnerability is defined as a weakness in a system that enables security to be violated. An example of an operations vulnerability would be a weak implementation of the separation of duties.
- An asset is considered anything that is a computing resource or ability, such as hardware, software, data, and personnel.

Incorrect Answers:
A: Object Reuse is the concept of reusing data storage media after its initial use. Object reuse is one type of risk. Preventing object reuse alone is not the primary purpose of Operations Security.
B: Operations Security seeks to primarily protect against all types of asset threats. It does not seek to primarily protect against a single threat such as a facility disaster.
C: Operations Security does not seek to protect against a single threat such as compromising emanations. It protects all assets against all threats.
References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 302

QUESTION 544
The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

A. Preventative control.
B. Detective control
C. Compensating control
D. Corrective control

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The question states that you are looking at recorded events on closed-circuit TV camera. This is a detective control. The purpose of a detective control is to identify an incident's activities after it took place. Examples or detective controls are cameras, logs, investigations and IDS.

Incorrect Answers:

A: Preventative controls are intended to avoid an incident from occurring. In this question, the event has occurred. Therefore, this answer is incorrect. C: Compensating control are controls that provide an alternative measure of control. This is not what is described in the question. Therefore, this answer is incorrect.
D: Corrective controls fix components or systems after an incident has occurred. Watching camera footage does not fix anything. Therefore, this answer is incorrect.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 30

QUESTION 545
Which of the following questions is LESS likely to help in assessing identification and authentication controls?

A. Is a current list maintained and approved of authorized users and their access?
B. Are passwords changed at least every ninety days or earlier if needed?
C. Are inactive user identifications disabled after a specified period of time?
D. Is there a process for reporting incidents?

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Identification and authentication controls ensure standard security practices are adhered to. These include maintaining a list of authorized users and their access, password expiration and disabling inactive user accounts.
Incident reporting is not related to identification or authentication. Therefore, the question: “Is there a process for reporting incidents?” will not help in assessing identification and authentication controls.

Incorrect Answers:
A: Identification and authentication controls should include a maintained and approved list of authorized users and their access. Asking about this will help in assessing identification and authentication controls.
B: Identification and authentication controls should include a password expiration policy to ensure passwords are changed on a regular basis. Asking about this will help in assessing identification and authentication controls.
C: Identification and authentication controls should include inactive accounts being disabled. Asking about this will help in assessing identification and authentication controls.

QUESTION 546
Which of the following is NOT an example of an operational control?

A. Backup and recovery

B. Auditing
C. Contingency planning
D. Operations procedures

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
On the CISSP exam you can see control categories broken down into administrative, technical, and physical categories and the categories outlined by NIST, which are management, technical, and operational. You need to be familiar with both ways of categorizing control types. According to the NIST control categories, Auditing is in the Audit and Accountability Technical control group.

Operational controls are controls over the hardware, the media used and the operators using these resources.
Backup and recovery, contingency planning and operations procedures are operational controls.

Incorrect Answers:
A: Backup and recovery are listed under the Contingency Planning (CP) operational control group.
C: Contingency planning is a NIST operational control group.
D: Operations procedures are an example of an operational control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 58 http://infohost.nmt.edu/~sfs/Regs/sp800-53.pdf)

QUESTION 547
In what way can violation of clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.
B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.
C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.
D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.
Any violations recorded after the clipping level threshold is reached can be used to assist in violation tracking and analysis.

Incorrect Answers:
B: Clipping levels do not enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant. You would not record ONLY security relevant violations; when the number of violations reaches a defined threshold (the clipping level), all further violations would be recorded.
C: Clipping levels do not enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. All violations (after the clipping level has been reached) are recorded whether the user is a normal user or a privileged user.
D: Clipping levels do not enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations. This is not the function of clipping levels.

QUESTION 548
Which of the following control helps to identify an incident's activities and potentially an intruder?
A. Deterrent
B. Preventive
C. Detective
D. Compensating

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Detective control is an access control type that is effective during and after an attack. It is used to record and analyze the events of a breach to expose the source and target of the attack, the vulnerability targeted, and the specific tools and methodology used to commit the attack.

Incorrect Answers:
A: Deterrent controls discourage users from performing actions on a system.
B: Preventive controls stop actions from taking place.
D: A compensating control is an added security control put in place to counteract weaknesses in other controls.

References:
Conrad, Eric, Seth Misenar, Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 27, 28

QUESTION 549
Which of the following is NOT an example of preventive control?

A. Physical access control like locks and door
B. User login screen which allows only authorize user to access website
C. Encrypt the data so that only authorize user can view the same
D. Duplicate checking of a calculation

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Preventive Access Controls are intended to prevent an incident from occurring. Duplicate checking of a calculation is not an example of a preventive control.
Physical access control like locks and doors are an example of preventive/physical controls. These measures are intended to restrict the physical access to areas with systems holding sensitive information.
A user login screen which allows only authorized users to access a website is an example of preventive/technical control. The preventive/technical pairing uses technology to enforce access control policies. These technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Encrypting the data so that only authorized users can view it is another example of preventive/technical control. The preventive/technical pairing uses technology to enforce access control policies. Some typical preventive/technical controls are protocols, encryption, smart cards, biometrics (for authentication), local and remote access control software packages, call-back systems, passwords, constrained user interfaces, menus, shells, database views, limited keypads, and virus scanning software.

Incorrect Answers:
A: Physical access control like locks and doors are an example of preventive controls.
B: A user login screen which allows only authorized users to access a website is an example of preventive control.
C: Encrypting the data so that only authorized users can view it is an example of preventive control.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 49

QUESTION 550
Which of the following is NOT an example of a detective control?

A. System Monitor
B. IDS
C. Motion detector
D. Backup data restore

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Backup data restore is a Recovery/Technical control.

Incorrect Answers:
A, B, C: Detective controls include Motion detectors, Closed-circuit TVs, Monitoring and Supervising, Job rotation, Investigations, Audit logs, and IDS.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 32, 33

QUESTION 551
When attempting to establish liability, which of the following would be described as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?
A. Due care
B. Due concern
C. Due diligence
D. Due practice

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Due care is performing the ongoing maintenance necessary to keep something in proper working order, or to abide by what is commonly expected in a situation. This is especially important if the due care situation exists because of a contract, regulation, or law. The opposite of due care is "negligence."

EXAM TIP:

The Due Diligence refers to the steps taken to identify risks that exist within the environment. This is based on best practices, standards such as ISO 27001, ISO 17799, and other consensus. The first letter of the word Due and the word Diligence should remind you of this. The two letters are DD = Do Detect.
In the case of due care, it is the actions that you have taken (implementing, designing, enforcing, updating) to reduce the risks identified and keep them at an acceptable level. The same apply here, the first letters of the work Due and the work Care are DC. Which should remind you that DC = Do correct.

Incorrect Answers:
B: Due concern is not a valid answer. Due Care is what is described in the question.
C: Due diligence is performing reasonable examination and research before committing to a course of action. Basically, "look before you leap." In law, you would perform due diligence by researching the terms of a contract before signing it. The opposite of due diligence might be "haphazard" or "not doing your homework." This is not what is described in the question.
D: Due practice is not a valid answer. Due Care is what is described in the question.

QUESTION 552
Which of the following is NOT a critical security aspect of Operations Controls?

A. Controls over hardware.
B. Data media used.
C. Operators using resources.
D. Environmental controls.

Correct Answer: D
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
While it is important that environmental concerns are addressed they are part of the Physical Security Domain.
The Operations Security domain is concerned with the controls that are used to protect hardware, software, and media resources from the following: ▪ Threats in an operating environment
▪ Internal or external intruders
▪ Operators who are inappropriately accessing resources

Incorrect Answers:
A: Controls over hardware are a critical security aspect of Operations Controls.
B: Controls over the data media used are a critical security aspect of Operations Controls.
C: Controls over the operators using resources are a critical security aspect of Operations Controls.

References:
Krutz, Ronald L. and Russel Dean Vines, *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*, John Wiley & Sons, New York, 2001, p. 207

QUESTION 553
Which of the following is required in order to provide accountability?

A. Authentication
B. Integrity
C. Confidentiality
D. Audit trails

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the system and network. Audit trails can be used for intrusion detection and for the reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at the log-on time should notify the user of any monitoring that is being conducted.

Incorrect Answers:
A: Authentication is proof that a user is who they say they are. This is important in accountability. However, you also need to be able to monitor that user's actions. This is provided by audit trails.
B: Integrity ensures that data is consistent and not modified. This does not provide accountability.
C: Confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of data. This does not provide accountability.
References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 72

QUESTION 554
Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?

A. Anomaly detection tends to produce more data
B. A pattern matching IDS can only identify known attacks
C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
D. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Pattern matching and anomaly detection analysis activities do not work with packets.

Incorrect Answers:
A: Anomaly detection collects data on normal activities. This produces data.
B: A pattern matching IDS uses a signature database and attempts to match all monitored events to its contents. It can only detect known attacks that are present in the database.
D: Anomaly detection collects data on normal activities. Once it has accumulated enough data about normal activity, it can detect abnormal and possible malicious activities and events.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 56

QUESTION 555
Which of the following is NOT a characteristic of a host-based intrusion detection system?

A. A HIDS does not consume large amounts of system resources
B. A HIDS can analyze system logs, processes and resources
C. A HIDS looks for unauthorized changes to the system
D. A HIDS can notify system administrators when unusual events are identified

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
HIDS constantly monitors the system. This can consume quite a few resources.

Incorrect Answers:
B: A HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.
C: HIDS detects unauthorized changes to the system.
D: When a HIDS detect an anomaly it typically alerts the system administrator of the intrusion.

References:
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

QUESTION 556
Which of the following best describes signature-based detection?

A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behavior patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Models of how the attacks are carried out are developed and called signatures. Each identified attack has a signature, which is used to detect an attack in progress or determine if one has occurred within the network. Any action that is not recognized as an attack is considered acceptable.

Incorrect Answers:
A: Signature-based detection checks activities and events. It does check source codes.
B: Signature-based detection checks for patterns of old known attacks. It does not check for new unknown patterns of attacks.
D: Signature-based detection monitors activities and events, not objects.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 257

QUESTION 557
Which of the following questions is LEAST likely to help in assessing controls covering audit trails?

A. Does the audit trail provide a trace of user actions?
B. Are incidents monitored and tracked until resolved?
C. Is access to online logs strictly controlled?
D. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Audit trail controls are considered technical controls.
Monitoring and tracking of incidents is more an operational control related to incident response capability. Therefore, asking if incidents monitored and tracked until resolved will not help in assessing controls covering audit trails.

Incorrect Answers:
A: An audit trail should provide a trace of user actions. Asking about this will help in assessing controls covering audit trails.
C: Access to online logs should be strictly controlled. Asking about this will help in assessing controls covering audit trails.
D: There should be separation of duties between security personnel who administer the access control function and those who administer the audit trail. Asking about this will help in assessing controls covering audit trails.

QUESTION 558
What IDS approach relies on a database of known attacks?

A. Signature-based intrusion detection
B. Statistical anomaly-based intrusion detection
C. Behavior-based intrusion detection
D. Network-based intrusion detection

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A signature based IDS monitors packets and compares them against a database of signatures or attributes from known malicious threats.
Incorrect Answers:
B: An IDS which is anomaly based monitors network traffic and compares it against an established baseline, which identifies what is “normal” for that network, and the alerts the relevant party when traffic is detected which is significantly different to the baseline.
C: A statistical anomaly–based IDS is a behavioral-based system, which does not relies on a database of known attacks.
D: On-line network-based IDS monitors network traffic in real time and it analyses the Ethernet packet and applies it on the same rules to decide if it is an attack or not.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 258

QUESTION 559
An Intrusion Detection System (IDS) is what type of control?

A. A preventive control.
B. A detective control.
C. A recovery control.
D. A directive control.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Detective controls include Motion detectors, Closed-circuit TVs, Monitoring and Supervising, Job rotation, Investigations, Audit logs, and IDS.
Incorrect Answers:
A: Preventive controls include Locks, Badge system, Security guard, Security policy, Testing, ACLs, Encryption, and Smart cards.
C: Recovery controls include Offsite facility, and Data backup.
D: Directive controls, which are also known as administrative controls, include Security policy, Monitoring and Supervising, Separation of duties, Job rotation, Information Classification, Personnel Procedures, Testing, and Security-awareness training.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 32, 33

QUESTION 560
Which of the following is most appropriate to notify an external user that session monitoring is being conducted?

A. Logon Banners

B. Wall poster
C. Employee Handbook
D. Written agreement

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
Logon banners should be used to notify an external user that session monitoring is being conducted. This provides legal protection for the company.
A logon banner is text that appears on the computer screen when a user logs in to a system. By using a logon banner, the user cannot claim that he or she did not know that their session was being monitored.

B: A wall poster is not the most appropriate to notify an external user that session monitoring is being conducted. The user is external so he or she would not be able to see the poster.
C: An employee handbook is not the most appropriate to notify an external user that session monitoring is being conducted. The external user would not have access to the employee handbook.
D: A written agreement is not the most appropriate to notify an external user that session monitoring is being conducted. The user is external so he or she would not be able to read a written agreement.

QUESTION 561
What is the essential difference between a self-audit and an independent audit?

A. Tools used
B. Results
C. Objectivity
D. Competence

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
To maintain operational assurance, organizations use two basic methods: system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a self-audit and an independent audit is objectivity, thus indirectly affecting the results of the audit.

Incorrect Answers:
A: Internal and external auditors can use the same tools.
B: Internal and external auditors should return the same results. However, the objectivity of an independent audit may return more comprehensive results.
D: Internal and external auditors should have the same level of competence.

QUESTION 562
Which of the following is NOT a form of detective technical control?

A. Audit trails

B. Access control software
C. Honeypot
D. Intrusion detection system

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Access control software is an example of a preventive/technical control, not a detective/technical control.
By combining preventive and detective controls, types with the administrative, technical (logical), and physical means of implementation, the following pairings are obtained:

- Preventive/administrative
- Preventive/technical
- Preventive/physical
- Detective/administrative
- Detective/technical
- Detective/physical

The detective/technical control measures are intended to reveal the violations of security policy using technical means. These measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from “normal” operation or detect known signatures of unauthorized access episodes.
A honeypot is a system designed with the purpose of being attacked so that the attack can be monitored and the attack techniques noted. This is another example of a detective technical control.

Incorrect Answers:
A: Audit trails are an example of a detective/technical control.
C: A honeypot is an example of a detective/technical control.
D: An intrusion detection system is an example of a detective/technical control.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, pp. 48-50
QUESTION 563
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?

A. Intrusion Detection System
B. Compliance Validation System

C. Intrusion Management System (IMS)
D. Compliance Monitoring System

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An intrusion detection system (IDS) monitors network or system activities for malicious activities or policy violations and generates reports to a management station.

Incorrect Answers:
B: Compliance Validation is a formal procedure to determine how well an official or prescribed plan or course of action is being carried out.
C: Intrusion Management System (IMS) is not a valid type of system with regards to this exam.
D: Compliance Monitoring System is not a valid type of system with regards to this exam.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system
http://searchcompliance.techtarget.com/definition/compliance-validation

QUESTION 564
Which of the following monitors network traffic in real time?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
On-line network-based IDS monitors network traffic in real time and it analyses the Ethernet packet and applies it on the same rules to decide if it is an attack or not.

Incorrect Answers:

B: A host-based intrusion detection system (HIDS) monitors and analyzes the internals of a computing system, as well as the network packets on its network interfaces in certain instances.
C: An application-based IDS is designed to monitor a specific application.
D: Firewalls are different to IDS because it looks outwardly for intrusions in order to stop them from happening.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

QUESTION 565
What is the process that RAID Level 0 uses as it creates one large disk by using several disks?

A. striping
B. mirroring
C. integrating
D. clustering

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
With RAID Level 0 data is striped over several drives creating one single logical disk.

Incorrect Answers:
B: Mirroring is RAID Level 1 and uses only two disks.
C: There is not RAID Level named integrating.
D: There is not RAID Level named clustering.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 566
RAID Level 1 mirrors the data from one disk or set of disks using which of the following techniques?

A. Duplicating the data onto another disk or set of disks.

B. Moving the data onto another disk or set of disks.

C. Establishing dual connectivity to another disk or set of disks.
D. Establishing dual addressing to another disk or set of disks.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
With RAID Level 1 data are written to two drives at once. If one drive fails, the other drive has the exact same data available.

Incorrect Answers:
B: RAID Level 1 does not move data, it make two copies of it and stores it on two separate disks.
C: Dual connectivity is not used by any RAID level.
D: Dual addressing is not used by any RAID level.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 567
Which of the following stripes the data and the parity information at the block level across all the drives in the set?

A. RAID Level 5 B.
RAID Level 0 C.
RAID Level 2
D. RAID Level 1

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
With RAID level 5 data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.

Incorrect Answers:
B: RAID Level 0 does not use a parity bit. It just stripes data over several drives.
C: RAID Level 2 does not use block level parity. It uses hamming code parity.
D: RAID Level 1 does not use a parity bit. It uses mirroring of drives.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

QUESTION 568
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

A. server cluster.
B. client cluster.
C. guest cluster.
D. host cluster.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which provides immunity to faults and improves performance.

Incorrect Answers:
B: A cluster contains servers, not clients.
C: A guest cluster is referring to something more specific compared to a server cluster. For example, for Windows Server 2012, a failover cluster that is made up of two or more virtual machines is typically referred to as a guest cluster.
D: A host cluster is a more specific notion compared to server cluster, specifically, it is a type of web hosting.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1272

QUESTION 569
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:

A. server farm
B. client farm
C. cluster farm
D. host farm

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Clusters may also be referred to as server farms. If one of the systems within the cluster fails, processing continues because the rest pick up the load, although degradation in performance could occur.

Incorrect Answers:
B: A cluster contains servers, not clients.
C: A cluster and a cluster farm is not the same thing. A cluster is server farm.
D: A cluster and a host farm is not the same thing. A cluster is server farm.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1272

QUESTION 570
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In a full backup all data are backed up and saved to some type of storage media. From this baseline differential and incremental backups can later be made.

Incorrect Answers:
B: An incremental process backs up all the files that have changed since the last full or incremental backup.
C: A differential backup backs up the files that have been modified since the last full backup. When the data need to be restored, the full backup is laid down first, and then the most recent differential backup is put down on top of it.
D: A tape backup is any type of backup which backs up data to the tape medium. It can be a full backup, an incremental backup, or a differential backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 571
Which backup method is used if backup time is critical and tape space is at an extreme premium?

A. Incremental backup method.
B. Differential backup method.
C. Full backup method.
D. Tape backup method.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An incremental process backs up only the files that have changed since the last full or incremental backup. Compared to a differential or a full back, an incremental backup copies less files.

Incorrect Answers:
B: A differential backup backs up the files that have been modified since the last full backup. More files are copies compared to an incremental backup.
C: In a full backup all data are backed up and saved to some type of storage media.
D: A tape backup is any type of backup which backs up data to the tape medium. It can be a full backup, an incremental backup, or a differential backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 936

QUESTION 572
Hierarchical Storage Management (HSM) is commonly employed in:

A. very large data retrieval systems.
B. very small data retrieval systems.
C. shorter data retrieval systems.
D. most data retrieval systems.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
HSM (Hierarchical Storage Management) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. HSM is typically used in very large data retrieval systems.

Incorrect Answers:
B: HSM is typically not used in small data retrieval systems.
C: HSM is not used in small data retrieval systems.
D: Due to the added complexity of HSM, it is used only in very large data retrieval systems.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1274

QUESTION 573
Which of the following best describes what would be expected at a "hot site"?

A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The hot site would include computers, cables and peripherals.

A climate control system might be required as well as most electronic equipment must operate in a climate-controlled atmosphere.

Incorrect Answers:
B: Computer cables would be required as well.
C: Peripherals and cables would be required as well.
D: A hot site would require computers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 920

QUESTION 574
Which of the following computer recovery sites is only partially equipped with processing equipment?

A. hot site.
B. rolling hot site.
C. warm site.
D. cold site.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.

Incorrect Answers:
A: A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data.
B: A rolling hot site is a mobile facility, typically the back of an 18-wheel truck. It has all of the capabilities of a hot site and is very versatile, but expensive. Hot sites are fully equipped.
D: A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 575

Which of the following computer recovery sites is the least expensive and the most difficult to test?

A. non-mobile hot site.
B. mobile hot site.
C. warm site.
D. cold site.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A cold site is less expensive compared to a warm site or a hot site. A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site is essentially an empty data center.

Incorrect Answers:
A: A hot site is fully equipped and is therefore more expensive than a cold site.
B: A mobile (rolling) hot site is a mobile facility, typically the back of an 18-wheel truck. It has all of the capabilities of a hot site and is very versatile, but expensive.
C: A warm site is more expensive than a cold site, since it is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 576
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about, for example, tornado damage, because the backup site could also be affected or destroyed.

Incorrect Answers:
B: The alternate site should be too close so that one disaster does not take out both locations.
C: The alternate site should be too close so that one disaster does not take out both locations.
D: That the alternate city is convenient to airports and hotels is A major factor when considering an alternate site.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 924

QUESTION 577
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

A. hot site.
B. warm site.
C. cold site.
D. reciprocal agreement.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Reciprocal agreements are Enforceable. This means that although company A said company B could use its facility when needed, when the need arises, company A legally does not have to fulfill this promise.

Incorrect Answers:
A: A hot site contract is enforceable, while a reciprocal agreement could be hard to enforce.
B: A warm site contract is enforceable, while a reciprocal agreement could be hard to enforce.
C: A cold site contract is enforceable, while a reciprocal agreement could be hard to enforce.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 924

QUESTION 578
A Differential backup process will:

A. Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
B. Backs up data labeled with archive bit 1 and changes the data label to archive bit 0
C. Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
D. Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When a file is modified or created, the file system sets the archive bit to 1. A differential backup process backs up the files that have been modified since the last full backup, but does not change the archive bit value.

Incorrect Answers:
B: A differential backup process does not change the archive bit value.
C: Because a differential backup process backs up the files that have been modified since the last full backup, the archive bit at the start of the process would be set to 1.
D: Because a differential backup process backs up the files that have been modified since the last full backup, the archive bit at the start of the process would be set to 1.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 935-936

QUESTION 579
Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

The disaster recovery manager should direct short-term recovery actions immediately following a disaster.

Incorrect Answers:
A: The Chief Information Officer (CIO) does not handle disaster recovery.
As a CIO must make executive decisions regarding things such as the purchase of IT equipment from suppliers or the creation of new systems, they are therefore responsible to lead and direct the workforce of their specific organization. In addition, the CIO is 'required to have strong organizational skills'. This is particularly relevant for a Chief Information Officer of an organization, who must balance roles in order to gain a competitive advantage and keep the best interests of the organization's employees. CIOs also have the responsibility of recruiting, so it is important that they take on the best employees to complete the jobs the company needs fulfilling.
B: The Chief Operating Officer does Direct recovery actions following a disaster. The Chief Operating Officer is responsible for the daily operation of the company, and routinely reports to the highest ranking executive.
D: The Chief Executive Officer (CEO) does not handle disaster recovery. The CEO has responsibilities as a director, decision maker, leader, manager and executor.
References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 657

QUESTION 580
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?

A. Composition
B. Priorities
C. Dependencies
D. Service levels

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Data points obtained as part of the BIA information gathering process will be used later during analysis. It is important that the team members ask about how different tasks—whether processes, transactions, or services, along with any relevant dependencies—get accomplished within the organization.

Incorrect Answers:
A: To determine the dependencies, not the composition, between the business processes is an import step of the BIA process.
B: To determine the dependencies, not the priorities, between the business processes is an import step of the BIA process.
D: To determine the service levels, not the priorities, between the business processes is an import step of the BIA process.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 905

QUESTION 581
Which of the following recovery plan test results would be most useful to management?

A. elapsed time to perform various activities.
B. list of successful and unsuccessful activities.
C. amount of work completed.
D. description of each activity.

Correct Answer: B
Section: Security Operations
Explanation
Explanation/Reference:
The team of testers must agree upon what activities are getting tested and how to properly determine success or failure.

Incorrect Answers:
A: The key when testing the recovery plan is to know fail or success of the activities, not the elapsed time of them.
C: The recovery plan test refers to activities not to work completed.
D: The key when testing the recovery plan is to know fail or success of the activities, not the description time of time.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 954

QUESTION 582
Which of the following answers BEST indicates the most important part of a data backup plan?

A. Testing the backups with restore operations
B. An effective backup plan
C. A reliable network infrastructure
D. Expensive backup hardware

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
If you can't restore lost files from your backup system then your backup plan is useless. You could have the best backup system and plan available but if you are unable to restore files then the system cannot assure data availability.

Develop an effective disaster recovery plan and include in that plan a good backup strategy that meets the needs of your organization. Be sure to include periodic recovery practice operations to prove the effectiveness of the system.

Incorrect Answers:
B: This question is asking for the BEST answer for the most important part of a data backup plan. An effective backup plan is what you want; however the MOST IMPORTANT part of the backup plan is the ability to restore the data.
C: A reliable network infrastructure makes it easier to backup and restore your data. However, network reliability is not the MOST IMPORTANT part of a backup plan. The ability to restore the data is more important.
D: Expensive backup hardware is not the BEST answer. If your expensive backup hardware cannot restore your data, it is no good to you.

QUESTION 583
Fault tolerance countermeasures are designed to combat threats to which of the following?
A. an uninterruptible power supply.
B. backup and retention capability.
C. design reliability.
D. data integrity.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
One of the ways to provide uninterrupted access to information assets is through redundancy and fault tolerance. Redundancy refers to providing multiple instances of either a physical or logical component such that a second component is available if the first fails. Fault tolerance is a broader concept that includes redundancy but refers to any process that allows a system to continue making information assets available in the case of a failure.
Fault tolerance countermeasures are designed to combat threats to design reliability. Although fault tolerance can include redundancy, it also refers to systems such as RAID where if a disk fails, the data can be made available from the remaining disks.

Incorrect Answers:
A: Fault tolerance countermeasures ensure that data assets remain available in the event of a failure of any component, not just an uninterruptible power supply.
B: Fault tolerance countermeasures ensure that data assets remain available in the event of a failure of any component, not just the backup and retention capability. D: Fault tolerance countermeasures do not protect data integrity.

QUESTION 584

An incremental backup process

A. Backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
B. Backs up the files that been modified since the last full backup. It does not change the archive bit value.
C. Backs up all the data and changes the archive bit to 0.
D. Backs up all the data and changes the archive bit to 1.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The incremental backup method backs up all the files that have changed since the last full or incremental backup and resets the archive bit to 0. This is known as "clearing the archive bit". A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
The archive bit is used by the backup process to determine whether a file has been changed. When you modify a file or create a new file, the archive bit is set to 1. This tells the backups process that the file has changed (or is a new file) and needs to be backed up. When an incremental backup backs up the file, it sets the archive bit to 0. When the next incremental backup runs and sees that the archive bit is 0, the incremental backup knows that the file has not changed since the last backup and so will not back up the file again.

Incorrect Answers:
B: This answer describes the differential backup process. The differential backup does not change the archive bit value; an incremental backup does change the archive bit value to 0.
C: This answer describes the full backup process. An incremental backup does not back up ALL files; it only backs up changed files.
D: An incremental backup does not back up ALL files; it only backs up changed files. Furthermore, it changes the archive bit value to 0, not 1.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 801-802

QUESTION 585
A Differential backup process:

A. Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
B. Backs up data labeled with archive bit 1 and changes the data label to archive bit 0
C. Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
D. Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Correct Answer: A

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Archive bit 1 = On (the archive bit is set).
Archive bit 0 = Off (the archive bit is NOT set).

A full backup backs up all files regardless of whether the archive bit is 1 or 0 and sets the archive bit to 0.
When the archive bit is set to ON, it indicates a file that has changed and needs to be backed up. Differential backups back up all files that have changed since the last full backup - all files that have their archive bit value set to 1. Differential backups do not change the archive bit value when they backup a file; they leave the archive bit value set to 1.
Incorrect Answers:
B: Backs up data labeled with archive bit 1 and changes the data label to archive bit 0. - This is the behavior of an incremental backup, not a differential backup.
C: Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0. - If the archive bit is set to 0 (Off), it will only be backed up with a Full backup. Differential and incremental backups will not back up the file.
D: Backs up data labeled with archive bit 0 and changes the data label to archive bit 1. - If the archive bit is set to 0 (Off), it will only be backed up with a Full backup. Differential and incremental backups will not back up the file.
References:
https://en.wikipedia.org/wiki/Archive_bit

QUESTION 586
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?

A. Restore all files in preparation for the test.
B. Document expected findings.
C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Full Interruption Test is the most intrusive to regular operations and business productivity. The original site is actually shut down, and processing takes place at the alternate site. A parallel test is one in which some systems are actually run at the alternate site.

Incorrect Answers:

A: Restoration of files is not the most important when conducting a Full Interruption. The most important is to set up a secondary site and conduct a parallel test on that site.
B: To document expected findings is not the most important when conducting a Full Interruption. The most important is to set up a secondary site and conduct a parallel test on that site.
C: To arrange physical security for the test site is not the most important when conducting a Full Interruption. The most important is to conduct a parallel test on the test site.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 956

QUESTION 587
Organizations should not view disaster recovery as which of the following?

A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A discretionary expense is a cost which is Essential for the operation of a business. The disaster recovery is concerned with business functions and costs that are essential for the business, and does Address discretionary expense.

Incorrect Answers:
A: A committed expense is an unavoidable expensive. Disaster recovery must take unavoidable expenses into account.
C: The disaster recovery procedures must be in compliance with the law. D:
The disaster recovery procedures must be in compliance with regulations

References:
http://www.investopedia.com/terms/d/discretionary-expense.asp

QUESTION 588
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity

B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Physical controls are controls that pertain to controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and checking environmental controls.
Fencing (protecting the perimeter of the facility) is an example of a physical control.

Incorrect Answers:
A: Monitoring of system activity is an example of a technical control.
C: Identification and authentication methods are an example of a technical control.
D: Logical access control mechanisms are an example of a technical control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 28

QUESTION 589
Which of the following is a NOT a guideline necessary to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations?

A. Restrict access to main air intake points to persons who have a work-related reason to be there
B. Maintain access rosters of maintenance personnel who are not authorized to work on the system
C. Escort all contractors with access to the system while on site
D. Ensure that all air intake points are adequately secured with locking devices

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Over the past several years, there has been an increasing awareness dealing with anthrax and airborne attacks. Harmful agents introduced into the HVAC system can rapidly spread throughout the structure and infect all persons exposed to the circulated air.
The following is a list of guidelines necessary to enhance security in this critical aspect of facility operations:

- Restrict access to main air intake points to persons who have a work-related reason to be there.
- Escort all contractors with access to the system while on site.
- Ensure that all air intake points are adequately secured with locking devices.

Maintaining access rosters of maintenance personnel who are not authorized to work on the system is a recommended guideline; however, it is not a 'necessary' guideline to ensure safety.

Incorrect Answers:
A: Restricting access to main air intake points to persons who have a work-related reason to be there is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.
C: Escorting all contractors with access to the system while on site is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.
D: Ensuring that all air intake points are adequately secured with locking devices is a necessary guideline to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations. Therefore, this answer is incorrect.

QUESTION 590
Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems
B. Acceptability of biometrics systems
C. Availability of biometrics systems
D. Adaptability of biometrics systems

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:
A: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of accountability of biometrics systems.
C: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of availability of biometrics systems.
D: Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are not elements of adaptability of biometrics systems.

References:

Krutz, Ronald L. and Russell Dean Vines, *The CISSP and CAP Prep Guide: Mastering CISSP and CAP*, Wiley Publishing, Indianapolis, 2007, p. 60

QUESTION 591
The Orange Book requires auditing mechanisms for any systems evaluated at which of the following levels?

A. C1 and above.
B. C2 and above.
C. B1 and above.
D. B2 and above.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The Orange Book provides a classification system that is divided into hierarchical divisions of assurance levels:
A. Verified protection
B. Mandatory protection
C. Discretionary protection
D. Minimal security

Classification A represents the highest level of assurance, and D represents the lowest level of assurance. Each division can have one or more numbered classes with a corresponding set of requirements that must be met for a system to achieve that particular rating. The classes with higher numbers offer a greater degree of trust and assurance. So B2 would offer more assurance than B1, and C2 would offer more assurance than C1. Each division and class incorporates the requirements of the ones below it. This means that C2 must meet its criteria requirements and all of C1's requirements, and B3 has its requirements to fulfill along with those of C1, C2, B1, and B2.
C2: Controlled Access Protection Users need to be identified individually to provide more precise access control and auditing functionality. Logical access control mechanisms are used to enforce authentication and the uniqueness of each individual's identification. Security-relevant events are audited, and these records must be protected from unauthorized modification.

Incorrect Answers:
A: Auditing mechanisms are not required for systems at C1 level.
C: Auditing mechanisms are at C2 level which is lower than B1.
D: Auditing mechanisms are at C2 level which is lower than B2.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 392-395

QUESTION 592
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Orange Book Pages 15 states:
2.1.3.1.2 System Integrity:
Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Incorrect Answers:
A: The requirement for security testing: The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. This is not what is described in the question.
B: There are five requirements defined for design verification. The statement in the question is not one of those five requirements.
D: The statement in the question is not one of the requirements for System Architecture Specification.
References:
http://csrc.nist.gov/publications/history/dod85.pdf, pp. 15, 101

QUESTION 593
Covert Channel Analysis is FIRST introduced at what level of the TCSEC rating?

A. C2 and above.
B. B1 and above.C. B2 and above.
D. B3 and above.

Correct Answer: C

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In the Orange Book, covert channels in operating systems are not addressed until security level B2 and above because these are the systems that would be holding data sensitive enough for others to go through all the necessary trouble to access data in this fashion.

B2: Structured Protection: The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system **must not allow covert channels**. A trusted path for logon and authentication processes must be in place, which means the subject communicates directly with the application or operating system, and no trapdoors exist. There is no way to circumvent or compromise this communication channel. Operator and administration functions are separated within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The type of environment that would require B2 systems is one that processes sensitive data that require a higher degree of security. This type of environment would require systems that are relatively resistant to penetration and compromise.

Incorrect Answers:
A: Covert Channel Analysis is not used at layer C2.
B: Covert Channel Analysis is not used at layer B1.
D: B3 is not the lowest level that uses Covert Channel Analysis. Level B2 uses Covert Channel Analysis.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 380, 396

QUESTION 594
Which of the following is most concerned with personnel security?
A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

On the CISSP exam you can see control categories broken down into administrative, technical, and physical categories and the categories outlined by NIST, which are management, technical, and operational. You need to be familiar with both ways of categorizing control types.

According to the NIST control categories, Personnel Security is an Operational control.

Incorrect Answers:
A: Personnel security is not a management control.
C: Personnel security is not a technical control.
D: Human resources controls are not a defined control category although there are human resource controls listed in the administrative control category.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 58

QUESTION 595
Which of the following backup sites is the most effective for disaster recovery?

A. Time brokers
B. Hot sites
C. Cold sites
D. Reciprocal Agreement

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Hot sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible. The only missing resources from a hot site are usually the data. A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours.
Incorrect Answers:
A: A time brokers backup solution would be less effective compared to hot or cold sites.
C: A cold site is less effective than a hot site since the cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site is essentially an empty data center.
D: Reciprocal agreements are less effective compared to hot or cold sites, since reciprocal agreements are Enforceable. This means that although company A said company B could use its facility when needed, when the need arises, company A legally does not have to fulfill this promise.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 596
Which of the following is a transaction redundancy implementation?

A. On-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
On-site mirroring is a transaction redundancy solution.

Incorrect Answers:
B: Electronic vaulting is one type of transaction redundancy solution. Electronic vaulting makes copies of files as they are modified and periodically transmits them to an offsite backup site.
C: Remote journaling is one type of transaction redundancy solution. Remote journaling is a method of transmitting data offsite. It usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data.
D: Database Shadowing is one type of transaction redundancy solution. It is a mirroring technology used in databases, in which information is written to at least two hard drives for the purpose of redundancy.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 938-939

QUESTION 597
A site that is owned by the company and mirrors the original production site is referred to as a _____?
A. Hot site.
B. Warm Site.
C. Reciprocal site.
D. Redundant Site.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A redundant site is owned by the company and is a mirror of the original production environment.

Incorrect Answers:
A: A hot site is not owned by the company. A hot site is leased or rented.
B: A warm site is a leased or rented facility. It is not owned by the company.
C: A reciprocal site is owned by another company, and is set up through a reciprocal agreement. A reciprocal agreement is one in which a company promises another company it can move in and share space if it experiences a disaster, and vice versa.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 925

QUESTION 598
Which of the following is the most critical item from a disaster recovery point of view?

A. Data
B. Hardware/Software
C. Communication LinksD. Software Applications

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Data loss has the most negative impact on business functions. Data loss often lead to business failure.

Incorrect Answers:
B: Software can be reinstalled and hardware can replaced, and are therefore less critical compared to loss of data.
C: Communication links can quite easily put back again, compared to loss of data.
D: Loss of applications is Critical as they can be reinstalled.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 957

QUESTION 599
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Recovery Point Objective (RPO) is the maximum period of time in which data might be lost if a disaster strikes. It is the most recent point in time to which data must be synchronized to avoid major negative impact on the organization.

Incorrect Answers:
B: The Recovery Time Objective is the amount of time in which you think you can feasibly recover the function in the event of a disruption.
C: There is no Point of Time Objective within the CISSP framework.
D: There is no Critical Time Objective within the CISSP framework.

QUESTION 600
Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organization
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. A cold site cannot provide a quick recovery. A warm site is needed for a quick recovery.

Incorrect Answers:
A: A cold site is a separate site and would Be a resource contention with another company.

C: A cold site is located at another location where the original site can be reconstructed.
D: Compared to a hot site, or a warm site, a cold site has a lower cost.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 601
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is known as?

A. Shadowing
B. Data mirroring
C. Backup
D. Archiving

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Database Shadowing is one type of transaction redundancy solution whereby a full copy of the user's database is maintained at an alternate information processing facility.

Incorrect Answers:
B: Data mirroring does not necessarily use a remote location. Data mirroring mirrors data to another server, or to another hard drive on the same server, on the local network.
C: A backup solution would not handle database records. It handles data at the file level.
D: An archiving solution would not handle database records. It handles data at the file level.

References:
http://www.bcmpedia.org/wiki/Database_Shadowing

QUESTION 602
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site
B. Warm Site

C. Internal Hot Site
D. Dual Data Center

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
An internal hot site is standby ready with all the technology and equipment necessary to run the applications to be recovered there.

Incorrect Answers:
A: An external hot site has equipment on the floor waiting for recovery, but the environment must be rebuilt for the recovery. An external hot site is not standby ready.
B: A warm site is not standby ready. A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.
D: A dual data center is employed for application that canAccept any downtime without unacceptably impacting the business. A dual data center would be more than standby ready, but it would be more expensive.

QUESTION 603
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You move items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Correct Answer: C
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
The salvage team must ensure the reliability of primary site. This is done by returning the least-mission-critical processes to the restored original site to stress – test the rebuilt network. As the restored site shows resiliency, more important processes are transferred.

Incorrect Answers:

A: The most critical operations should be to the primary site after, Before, the other less critical operations have been moved.
B: As many operations that the salvage team handles are the same as the operations carried out by the disaster recovery team, there can be very well be an overlap between the team members. A person can be a member of both teams.
D: The order in which the operations are restored should Be exactly the same order in which the operations where moved to the alternative site. You should transfer the least critical operations first.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 669

QUESTION 604
Which of the following is a large hardware/software backup system that uses the RAID technology?

A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Cheyenne Software (now owned by Computer Associates) was the first to offer RAID 5 for tape devices. Because by nature tape devices employ a sequential access method, RAID 5 is an ideal solution for a tape array.

Incorrect Answers:
B: A scale array is A RAID backup system.
C: A crimson array is A RAID backup system.
D: A table array is A RAID backup system.

QUESTION 605
What is the MOST critical piece to disaster recovery and continuity planning?
A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The most critical part of establishing and maintaining a current continuity plan is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support.

Incorrect Answers:
A: Compared to get management support for the plan, security policy is less important.
C: Compared to get management support for the plan, availability of backup facilities is less important.
D: Compared to get management support for the plan, staff training is less important.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 897

QUESTION 606
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Once you develop a list of threats, you must individually evaluate each threat and its related risk. There are two risk assessment methodologies: quantitative and qualitative. Quantitative risk analysis assigns real dollar figures to the loss of an asset.

Incorrect Answers:
A: Accuracy is not measured. It is the list of threats that are quantitative measured.
B: Elapsed time for completion of critical tasks is Critical. It is critical to evaluate the risks.
D: the observed test results are Evaluated. The business function either passes or fails the test.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 243

QUESTION 607
Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.
C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The physical access restrictions at the off-site facility does Be at same level as at the original site.

Incorrect Answers:
B: An off-site location which is close would be ill-advised as the same disaster can strike both the main site and the alternate site. C: The off-site facility must be readily accessed and should be easily identified from the outside. D: The same operational environment should be possible at the alternate location.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 444

QUESTION 608
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:

A. Availability of the CIA triad
B. Confidentiality of the CIA triad
C. Integrity of the CIA triad
D. Availability, Confidentiality and Integrity of the CIA triad

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Availability is one of the main themes behind business continuity planning, in that it ensures that the resources required to keep the business going will continue to be available to the people and systems that rely upon them.
Note: The CIA Triad, primary goals and objectives of security, is the three essential security principles of confidentiality, integrity, and availability. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principles.

Incorrect Answers:
B: Business Continuity and Disaster Recovery Planning primarily addresses availability, Confidentiality.
C: Business Continuity and Disaster Recovery Planning primarily addresses availability, not integrity.
D: Business Continuity and Disaster Recovery Planning primarily addresses availability, , Confidentiality or integrity.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 888

QUESTION 609
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.
D. An organization that disseminates incident-related information to its constituency and other involved parties.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs).
Note: When an incident occurs, the response team has four primary responsibilities:
- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident - related damages.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Incorrect Answers:
A: The CSIRT is not set up to receive reports on security incidents. The CSIRT handles the security incidents when they occur.

B: The CSIRT is not set up to alert authorities of security incidents. The CSIRT handles the security incidents when they occur.
D: The CSIRT is not set up to inform on security incidents. The CSIRT handles the security incidents when they occur.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 726

QUESTION 610
If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification
B. Analysis
C. Storage, preservation, and transportation
D. Destruction

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The evidence lifecycle does not include destruction. The evidence need to be preserved.

Incorrect Answers:
A: The evidence lifecycle include collection and identification of evidence.
B: Analysis of evidence is included in the evidence lifecycle.
C: The evidence lifecycle include storage, preservation, and transportation of evidence.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1054

QUESTION 611
If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.
B. Inform all employees that e-mail is being monitored.
C. Explain who can read the e-mail and how long it is backed up.

D. Explain what is considered an acceptable use of the e-mail system.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
All the employees should be monitored, not only a few.

Incorrect Answers:
B: If a company feels it may be necessary to monitor e-mail messages and usage, this must be explained to the employees.
C: The company should outline who can and cannot read employee messages, describe the circumstances under which e-mail monitoring may be acceptable, and specify where the e-mail can be accessed.
D: The company should state which e-mail activity is acceptable.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1020

QUESTION 612
A server farm consisting of multiple similar servers seen as a single IP address from users interacting with the group of servers is an example of which of the following?

A. Server clustering
B. Redundant servers
C. Multiple servers
D. Server fault tolerance

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system through a single IP address.

Incorrect Answers:
B: Redundant servers are not grouped together and can be managed through a single IP address.
C: In general, a group of multiple servers can be grouped together and managed through a single IP address.

D: Server fault tolerance is not related to managing a group of servers through a single IP address.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1272

QUESTION 613
Which of the following is NOT a common backup method?

A. Full backup method
B. Daily backup method
C. Incremental backup method
D. Differential backup method

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
You can have daily backup schedule, but there is no specific backup method called daily backup.

Incorrect Answers:
A: The full backup method copies all the data from the system to the backup medium.
C: The incremental backup method copies only the files that have been modified since the previous backup.
D: The differential backup method is a type of data backup that preserves data, saving only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 614
Which common backup method is the fastest on a daily basis?

A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method

Correct Answer: B

Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
An incremental backup is fast because it copies only the files that have been modified since the previous backup.

Incorrect Answers:
A: A full backup is not fast as it copies all the data from the system to the backup medium.
C: There is no backup method called the fast backup method.
D: A differential backup is slower than an incremental backup since it copies more data. A differential backup copies only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 615
Which of the following backup methods is most appropriate for off-site archiving?

A. Incremental backup method
B. Off-site backup method
C. Full backup method
D. Differential backup method

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

All data should be archived. A full backup copies all the data from the system to the backup medium. After the full backup has finished, the backup media is physically transported to another off-site location.

Incorrect Answers:
A: Archiving should copy all the data, but an incremental backup copies only the files that have been modified since the previous backup.
B: There is no special off-site backup method. Instead use a standard full backup and transport the backup media to the other site.
D: Archiving should copy all the data, but a differential backup copies only the difference in the data since the last full backup.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 616
Which of the following statements pertaining to RAID technologies is incorrect?

A. RAID-5 has a higher performance in read/write speeds than the other levels.
B. RAID-3 uses byte-level striping with dedicated parity.
C. RAID-0 relies solely on striping.
D. RAID-4 uses dedicated parity.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
RAID-0 is faster than RAID-5 since RAID-0 is striping without parity, while RAID-5 uses parity which makes it slower.

Incorrect Answers:
B: RAID-3 uses byte-level parity. The Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.
C: With RAID-0 the data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.
D: RAID-4 uses block-level parity. The Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1270

QUESTION 617
A contingency plan should address:

A. Potential risks. B.
Residual risks.
C. Identified risks.
D. All answers are correct.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Contingency plans are developed as a result of a risk being identified. Contingency plans are pre-defined actions plans that can be implemented if identified risks actually occur. One type of identified risk is a residual risk. Residual risks are those risks that are expected to remain after implementing the planned risk response, as well as those that have been deliberately accepted.
A contingency plan should address the risks found during risk assessment. Risk assessment includes both the identification of potential risk and the evaluation of the potential impact of the risk.

Incorrect Answers:
A: Contingency plans should not just address potential risks. It should address identified risks and residual risks as well.
B: Contingency plans should not just address residual risks. It should address identified risks and potential risks as well.
C: Contingency plans should not just address identified risks. It should address potential risks and residual risks as well.

QUESTION 618
Which of the following focuses on sustaining an organization's business functions during and after a disruption?

A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained.

Incorrect Answers:
B: A recovery plan is focused on what actions to take after the disruption, while a Business continuity plan also includes procedures to keep critical business functions working during a disruption.
C: The plan that keeps the business functions operating during a disruption is not named continuity of operations plan; it is called a Business continuity plan. D: A Disaster recovery plan is a plan developed to help a company recover from a disaster. It does not include operations to sustain business functions during a disruption.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 961

QUESTION 619

Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?

A. Risk assessment
B. Residual risks
C. Security controls
D. Business units

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A risk assessment is a critical part of the disaster recovery planning process. In disaster recovery planning, once you've completed a business impact analysis (BIA), the next step is to perform a risk assessment.
Once risks and vulnerabilities have been identified, i.e. after the risk assessment has been completed, four types of defensive responses can be considered: Protective measures Mitigation measures
Recovery activities
Contingency plans

Incorrect Answers:
B: Contingency plans depend on risk assessments, not on residual risks. The residual risk is remaining risk after the security controls have been applied. C: Contingency plans depend on risk assessments, not on Security controls. D: Contingency plans depend on risk assessments, not on Business units.

References:
http://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT-risk-assessment-template-and-guide

QUESTION 620
Failure of a contingency plan is usually:

A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Failure of the contingency plan is usually considered as a management failure.

Incorrect Answers:
A: A technical failure is not usually thought to be a failure of the contingency plan.
C: A lack of awareness is not usually thought to be a failure of the contingency plan.
D: Lack of training is not usually thought to be a failure of the contingency plan.

QUESTION 621
A business continuity plan is an example of which of the following?

A. Corrective control
B. Detective control
C. Preventive control
D. Compensating control

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A corrective control, such as business continuity plan (BCP), consists of instructions, procedures, or guidelines used to reverse the effects of an unwanted activity, such as attacks or errors. In particular a BCP is the assessment of a variety of risks to organizational processes and the creation of policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur.

Incorrect Answers:
B: A business continuity plan is A detective control. A detective control is an access control deployed to discover unwanted or unauthorized activity. Examples of detective access controls include security guards, supervising users, incident investigations, and intrusion detection systems (IDSs).
C: A preventive control is any security mechanism, tool, or practice that can deter and mitigate undesirable actions or events. A business continuity plan is A preventive control.
D: A compensating control is a data security measure that is designed to satisfy the requirement for some other security measure that is deemed too difficult or impractical to implement. A business continuity plan is A compensating control.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p.
14

QUESTION 622
Which of the following statements pertaining to disaster recovery is incorrect?

A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.
C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.
D. When returning to the primary site, the most critical applications should be brought back first.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The salvage team must ensure the reliability of primary site. This is done by returning the least-mission-critical processes to the restored original site to stress – test the rebuilt network. As the restored site shows resiliency, more important processes are transferred.

Incorrect Answers:
A: The restoration team should be responsible for getting the alternate site into a working and functioning environment
B: The salvage team must ensure the reliability of primary site by returning it to normal processing conditions.
C: Within the recovery plan the salvage team is responsible for starting the recovery of the original site. The recovery plan must include how the original site is recovered.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 669

QUESTION 623
For which areas of the enterprise are business continuity plans required?

A. All areas of the enterprise.
B. The financial and information processing areas of the enterprise.
C. The operating areas of the enterprise.
D. The marketing, finance, and information processing areas.

Correct Answer: A
Section: Security Operations
Explanation
Explanation/Reference:
Explanation:
A Business Impact Analysis (BIA) is performed at the beginning of business continuity planning to identify all the areas of the enterprise that would suffer the greatest financial or operational loss in the event of a disaster or disruption.
Incorrect Answers:
B: All areas of the operations must be considered, not only the financial an information processing areas.
C: All areas of the operations must be considered, not only the operating areas.
D: All areas of the operations must be considered, not only the marketing, finance, and information processing areas.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 911

QUESTION 624
Which of the following will a Business Impact Analysis NOT identify?

A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
B. Systems critical to the survival of the enterprise.
C. The names of individuals to be contacted during a disaster.
D. The outage time that can be tolerated by the enterprise as a result of a disaster.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Business Impact Analysis (BIA) does not identify persons that should be contacted during a disaster.

Incorrect Answers:
A: A Business Impact Analysis (BIA) is performed at the beginning of business continuity planning to identify all the areas of the enterprise that would suffer the greatest financial or operational loss in the event of a disaster or disruption.
B: The BIA identifies the company's critical systems needed for survival.
D: The BIA estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 911

QUESTION 625
What is a hot-site facility?

A. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
B. A site in which space is reserved with pre-installed wiring and raised floors.
C. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
D. A site with readymade work space with telecommunications equipment, LANs, PCs, and terminals for work groups.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A hot site is a backup facility is maintained in constant working order, with a full complement of pre-installed servers and workstations, raised flooring, air conditioning, network equipment including communications links, and UPS ready to assume primary operations responsibilities.

Incorrect Answers:
B: A site in which space is reserved with pre-installed wiring and raised floors is called a cold site, A hot site.
C: A hot site includes pre-installed servers.
D: A hot site includes pre-installed servers.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 656

QUESTION 626
Which of the following best describes remote journaling?

A. Send hourly tapes containing transactions off-site.

B. Send daily tapes containing transactions off-site.
C. Real-time capture of transactions to multiple storage devices.
D. Real time transmission of copies of the entries in the journal of transactions to an alternate site.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Remote journaling is a method of transmitting data offsite. It usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data.
Incorrect Answers:
A: Remote journaling does not involve tapes that are sent on an hourly schedule.
B: Remote journaling does not involve tapes that are sent on a daily schedule.
C: Remote journaling send log files, not transactions, to a remote location.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 938-939

QUESTION 627
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would be considered an essential element of the BIA but an important topic to include within the BCP plan?

A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Public Relations is part of the BCP, but it is not part of the BIA. Public relations and Crisis Communication should be part of the BCP.

Incorrect Answers:
A: IT Network Support is part of both the BCP and the BIA.
B: Accounting is part of both the BCP and the BIA.
D: Purchasing is part of both the BCP and the BIA.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 905

QUESTION 628
Of the following, which is NOT a specific loss criteria that should be considered while developing a BIA?

A. Loss of skilled workers knowledge
B. Loss in revenue
C. Loss in profits
D. Loss in reputation

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Although a loss of skilled workers knowledge would cause the company a great loss, it is not identified as a specific loss criteria. It would fall under one of the three other criteria listed as distracters.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

QUESTION 629
Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continuous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Auditing would affect the Disaster Recovery plan.

Note: The main reasons Disaster Recovery plans become outdated include the following:
- Personnel turn over.
- Large plans take a lot of work to maintain.
- Changes occur to the infrastructure and environment.

Other reasons include:
- The business continuity process is not integrated into the change management process.
- Reorganization of the company, layoffs, or mergers occurs.
- Changes in hardware, software, and applications occur.
- After the plan is constructed, people feel their job is done.

Plans do not have a direct line to profitability.

Incorrect Answers:
A: Personnel turnover can make the Disaster Recovery plan outdated.
B: Large plans take a lot of work to maintain can make the Disaster Recovery plan outdated.
C: Changes that occur to the infrastructure and environment can make the Disaster Recovery plan outdated.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 958

QUESTION 630
Which backup type run at regular intervals would take the least time to complete?

A. Full Backup
B. Differential Backup
C. Incremental Backup
D. Disk Mirroring

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

An incremental backup copies only the files that have been modified since the previous backup. An incremental backup copies less data compared to full and differential backups.

Incorrect Answers:
A: A full backup copies all the data from the system to the backup medium. It copies more data compared to an incremental backup.
B: A differential backup is a type of data backup that preserves data, saving only the difference in the data since the last full backup. But a differential backup copies more data compared to an incremental backup.
D: Disk mirroring works dynamically in real-time. Disk mirroring does not take place at regular intervals.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 1410

QUESTION 631
What is electronic vaulting?

A. Information is backed up to tape on a hourly basis and is stored in an on-site vault.
B. Information is backed up to tape on a daily basis and is stored in an on-site vault.
C. Transferring electronic journals or transaction logs to an off-site storage facility
D. A transfer of bulk information to a remote central backup facility.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Electronic vaulting makes copies of files as they are modified and periodically transmits them in a bulk to an offsite backup site.

Incorrect Answers:
A: Electronic vaulting does not use tape backup on an hourly basis.
B: Electronic vaulting does not use tape backup on a daily basis.
C: Electronic vaulting copies data files not transaction logs. Remote journaling transfer log files.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, pp. 938-939

QUESTION 632
After a company is out of an emergency state, what should be moved back to the original site first?

A. Executives

B. Least critical components
C. IT support staff
D. Most critical components

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The salvage team must ensure the reliability of primary site. This is done by returning the least-mission-critical processes to the restored original site to stress – test the rebuilt network. As the restored site shows resiliency, more important processes are transferred.

Incorrect Answers:
A: There is no priority to move the Executives back to the original site fast. The salvage team, not the Executives brings the original site back in order.
C: The salvage team, not the IT support staff brings the original site back in order. There is no priority to move the IT support staff back to the original site fast.
D: The most critical operations should be to the primary site after, before, the other less critical operations have been moved.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 669

QUESTION 633
How often should tests and disaster recovery drills be performed?

A. At least once a quarter
B. At least once every 6 months
C. At least once a year
D. At least once every 2 years

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The drills should take place at least once a year, and the entire program should be continually updated and improved.

Incorrect Answers:

A: Once a quarter would be too much. Once a year is fine.
B: Once every 6 months would be too much. Once a year is fine.
D: Once every 2 years would Be enough. Once a year is the recommended frequency.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 951

QUESTION 634
A business impact assessment is one element in business continuity planning. What are the three primary goals of a BIA?

A. Data processing continuity planning, data recovery plan maintenance, and testing the disaster recovery plan.
B. Scope and plan initiation, business continuity plan development, and plan approval and implementation.
C. Facility requirements planning, facility security management, and administrative personnel controls.
D. Criticality prioritization, downtime estimation, and resource requirements.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The first business impact assessment (BIA) task facing the BCP team is identifying business priorities. The second quantitative measure that the team must develop is the maximum tolerable downtime (MTD). The final step of the BIA is to prioritize the allocation of business continuity resources to the various risks that you identified and assessed in the preceding tasks of the BIA.
Incorrect Answers:
A: Continuity planning and data recovery planning are not part of the BIA.
B: Business continuity plan development is not part of the BIA.
C: Facility planning is not part of the BIA.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 623-624

QUESTION 635
Business Continuity Planning (BCP) is defined as a preparation that facilitates:

A. the rapid recovery of mission-critical business operations
B. the continuation of critical business functions
C. the monitoring of threat activity for adjustment of technical controls

D. the reduction of the impact of a disaster

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The BCP is concerned with monitoring threat activity.

Incorrect Answers:
A: One goal of BCP is to enhance a company's ability to recover from a disruptive event promptly.
B: BCP is used to maintain the continuous operation of a business in the event of an emergency situation.
D: The goal of BCP planners is to implement a combination of policies, procedures, and processes such that a potentially disruptive event has as little impact on the business as possible.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 612

QUESTION 636
During a test of a disaster recovery plan the IT systems are concurrently set up at the alternate site. The results are compared to the results of regular processing at the original site. What kind of testing has taken place?
A. Simulation
B. Parallel
C. Checklist
D. Full interruption

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In a parallel test the employees are relocated to the site perform their disaster recovery responsibilities just as they would for an actual disaster. The only difference is that operations at the main facility are not interrupted. That site retains full responsibility for conducting the day - to - day business of the organization.

Incorrect Answers:

A: A simulation test does not use an alternate site. In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response.
C: In a checklist test you simply distribute copies of disaster recovery checklists to the members of the disaster recovery team for review. You do not set up an alternate site.
D: Full - interruption tests actually shut down operations at the primary site and shifting them to the recovery site.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 671

QUESTION 637
During a business impact analysis it is concluded that a system has maximum tolerable downtime of 2 hours. What would this system be classified as?

A. Important
B. Urgent
C. Critical
D. Vital

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A classification of critical has a maximum tolerable downtime (MTD) in minutes to hours, such as 2 hours.
Incorrect Answers:

A: A classification as Important would have a MTD of around 72 hours.
B: A classification as urgent would have a MTD of around 24 hours.
D: There is no MTD classification named vital. The classifications are Nonessential (30 days), Normal (7 days), Important (72 hours), Urgent (24 hours), and Critical/Essential (minutes to hours).

References:
http://docplayer.net/1184175-Cissp-common-body-of-knowledge-business-continuity-disaster-recovery-planning-domain-version-5-9-2.html

QUESTION 638
Business Impact Analysis (BIA) is about:

A. Technology

B. Supporting the mission of the organization
C. Due Care
D. Risk Assessment

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Business Impact Assessment (BIA) supports the mission of the organization by identifying the resources that are critical to an organization's ongoing viability and the threats posed to those resources. The BIA also assesses the likelihood that each threat will actually occur and the impact those occurrences will have on the business.

Incorrect Answers:
A: BIA is about critical business functions, and about technology.
C: While due care concerns using reasonable care to protect the interests of an organization, BIA is about supporting the mission of the organization.
D: BIA is about risk assessment. A BIA often takes place prior to a risk assessment. The BIA focuses on the effects or consequences of the interruption to critical business functions and attempts to quantify the financial and non-financial costs associated with a disaster. The business impact assessment looks at the parts of the organization that are most crucial.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 825

QUESTION 639
What is the MOST important step in business continuity planning?

A. Risk Assessment
B. Due Care
C. Business Impact Analysis (BIA)
D. Due Diligence

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:

Explanation:
In order to develop the in business continuity planning (BCP), the scope of the project must be determined and agreed upon. This involves some distinct milestones including Conduct the business impact analysis (BIA). The BIA helps to identify and prioritize critical IT systems and components.

Incorrect Answers:
A: Risk assessment is part of the business continuity planning, but it is less important compared to the BIA.
B: Due care is not the most important to the business continuity planning. Due care concerns using reasonable care to protect the interests of an organization.
D: Due diligence is A factor for continuity planning. Due diligence is an investigation of a business or person prior to signing a contract, or an act with a certain standard of care.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 356

QUESTION 640
You have been tasked with developing a Business Continuity Plan/Disaster Recovery (BCP/DR) plan. After several months of researching the various areas of the organization, you are ready to present the plan to Senior Management.

During the presentation meeting, the plan that you have dutifully created is not received positively. Senior Management is convinced that they need to enact your plan, nor are they prepared to invest any money in the plan.

What is the BEST reason, as to why Senior Management is not willing to enact your plan?

A. The business case was not initially made and thus did not secure their support.
B. They were not included in any of the Risk Assessment meetings.
C. They were not included in any of the Business Impact Assessment meetings.
D. A Business Impact Assessment was not performed.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The most critical part of establishing and maintaining a current continuity plan is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support.

In order to convince Senior Management of the viability of the plan you need to convince them of the business case. The Senior Management usually wants information stated in monetary, quantitative terms, not in subjective, qualitative terms.

Incorrect Answers:
B: Senior Management does not need to attend the Risk Assessment meetings.
C: Senior Management does not need to attend the Business Impact Assessment meetings.
D: The Business Impact Assessment is made after the BCP plan has been approved. To make a Business Impact Assessment the BCP team must sit down and discuss, preferably with the involvement of senior management, qualitative concerns to develop a comprehensive approach that satisfies all stakeholders.

QUESTION 641
When planning for disaster recovery it is important to know a chain of command should one or more people become missing, incapacitated or otherwise available to lead the organization.

Which of the following terms BEST describes this process?

A. Succession Planning
B. Continuity of Operations
C. Business Impact Analysis
D. Business Continuity Planning

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Organizations must ensure that there is always an executive available to make decisions during a disaster. Executive succession planning determines an organization's line of succession. Executives may become unavailable due to a variety of disasters, ranging from injury and loss of life to strikes, travel restrictions, and medical quarantines.

Incorrect Answers:
B: The purpose of a Continuity of Operations plan is to maintain operations during a disaster. Continuity of Operations does address chain of command recovery.
C: A Business Impact Assessment (BIA) is an analysis that identifies the resources that are critical to an organization's ongoing viability and the threats posed to those resources. A BIA does address chain of command recovery.
D: Business continuity planning is focused on keeping business functions uninterrupted when a disaster strikes. Business continuity planning does address chain of command recovery.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 372

QUESTION 642
Of the three types of alternate sites: hot, warm or cold, which is BEST described by the following facility description?

- Configured and functional facility
- Available with a few hours
- Requires constant maintenance
- Is expensive to maintain

A. Hot Site
B. Warm Site
C. Cold Site
D. Remote Site

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A hot site is a facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The hot site would include computers, cables and peripherals.

Incorrect Answers:
B: A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers. C: A cold site is a leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services.
D: A remote site is just a site at a remote location. There are no specification on what equipment or services, if any, would be available at the remote location.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 920

QUESTION 643
Which of the following plan provides procedures for sustaining essential business operations while recovering from significant disruption?

A. Business Continuity Plan
B. Occupant Emergency Plan
C. Cyber Incident Response Plan
D. Disaster Recovery Plan

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A business continuity plan provides procedures for sustaining essential business operations while recovering from a significant disruption.

Incorrect Answers:
B: The occupant emergency plan (OEP) provides the "response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency." C: A Cyber Incident response plan focuses on malware, hackers, intrusions, attacks, and other security issues. It outlines procedures for incident response. D: A Disaster recovery plan provides detailed procedures to facilitate recovery of capabilities at an alternate site, while occupant emergency plan provides coordinated procedures for minimizing loss of life or injury and protecting properly damage in response to a physical threat.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, pp. 369-370

QUESTION 644
Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan
B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Every organization should have a disaster recovery plan, but there is no requirement of a disaster recovery plan.
Incorrect Answers:
B: The DRP is carried out when everything is still in emergency mode, and everyone is scrambling to get all critical systems back online. But the DRP also includes comprehensive instructions for essential personnel to follow immediately upon recognizing that a disaster is imminent.
C: The disaster recovery plan (DRP) guides the recovery efforts necessary to restore your business to normal operations as quickly as possible. The DRP guides the actions of emergency - response personnel until the end goal is reached, which is to see the business restored to full operating capacity in its primary operations facilities.

D: One of the most important elements of the disaster recovery plan is the selection of alternate processing sites to be used when the primary sites are unavailable.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 887

QUESTION 645
Which of the following statements do apply to a hot site?

A. It is expensive.
B. There are cases of common overselling of processing capabilities by the service provider.
C. It provides a false sense of security.
D. It is accessible on a first come first serve basis. In case of large disaster it might Be accessible.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A hot site is Accessible on first come first server basis. With a hot site arrangement, a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software.

Incorrect Answers:
A: One disadvantage of a hot site is that it is very expensive.
B: The hot site service provider might oversell the processing capabilities.
C: The level of disaster recovery protection provided by a hot site is unsurpassed. A hot site does not give a false sense of security.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 921

QUESTION 646
What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?
A. Remote journaling
B. Electronic vaulting
C. Data clustering
D. Database shadowing

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In an electronic vaulting scenario, database backups are transferred to a remote site using bulk transfers. The transfers occur in infrequent batches.

Incorrect Answers:
A: With remote journaling, data transfers are performed in a expeditious manner. Data transfers occur in a bulk transfer mode, but they occur on a frequent basis, usually once every hour if not more frequently.
C: Data clustering does not include batch processing dumping data at an alternate location.
D: Database shadowing is remote journaling to more than one destination duplicate server. Remote journaling is Batch processing dumping backup data to an alternate location.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 660

QUESTION 647
Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

A. Full Interruption test
B. Checklist test
C. Simulation test
D. Structured walk-through test

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Full-interruption tests operate like parallel tests, but they involve actually shutting down operations at the primary site and shifting them to the recovery site. After a parallel test has been completed the next step is to perform a full-interruption test.
Incorrect Answers:
B: The checklist test is one of the simplest tests to conduct. You should perform it before, after, you perform a Parallel test.
C: Simulation tests are similar to the structured walk – through tests, and should be performed before parallel test, after parallel tests.
D: Parallel tests represent the next level in testing compared to a structured walk-through test, not vice versa.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 671

QUESTION 648
What is the Maximum Tolerable Downtime (MTD)?

A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data
C. Maximum elapsed time required to move back to primary site after a major disruption
D. It is maximum delay businesses can tolerate and still remain viable

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD).

Incorrect Answers:
A: Maximum Tolerable Downtime does not refer to application data. Maximum Tolerable Downtime is the time delay that the business can tolerate.
B: Maximum Tolerable Downtime does not refer to application data. Maximum Tolerable Downtime is the time delay that the business can tolerate.
C: Maximum Tolerable Downtime does not refer to the time needed to move back to the primary site after a disruption. Maximum Tolerable Downtime is the time delay that the business can tolerate.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 909

QUESTION 649
Which of the following specifically addresses cyber-attacks against an organization's IT systems?

A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan

Correct Answer: C

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A Cyber incident response plan focuses on malware, hackers, intrusions, attacks, and other security issues. It outlines procedures for incident response. There are no other types of Incident response plans.

Incorrect Answers:
A: There is no continuity of support plan which addresses cyber-attacks. The Incident response plan addresses cyber-attacks.
B: A business continuity plan (BCP) does address cyber-attacks. A BCP contains strategy documents that provide detailed procedures that ensure critical business functions are maintained.
D: There is no continuity of operations plan which addresses cyber-attacks. The Incident response plan addresses cyber-attacks.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 953

QUESTION 650
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The damage assessment team should be responsible determining the disaster's cause and the amount of damage that has occurred to organizational assets. The assessment of the damage should include the status of the equipment at the site such as servers and network devices.

Incorrect Answers:
A: Damage mitigation is a preventive method which is applied prior to a disaster, while salvage are done after a disaster.
B: Before installing new equipment the damage must be assessed and the equipment must be salvaged.
D: Before the salvage team starts to recover the equipment, the damage assessment team should assess the damage on the site.

QUESTION 651
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In a Structured walk-through test representatives from each department or functional area come together and go over the plan to ensure its accuracy. The group reviews the objectives of the plan; discusses the scope and assumptions of the plan; reviews the organization and reporting structure; and evaluates the testing, maintenance, and training requirements described.

Incorrect Answers:
A: In a Simulation test the plan is not reviewed in detail. In a Simulation test all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario.
B: A Checklist test, like a Structured walk-through test, has the aim to review the plan, but in a Checklist test the functional representatives do not meet. Instead copies of the BCP are distributed to the different departments and functional areas for review.
C: The purpose of a Parallel test is not to review the plan in detail. A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 955

QUESTION 652
When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff
B. Senior business unit management
C. BCP committee
D. Functional business units
Correct Answer: B

Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Senior management is ultimately responsible for all phases of the plan, and who should be most concerned about the protection of its assets. They must sign off on all policy issues, and they will be held liable for overall success or failure of a security solution.

Incorrect Answers:
A: If possible the BCP plan should by endorsed by the Executive management staff, but the Executive management staff is not responsible for identifying and prioritizing time-critical systems.
C: The BCP committee does not identify and prioritize systems. The BCP committee oversees, initiates, plans, approves, tests and audits the BCP. It also implements the BCP, coordinates activities, approve the BIA survey. The BCP committee also oversees the creation of continuity plans and reviews the results of quality assurance activities
D: Functional business units are a part of the BCP committee. Functional business units are not responsible for identifying and prioritizing time-critical system.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 55

QUESTION 653
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
If the incident response team determines that a crime has been carried out, senior management should be informed immediately. If the suspect is an employee, a human resources representative must be called right away.

Incorrect Answers:
B: Industrial Security does not need to be involved when an employee is suspected of a crime.

C: Public Relations does not need to be involved when an employee is suspected of a crime.
D: The External Audit Group does not need to be involved when an employee is suspected of a crime.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1035

QUESTION 654
To be admissible in court, computer evidence must be which of the following?

A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
For evidence to be admissible in court, it needs to be relevant, sufficient, and reliable.

Incorrect Answers:
B: The evidence should not be changed. If it is encrypted it should be kept encrypted.
C: Evidence should not be changed or edited.
D: Evidence does not need to be incriminating. It can very well be used in favor of the suspect, such as an alibi.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1068

QUESTION 655
Once evidence is seized, a law enforcement officer should emphasize which of the following?

A. Chain of command
B. Chain of custody
C. Chain of control D. Chain of communications

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When evidence is seized, it is important to make sure a proper chain of custody is maintained to ensure any data collected can later be properly and accurately represented in case it needs to be used for later events such as criminal proceedings or a successful prosecution.

Incorrect Answers:
A: Chain of command is not related to the collection of evidence. In a military context, the chain of command is the line of authority and responsibility along which orders are passed within a military unit and between different units.
C: Chain of control is not related to collection of evidence. Chain of custody relates to how evidence is collected.
D: Chain of communication is not related to collection of evidence. Chain of custody relates to how evidence is collected.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 248

QUESTION 656
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

A. System development activity
B. Help-desk function
C. System Imaging

D. Risk management process

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The computer system should not be changed, while the incident handling is ongoing. System development should not occur during incident handling.

Incorrect Answers:
B: As part of the ongoing incident handling employees, vendors, customers, partner, devices or sensors report the event to Help Desk.
C: System imaging would not affect the ongoing incident handling and should take place to
D: The Risk management process would not affect the ongoing incident handling.

References:
https://en.wikipedia.org/wiki/Computer_security_incident_management

QUESTION 657
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files
D. Displayed the contents of a folder

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The original media should have two copies created: a primary image (a control copy that is stored in a library) and a working image (used for analysis and evidence collection). These should be timestamped to show when the evidence was collected. Displaying the contents of a folder would affect the original media, and would compromise the evidence collection process.

Incorrect Answers:
A: A write blocker would be a step to secure the integrity of the media.

B: Making a full-disk image would be a part of the investigation process.
C: To create a message digest for log files would be part of the documentation.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1049

QUESTION 658
What is the PRIMARY goal of incident handling?

A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
The primary goal of incident handling is to contain, eradicate, and recovery from the incident. See step 3 below.
Note: The Incident Handling lifecycle can be divided into the following four steps:
1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident Activity

Incorrect Answers:
A: Retrieving evidence to prosecute is not part of Incident Handling.
B: Preparation is part of incident handling lifecycle, but it is not the most important goal.
C: Improving the disaster recovery plan is not a goal of incident handling.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 331

QUESTION 659
Which of the following would be LESS likely to prevent an employee from reporting an incident?

A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.

C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A centralized incident reporting would increase, not decrease, the likelihood that an employee would report an incident.

Incorrect Answers:
A: An employee could be afraid to get involved and refrain from reporting an incident.
C: Employees that are afraid of being accused of something they didn't do would be less likely to report an incident.
D: Employees that are unaware of the company's security policies and procedures would be less likely to report an incident.
References:
https://en.wikipedia.org/wiki/Computer_security_incident_management

QUESTION 660
What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?

A. To ensure that no evidence is lost.
B. To ensure that all possible evidence is gathered.
C. To ensure that it will be admissible in court
D. To ensure that incidents were handled with due care and due diligence.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Real evidence, like any type of evidence, must meet the relevancy, materiality, and competency requirements before being admitted into court. In many cases, it is not possible for a witness to uniquely identify an object in court. In those cases, a chain of evidence (also known as a chain of custody) must be established.

Incorrect Answers:
A: Chain of custody is not used to avoid loss of evidence. It is used to ensure that evidence can be admitted.
B: Chain of custody is not used to ensure that all possible evidence is collected. It is used to ensure that evidence can be admitted.
D: Chain of custody concern evidence, it does not concern incidents.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 704

QUESTION 661
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine
D. Exigent Probable Doctrine

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances.

Incorrect Answers:
A: The exception to the search warrant is called exigent Circumstance, not Evidence Circumstance.
C: Admissible evidence is not related to any search warrant.
The general rule in evidence is that all relevant evidence is admissible and all irrelevant evidence is inadmissible.
D: A search without a warrant can only be executed under exigent circumstances, not under exigent probabilities.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1057

QUESTION 662
A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

A. Direct evidence
B. Circumstantial evidence
C. Hearsay evidence

D. Secondary evidence

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Oral evidence, such as a witness's testimony, and copies of original documents are placed in the secondary evidence category.
Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence.

Incorrect Answers:
A: Direct evidence can prove a fact all by itself and does not need backup information to refer to.
B: Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.
C: Hearsay evidence pertains to oral or written evidence presented in court that is secondhand and has no firsthand proof of accuracy or reliability. Hearsay is even less reliable compared to secondary evidence.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 663
Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Direct evidence.
B. Circumstantial evidence.
C. Conclusive evidence.
D. Corroborative evidence.

Correct Answer: A
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Direct evidence can prove a fact all by itself and does not need backup information to refer to. Direct evidence often is based on information gathered from a witness's five senses.

Incorrect Answers:
B: Circumstantial evidence can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact.

C: Conclusive evidence is not collected from the five senses of a witness. Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.
D: Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand its own, so it cannot disprove a specific act.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 664
This type of supporting evidence is used to help prove an idea or a point, however it cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand its own.

Incorrect Answers:
A: Circumstantial evidence can prove an intermediate fact, but not a direct fact by itself. The intermediate fact can then be used to deduce or assume the existence of another fact. This type of fact is used so the judge or jury will logically assume the existence of a primary fact.
C: Opinion evidence would be the opinion of a witness, but the opinion rule dictates that the witness must testify to only the facts of the issue and not her opinion of the facts.
D: Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence. Oral evidence, such as a witness's testimony, and copies of original documents are placed in the secondary evidence category.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1055

QUESTION 665
Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.

B. Its reliability must be proven.
C. The process for producing it must be documented and repeatable.
D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Correct Answer: D
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
A chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

Incorrect Answers:
A: The immateriality of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.
B: The reliability of the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.
C: The process of producing the evidence is not the most important. It is more important to show how the evidence was collected, analyzed, transported, and preserved. This is called the chain of custody.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1050

QUESTION 666
Why would a memory dump be admissible as evidence in court?

A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:

A memory dump identifies the state of the system.
Computer-generated evidence that is in the form of routine operational business data or reports and binary disk or memory dumps now constitute exceptions to the rule that computer-generated evidence is hearsay, and is therefore admissible in court.

Incorrect Answers:
A: A memory dump does not identify the truth, it is identification of the state of the system.
C: The state of the memory, the system state, can be admissible as evidence in court.
D: The exclusionary rule refers to evidence that is inadmissible. The exclusionary rule is a legal principle in the United States, under constitutional law, which holds that evidence collected or analyzed in violation of the defendant's constitutional rights is sometimes inadmissible for a criminal prosecution in a court of law.

References:
Stewart, James M., Ed Tittel, and Mike Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*, 5th Edition, Sybex, Indianapolis, 2011, p. 504

QUESTION 667
When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?

A. Eliminate all means of intruder access.
B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
If the event is determined to be a real incident, it is identified and classified. Once we understand the severity of the incident taking place, we move on to the next stage, which is investigation. Investigation involves the proper collection of relevant data, which will be used in the analysis and following stages. The goals of these stages are to reduce the impact of the incident, identify the cause of the incident, resume operations as soon as possible, and apply what was learned to prevent the incident from recurring.

Incorrect Answers:
A: Before we can eliminate intruder access we would have to determine the extent of the intrusion.
B: Before containing the intrusion we need to determine the extent of the intrusion.
D: Before we can communicate with the relevant parties we need to determine the extent of the intrusion.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1038

QUESTION 668
When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?

A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.

Correct Answer: C
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
For a crime to be successfully prosecuted, solid evidence is required. Computer forensics is the art of retrieving this evidence and preserving it in the proper ways to make it admissible in court. Related system information must be captures and recorded.

Incorrect Answers:
A: To backup up a compromised system is a good idea, but it is not required for prosecution.
B: Identifying the attacks would be a useful further step, but first the evidence must be safeguarded.
D: To isolate a compromised system is a good idea, but it is not required for prosecution.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1052

QUESTION 669
In order to be able to successfully prosecute an intruder:

A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.

Correct Answer: B
Section: Security Operations
Explanation

Explanation/Reference:
Explanation:
When evidence is seized, it is important to make sure a proper chain of custody is maintained to ensure any data collected can later be properly and accurately represented in case it needs to be used for later events such as criminal proceedings and a successful prosecution.

Incorrect Answers:
A: To successfully prosecute an intruder you do not need a designed point of contact. You need proper chain of custody of evidence.
C: To successfully prosecute an intruder you do not to follow predefined procedures. You need proper chain of custody of evidence.
D: It is import to make a replica of digital evidence to avoid tamping with evidence, though it is not strictly required to make a successfully prosecution.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 248

QUESTION 670
What does "System Integrity" mean?

A. The software of the system has been implemented as designed.
B. Users can't tamper with processes they do not own.
C. Hardware and firmware have undergone periodic testing to verify that they are functioning properly.
D. Design specifications have been verified against the formal top-level specification.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
System Integrity means that all components of the system cannot be tampered with by unauthorized personnel and can be verified that they work properly.

Incorrect Answers:
A: System Integrity concerns how software runs, and is not related to implementation of software.
C: System Integrity does not mean hardware and firmware verification. System Integrity relates to how running software behaves.
D: System Integrity is not part of the specification verification. System Integrity concerns how software runs.

References:
http://www.cerberussystems.com/INFOSEC/stds/d520028.htm
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 12

QUESTION 671
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.

A. virus
B. worm
C. Trojan horse
D. trapdoor

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A trojan horse is any code that appears to have some useful purpose but contains code that has a malicious or harmful purpose imbedded in it. It is non-selfreplicating malware that often includes a trapdoor as a means to gain access to a computer system bypassing security controls.

Incorrect Answers:
A: A Virus is a malicious program that can replicate itself and spread from one system to another. It does not appear to be harmless; its sole purpose is malicious intent often doing damage to a system.
B: A Worm is similar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system.
D A trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1213,
1214 http://en.wikipedia.org/wiki/Trojan_horse_(computing)
http://en.wikipedia.org/wiki/Computer_virus http://en.wikipedia.org/wiki/Computer_worm
http://en.wikipedia.org/wiki/Backdoor_(computing)

QUESTION 672
The security of a computer application is MOST effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.
B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is originally designed to provide the necessary security.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.

Incorrect Answers:
A: If you wait to implement security after a system is completed the cost of adding security increases dramatically and can become much more complex.
B: It is often difficult to add security to a system that has been procured off-the shelf.
C: This implies only a single threat.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 298, 357

QUESTION 673
Which of the following virus types changes some of its characteristics as it spreads?

A. Boot Sector
B. Parasitic
C. Stealth
D. Polymorphic

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A Polymorphic virus produces varied but operational copies of itself in an attempt to evade anti-virus software.

Incorrect Answers:
A: A boot sector virus attacks the boot sector of a drive. It describes the type of attack of the virus and not the characteristics of its composition. B: A parasitic virus attaches itself to other files but does not change its characteristics. C: A stealth virus attempts to hide changes of the affected files but not itself.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1199, 1200, 1201

QUESTION 674
Which of the following is commonly used for retrofitting multilevel security to a database management system?

A. trusted front-end
B. trusted back-end
C. controller
D. kernel

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
In a multilevel security (MLS) database system, a trusted front-end is configured. Users connect to the trusted front-end and the trusted front-end connects to the database system.
The trusted front end is responsible for directing queries to the correct database processor, for ensuring that there is no illegal flow of information between the database processors, for maintaining data consistency between replicated database fragments, and for properly labeling query responses and sending them back to the appropriate user. In addition, the trusted front end is responsible for user identification and authentication, maintenance of the trusted path to the user, and auditing.

Incorrect Answers:
B: A trusted back-end is not configured. The back-end would be the database system. Users connect to a trusted-front end which in turn connects to the back-end database system.
C: A 'controller' is not the correct term for a system that is configured for a multilevel security database system.
D: A kernel is the heart of an operating system. This is not what is configured for a multilevel security database system.

References:
http://www.acsac.org/secshelf/book001/19.pdf

QUESTION 675
Which of the following is an advantage of using a high-level programming language?

A. It decreases execution times for programs
B. It allows programmers to define syntax
C. It requires programmer-controlled storage management

D. It enforces coding standards

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
High-level languages enforce coding standards as a specific order to statements is required as well as a syntax that must be used.

Incorrect Answers:
A: High-level language makes a program easier to code but does not affect the execution times for a program.
B: High-level languages have a set syntax that the programmer needs to follow. It does not allow the programmer to define their own syntax.
C: High-level languages abstract the actual operation of the computer system such as memory usage, and storage.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1125-1128

QUESTION 676
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An online transaction processing system is used in conjunction with a database to commit transactions to a database in real time. The database must maintain its integrity, meaning the data in the database must be accurate at all times. Therefore, transactions must occur correctly or not at all to ensure that that only accurate data are entered into the database. If any of the steps in a transaction fails to complete to due invalid data, all the steps of the transaction are rolled back (dropped).

Incorrect Answers:

B: Invalid transactions should not be processed as it would affect the accuracy of the data and the integrity of the database. Instead, the transaction should be dropped.
C: Writing the transaction to a report for later review would help identify potential problems and/or threats. However, the database must maintain its integrity, meaning the data in the database must be accurate at all times. This means that the invalid transactions should not be allowed as it would compromise the database integrity. Therefore, the transaction should be dropped.
D: Generally, an online transaction processing system does not have mechanisms to correct invalid transactions. These transactions are made by information entered into a web form or other front-end interface. The user needs to correct their error and resubmit the information.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1180-1182, 1187-1188
http://en.wikipedia.org/wiki/Online_transaction_processing
http://databases.about.com/od/administration/g/concurrency.htm

QUESTION 677
When considering all the reasons that buffer overflow vulnerabilities exist what is the real reason?

A. Human error
B. The Windows Operating system
C. Insecure programming languages
D. Insecure Transport Protocols

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The human error in this answer is poor programming by the software developer.
A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed.
When a programmer writes a piece of software that will accept data, this data and its associated instructions will be stored in the buffers that make up a stack. The buffers need to be the right size to accept the inputted data. So if the input is supposed to be one character, the buffer should be one byte in size. If a programmer does not ensure that only one byte of data is being inserted into the software, then someone can input several characters at once and thus overflow that specific buffer.

Incorrect Answers:
B: The Windows Operating system does not cause buffer overflow vulnerabilities.

C: Insecure programming languages do not cause buffer overflow vulnerabilities.
D: Insecure Transport Protocols do not cause buffer overflow vulnerabilities.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, 2013, p. 332

QUESTION 678
What is RAD?

A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The Rapid Application Development (RAD) model is a software development model or methodology that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

Incorrect Answers:
B: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a project management technique.
C: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not a measure of system complexity
D: RAD, or Rapid Application Development, is a software development model that relies on the use of rapid prototyping and enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. It is not Risk-assessment diagramming.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1116-1118
QUESTION 679
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.

D. To compare source code versions before transferring to the test environment

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production. Logical errors and coding mistakes are referred to as bugs in the code.

Incorrect Answers:
A: The process of generating random data that can be sent to a target program in order to trigger failures is called fuzzing.
C: Debugging does not protect the program from changes.
D: Debugging is not used to compare code versions.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1102-1103, 1105
https://en.wikipedia.org/wiki/Debugging

QUESTION 680
Which of the following is one of the oldest and most common problem in software development that is still very prevalent today?

A. Buffer Overflow
B. Social Engineering
C. Code injection for machine languageD. Unassembled reversible DOS instructions.

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Buffer overflows are in the source code of various applications and operating systems. They have been around since programmers started developing software. This means it is very difficult for a user to identify and fix them. When a buffer overflow is identified, the vendor usually sends out a patch, so keeping systems current on updates, hotfixes, and patches is usually the best countermeasure.

A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by

commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.

Incorrect Answers:
B: Social engineering is when one person tricks another person into sharing confidential information, for example, by posing as someone authorized to have access to that information. This is a user issue; it is not a problem in software development.
C: Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. This is not one of the most common problems in software development today.
D: DOS applications are rare nowadays so unassembled reversible DOS instructions is not a prevalent problem today.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 332, 337

QUESTION 681
Which of the following is NOT true concerning Application Control?

A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Application control limits what users can see or do within the application. For example, if a user does not have the necessary access privilege to perform some functions, the functions can be hidden from the screen or the screen itself can be hidden so the user cannot select it within the application. In a similar way, only the records a user has access to can be displayed.
Application control is transparent to the user; the user does not know that a particular screen, function or data records have been hidden.
Application control can be implemented to record the activities a user performs within the application for auditing purposes.

Incorrect Answers:
A: It is true that application control limits end users use of applications in such a way that only particular screens are visible.
B: It is true that only specific records can be requested through the application controls.
C: It is true that particular usage of the application can be recorded for audit purposes by Application Control.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1084-1085

QUESTION 682
The object-relational and object-oriented models are better suited to managing complex data such as required for which of the following?

A. computer-aided development and imaging
B. computer-aided duplexing and imaging
C. computer-aided processing and imaging
D. computer-aided design and imaging

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-oriented database has classes to define the attributes and procedures of its objects, which can be a variety of data types such as images, audio, documents, and video. This complex data is required for computer-aided design and imaging.

Incorrect Answers:
A, B, C: Computer-aided development, computer-aided duplexing, and computer-aided processing are not valid computing terms. The correct term is computeraided design.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1173-1174

QUESTION 683
Which of the following is not an element of a relational database model?

A. Relations, tuples, attributes and domains
B. Data Manipulation Language (DML) on how the data will be accessed and manipulated
C. Constraints to determine valid ranges and values
D. Security structures called referential validation within tables

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A relational database model uses attributes (columns) and tuples (rows) to contain and organize information. The relational database model is the most widely used model today. It presents information in the form of tables. A relational database is composed of two-dimensional tables, and each table contains unique rows, columns, and cells (the intersection of a row and a column). Each cell contains only one data value that represents a specific attribute value within a given tuple. These data entities are linked by relationships. The relationships between the data entities provide the framework for organizing data. A primary key is a field that links all the data within a record to a unique value.
Data manipulation language (DML) contains all the commands that enable a user to view, manipulate, and use the database (view, add, modify, sort, and delete commands).
A constraint is usually associated with a table and is created with a CREATE CONSTRAINT or CREATE ASSERTION SQL statement. They define certain properties that data in a database must comply with. They can apply to a column, a whole table, more than one table or an entire schema.

Security structures called referential validation within tables are not an element of a relational database model. Referential integrity is used to ensure all foreign keys reference primary keys. Referential validation is not a security structure within a table.

Incorrect Answers:
A: Relations, tuples, attributes and domains are elements of a relational database model.
B: Data Manipulation Language (DML) is an element of a relational database model.
C: Constraints to determine valid ranges and values are an element of a relational database model.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1171-1177

QUESTION 684
A persistent collection of interrelated data items can be defined as which of the following?

A. database
B. database management system
C. database security
D. database shadowing

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A database can be defined as a persistent collection of interrelated data items.

Persistency is obtained through the preservation of integrity and through the use of nonvolatile storage media. The description of a database is a schema and a Data Description Language (DDL) defines the schema.

Incorrect Answers:
B: A database management system is the software that maintains and provides access to the database. This is not what is described in the question.
C: Database security restricts access to the database to authorized users and applications. This is not what is described in the question.
D: Database shadowing creates a replica of the database on another database server for redundancy purposes. This is not what is described in the question.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 67

QUESTION 685
The description of the database is called a schema. The schema is defined by which of the following?

A. Data Control Language (DCL).
B. Data Manipulation Language (DML).
C. Data Definition Language (DDL).
D. Search Query Language (SQL).

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The description of the database is called a schema, and the schema is defined by a Data Definition Language (DDL). DDL is similar to a computer programming language and is used for defining data structures, such as database schemas.

Incorrect Answers:
A: The Data Control Language (DCL) is a subset of the Structured Query Language (SQL) that allows database administrators to configure security access to relational databases.
B: The Data Manipulation Language (DML) is used to retrieve, insert and modify database information. These commands will be used by all database users during the routine operation of the database.
D: SQL is the abbreviation for structured query language and not search query language. SQL is a standardized query language for requesting information from a database.

References:

Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1177, 1178
https://secure.wikimedia.org/wikipedia/en/wiki/Data_Definition_Language
http://databases.about.com/od/Advanced-SQL-Topics/a/Data-Control-Language-Dcl.htm
http://www.webopedia.com/TERM/S/SQL.html http://www.w3schools.in/mysql/ddl-dml-dcl/
http://www.orafaq.com/faq/what_are_the_difference_between_ddl_dml_and_dcl_commands

QUESTION 686
Which of the following defines the software that maintains and provides access to the database?

A. database management system (DBMS)
B. relational database management system (RDBMS)
C. database identification system (DBIS)
D. Interface Definition Language system (IDLS)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.

Incorrect Answers:
B: A relational database management system (RDBMS) provides access to a relational database.
C: There is no database identification system.
D: An Interface Definition Language (IDL) is a language that is used to define the interface between a client and server process in a distributed system. It is not used to provide access to a database.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1170
http://csis.pace.edu/~marchese/CS865/Papers/interface-definition-language.pdf

QUESTION 687
Which of the following represents a relation, which is the basis of a relational database?

A. One-dimensional table
B. Two-dimensional table

C. Three-dimensional table
D. Four-dimensional table

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The relational database model is based on a series of interrelated two-dimensional tables that have columns representing the variables and rows that contain specific instances of data.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1171

QUESTION 688
Which of the following represents the rows of the table in a relational database?

A. attributes
B. records or tuples
C. record retention
D. relation

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The rows of the table represent records or tuples.

Incorrect Answers:
A: The columns of the table represent the attributes.
C: Record retention refers to the usually legal requirement to retain data that are no longer of value to the business for a period of time. This ensures compliance with legal requirements.
D: The relation represents the link between data entities, usually from different tables in the database.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1171, 1174

Miller, David R., *CISSP Training Kit*, O'Reilly Media, Sebastopol, 2013, pp. 687-688

QUESTION 689
Which of the following can be defined as the set of allowable values that an attribute can take?

A. domain of a relation

B. domain name service of a relation C.
domain analysis of a relation
D. domains, in database of a relation

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The domain of a relation is the set of allowable values that an attribute can take. In other words, it is the values that can be entered in a column (attribute) of a table (relation).

References:
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, p. 272

QUESTION 690
Which of the following can be defined as a unique identifier in the table that unambiguously points to an individual tuple or record in the table?

A. primary key
B. candidate key

C. secondary key
D. foreign key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The primary key is the attribute that is used to make each row or tuple in a table unique.
Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.
D: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 691
Which of the following can be defined as THE unique attribute used as a unique identifier within a given table to identify a tuple?

A. primary key
B. candidate key
C. foreign key

D. secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The primary key is the attribute that is used to make each row or tuple in a table unique.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.
D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 692
Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?

A. foreign key
B. candidate key
C. primary key
D. secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.

Incorrect Answers:

B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
C: The primary key is the attribute that is used to make each row or tuple in a table unique.
D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 693
Referential Integrity requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for which of the following?

A. primary key
B. secondary key
C. foreign key
D. candidate key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that references or matches the primary key of another table. The primary key is the attribute that is used to ensure that each row or tuple in a table unique. Together, the foreign key and the primary key ensure referential integrity.

Incorrect Answers:
B: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.
C: A foreign key is an attribute in one table that matches the primary key of another table and is used to cross-reference tables.
D: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180, 1181
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis,

2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 694
Matches between which of the following are important because they represent references from one relation to another and establish the connections among these relations?

A. foreign key to primary key
B. foreign key to candidate key
C. candidate key to primary key
D. primary key to secondary key

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A foreign key is an attribute in one table that references or matches the primary key of another table. The primary key is the attribute that is used to ensure that each row or tuple in a table unique. Together, the foreign key and the primary key ensure referential integrity.

Incorrect Answers:
B: Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table. There are usually more than one candidate key attributes in a table.
C: A foreign key is an attribute in one table that references or matches the primary key of another table. Candidate keys are a subset of attributes that from which the database developer can choose the primary key to uniquely identify any tuple or record in a table.
D: Secondary keys are candidate keys that have not been chosen as the primary key. The primary key is the attribute that is used to make each row or tuple in a table unique. Candidate keys are a subset of attributes that from which the database developer can choose the primary key.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1174, 1179-1180, 1181
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 276, 312 http://databases.about.com/cs/specificproducts/g/candidate.htm
http://rdbms.opengrass.net/2_Database
Design/2.1_TermsOfReference/2.1.2_Keys.html

QUESTION 695
A database view is the results of which of the following operations?

A. Join and Select.
B. Join, Insert, and Project.
C. Join, Project, and Create.
D. Join, Project, and Select.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
SQL offers three classes of operators for creating views: select, project, and join.
- The select operator serves to shrink the table vertically by eliminating unwanted rows (tuples).
- The project operator serves to shrink the table horizontally by removing unwanted columns (attributes). Most commercial implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output.
- The join operator allows the dynamic linking of two tables that share a common column value.

Incorrect Answers:
A: SQL offers three classes of operators for creating views: select, project, and join. However, modern implementations of SQL do not support a project operation, instead projections are achieved by specifying the columns desired in the output. Nevertheless, project is a SQL operator.
B: Insert is a SQL command used to insert data into a table. It is not used to output a view.
C: Create is a SQL command used to create a new database, table, view, or index. However, the data or output of the view requires a select statement to shrink the table vertically by not showing unwanted rows, a project operation that shrinks the table horizontally by not showing unwanted columns, and a join statement when data from more than one table is required.

References:
http://db.grussell.org/section010.html
http://databasemanagement.wikia.com/wiki/Relational_Database_Model

QUESTION 696
In regards to the query function of relational database operations, which of the following represent implementation procedures that correspond to each of the lowlevel operations in the query?

A. query plan
B. relational plan
C. database plan
D. structuring plan

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A query plan (or query execution plan) is an ordered set of steps used to access data in a SQL relational database management system. This is a specific case of the relational model concept of access plans.
Since SQL is declarative, there are typically a large number of alternative ways to execute a given query, with widely varying performance. When a query is submitted to the database, the query optimizer evaluates some of the different, correct possible plans for executing the query and returns what it considers the best option.

Incorrect Answers:
B: Relational plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.
C: Database plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.
D: Structural plan is not the correct term to describe implementation procedures that correspond to each of the low-level operations in the query.

References:
https://en.wikipedia.org/wiki/Query_plan

QUESTION 697
In regards to relational database operations using the Structure Query Language (SQL), which of the following is a value that can be bound to a placeholder declared within an SQL statement?

A. A bind value
B. An assimilation value
C. A reduction value
D. A resolution value

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bind parameters—also called dynamic parameters or bind variables—are an alternative way to pass data to the database. Instead of putting the values directly into the SQL statement, you just use a placeholder like ?, :name or @name and provide the actual values using a separate API call.
When using bind parameters you do not write the actual values but instead insert placeholders into the SQL statement. That way the statements do not change when executing them with different values.

Incorrect Answers:
B: An assimilation value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
C: A reduction value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
D: A resolution value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.

References:
http://use-the-index-luke.com/sql/where-clause/bind-parameters

QUESTION 698
Which of the following are placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server?

A. Bind variables
B. Assimilation variables
C. Reduction variables
D. Resolution variables

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bind variables placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server. The SQL statement is sent to the server for parsing and the later values are bound to the placeholders and sent separately to the server. This separate step is the origin of the term 'bind variable'.

Incorrect Answers:
B: An assimilation value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
C: A reduction value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.
D: A resolution value is not the correct term for a value that can be bound to a placeholder declared within an SQL statement.

References:
Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 84

QUESTION 699
Normalizing data within a database could include all or some of the following except which one?

A. Eliminate duplicative columns from the same table.

B. Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key
C. Eliminates Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
D. Eliminating duplicate key fields by putting them into separate tables.

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Normalizing data within a database does not eliminate duplicate key fields by putting them into separate tables.

An entity is in First Normal Form (1NF) when all tables are two-dimensional with no repeating groups.
A row is in first normal form (1NF) if all underlying domains contain atomic values only. 1NF eliminates repeating groups by putting each into a separate table and connecting them with a one-to-many relationship. Make a separate table for each set of related attributes and uniquely identify each record with a primary key.
- Eliminate duplicative columns from the same table.
- Create separate tables for each group of related data and identify each row with a unique column or set of columns (the primary key).

An entity is in Second Normal Form (2NF) when it meets the requirement of being in First Normal Form (1NF) and additionally:
- Does not have a composite primary key. Meaning that the primary key cannot be subdivided into separate logical entities.
- All the non-key columns are functionally dependent on the entire primary key.
- A row is in second normal form if, and only if, it is in first normal form and every non-key attribute is fully dependent on the key.
- 2NF eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key. An example is resolving many:many relationships using an intersecting entity

An entity is in Third Normal Form (3NF) when it meets the requirement of being in Second Normal Form (2NF) and additionally:
- Functional dependencies on non-key fields are eliminated by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
- A row is in third normal form if and only if it is in second normal form and if attributes that do not contribute to a description of the primary key are move into a separate table. An example is creating look-up tables.

Incorrect Answers:
A: Normalizing data within a database does eliminate duplicative columns from the same table.
B: Normalizing data within a database does eliminate functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key.
C: Normalizing data within a database does eliminate Functional dependencies on non-key fields by putting them in a separate table.

References:
http://psoug.org/reference/normalization.html
http://searchsqlserver.techtarget.com/definition/normalization?vgnextfmt=print

QUESTION 700
Which of the following is used to create and modify the structure of your tables and other objects in the database?

A. SQL Data Definition Language (DDL)
B. SQL Data Manipulation Language (DML)
C. SQL Data Relational Language (DRL)
D. SQL Data Identification Language (DIL)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The Data Definition Language (DDL) is similar to a computer programming language and is used for defining data structures, such as database schemas, database tables, and other database objects.

Incorrect Answers:
B: The Data Manipulation Language (DML) is used to retrieve, insert and modify database data. These commands will be used by all database users during the routine operation of the database.
C: The SQL language consists of three components: the Data Definition Language (DDL), the Data Manipulation Language (DML), and the Data Control Language (DCL). It does not contain a data relational language.
D: The SQL language consists of three components: the Data Definition Language (DDL), the Data Manipulation Language (DML), and the Data Control Language (DCL). It does not contain a data identification language.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1177

QUESTION 701
SQL commands do not include which of the following?

A. Select, Update
B. Grant, Revoke
C. Delete, Insert
D. Add, Relist

Correct Answer: D
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
There is no Add command within the Structure Query Language (SQL). Instead the Insert command is used to add new data to the database.

There is also no Relist command within SQL.

Incorrect Answers:
A: Select and Update are Data Manipulation Language (DML) commands. The Select statement is used to select data from a database while the Update statement is used to update existing records in a table.
B: Grant and Revoke are Data Control Language (DCL) commands are used to enforce database security. The Grant statement is used to provide access or privileges on the database objects while the Revoke statement is used to remove those privileges.
C: Delete and Insert are Data Manipulation Language (DML) commands. The Delete statement is used to remove data from a database while the Insert statement is used to add data to a table.

References:
https://technet.microsoft.com/en-us/library/ff848799.aspx https://technet.microsoft.com/en-us/library/ff848766.aspx http://www.cs.utexas.edu/~mitra/csFall2012/cs329/lectures/sql.html http://www.w3schools.com/SQl/sql_select.asp http://www.w3schools.com/SQl/sql_update.asp http://beginner-sql-tutorial.com/sql-grant-revoke-privileges-roles.htm

QUESTION 702
Complex applications involving multimedia, computer aided design, video, graphics, and expert systems are more suited to which of the following database type?

A. Object-Oriented Databases (OODB)
B. Object-Relational Databases
C. Relational Databases
D. Database management systems (DBMS)

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-oriented database (OODB) has classes to define the attributes and procedures of its objects, which can be a variety of data types such as images, audio, documents, and video. This complex data is required for computer-aided design and imaging.

Incorrect Answers:

B: An object-relational database (ORD) is a relational database with a software front end that is written in an object-oriented programming language and is used with Object-Oriented Databases (OODB). It does not store data.
C: A relational database organizes data into two-dimensional tables consisting of attributes (columns) and tuples (rows). It is not suited to storing complex data types such as video, graphics, etc.
D: The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1170, 1171, 1173-1174, 1175

QUESTION 703
With regard to databases, which of the following has characteristics of ease of reusing code and analysis and reduced maintenance?

A. Object-Oriented Databases (OODB)
B. Object-Relational Databases (ORDB)
C. Relational Databases
D. Database management systems (DBMS)

Correct Answer: A
Section: Software Development Security
Explanation
Explanation/Reference:
Explanation:
An object-oriented database (OODB) is more dynamic than a relational database as it stores data as objects. It allows object-oriented programming (OOP) code, including classes, to manipulate the objects. This also makes the reusing of code possible.

Incorrect Answers:
B: An object-relational database (ORD) is a relational database with a software front end that is written in an object-oriented programming language. This allows programmers to develop a front-end that incorporates the business logic procedures to be used by requesting applications and the data within the

database. C: A relational database stores data in a two-dimensional table and uses query language, such as Structured Query Language (SQL), to access and manipulate that data.
D: The database management system (DBMS) is a software suite that is used to manage access to the database and provides data integrity and redundancy. It is usually controlled by a database administrator.
References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1173-1174, 1175
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 202

QUESTION 704
Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?

A. object-relational database
B. object-oriented database
C. object-linking database
D. object-management database

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
An object-relational database is described as is the marriage of object-oriented and relational technologies combining the attributes of both.
An object-relational database (ORD) or object-relational database management system (ORDBMS) is a relational database with a software front end that is written in an object-oriented programming language. A relational database just holds data in static two-dimensional tables. When the data are accessed, some type of processing needs to be carried out on it—otherwise, there is really no reason to obtain the data. If we have a front end that provides the procedures (methods) that can be carried out on the data, then each and every application that accesses this database does not need to have the necessary procedures. This means that each and every application does not need to contain the procedures necessary to gain what it really wants from this database.

Incorrect Answers:
B: An object-oriented database is a database designed to handle a variety of data types (images, audio, documents, video). This is not what is described in the question.
C: An object-linking database is not a valid database type.
D: An object-management database is not a valid database type.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1175

QUESTION 705

What is used to hide data from unauthorized users by allowing a relation in a database to contain multiple tuples with the same primary keys with each instance distinguished by a security level?

A. Data mining
B. Polyinstantiation
C. Cell suppression
D. Noise and perturbation

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Polyinstantiation enables a table, which is also known as a relation, to contain multiple tuples with the same primary keys, with each instance distinguished by a security level. At a lower security level the tuple will not contain sensitive data and it will effectively be hidden from users who do not have the appropriate access permissions.

Incorrect Answers:
A: Data mining is the process of analyzing large amounts of data to determine patterns that would not previously be apparent.
C: Cell suppression is a technique used to hide specific cells in a database that contain information that could be used in inference attacks.
D: Noise and perturbation is a technique of inserting fake information in a database in an attempt to misdirect an attacker or create sufficient confuse that the actual attack will not be fruitful.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1185, 1186, 1188

QUESTION 706
Which of the following translates source code one command at a time for execution on a computer?

A. A translator
B. An interpreter
C. A compiler
D. An assembler

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Interpreters translate one command at a time during run-time or execution time.

Incorrect Answers:
A: A translator converts source code to another format, which could be another high-level language, an intermediate language, or machine language.
C: A compiler converts high-level language source code to the necessary a target language for specific processors to understand.
D: An assembler converts assembly language source code into machine code that the computer understands.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1128-1130

QUESTION 707
Which of the following statements relating to Distributed Computing Environment (DCE) is FALSE?

A. It is a layer of software that sits on the top of the network layer and provides services to the applications above it.
B. It uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
C. It provides the same functionality as DCOM, but it is more proprietary than DCOM.
D. It is a set of management services with a communication layer based on RPC.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Distributed Computing Environment (DCE) does provide the same functionality as DCOM, but it is NOT more proprietary than DCOM.
Distributed Computing Environment (DCE) is a standard developed by the Open Software Foundation (OSF), also called Open Group. It is a client/server framework that is available to many vendors to use within their products. This framework illustrates how various capabilities can be integrated and shared between heterogeneous systems. DCE provides a Remote Procedure Call (RPC) service, security service, directory service, time service, and distributed file support. It was one of the first attempts at distributed computing in the industry.
DCE is a set of management services with a communications layer based on RPC. It is a layer of software that sits on the top of the network layer and provides services to the applications above it. DCE and Distributed Component Object Model (DCOM) offer much of the same functionality. DCOM, however, was developed by Microsoft and is more proprietary in nature.
Incorrect Answers:
A: It is true that DCE is a layer of software that sits on the top of the network layer and provides services to the applications above it.
B: It is true that DCE uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
D: It is true that DCE is a set of management services with a communication layer based on RPC.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1146, 1142

QUESTION 708
Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?

A. Stealth viruses
B. Polymorphic viruses
C. Trojan horses
D. Logic bombs

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
A Polymorphic virus produces varied but operational copies of itself in an attempt to evade anti-virus software.

Incorrect Answers:
A: A stealth virus attempts to hide changes of the affected files but not itself.
C: A Trojan horse is code that is disguised as a useful application but contains code that has a malicious or harmful purpose imbedded in it.
D: A logic bomb executes a set of instructions when specific conditions are met.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, pp. 1199, 1200, 1201, 1206

QUESTION 709
Why would a database be denormalized?

A. To ensure data integrity
B. To increase processing efficiency
C. To prevent duplication of data
D. To save storage space
Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The purpose of denormalization is to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data.

Incorrect Answers:
A: The duplication of data creates a problem for data integrity as the data needs to be updated in numerous places. Normalization, which eliminates the duplication of data, improves data integrity.
C: The purpose of normalization is to eliminate duplication of the data. All duplicated data items should be deleted and replaced by a pointer. Denormalization could reverse this process. It attempts to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data.
D: The purpose of denormalization is to improve the read performance and processing efficiency of a database by adding redundant data or by grouping data. This increases storage space consumption.

References:
https://en.wikipedia.org/wiki/Denormalization
https://en.wikipedia.org/wiki/Database_normalization
Miller, David R., *CISSP Training Kit*, O'Reilly Media, Sebastopol, 2013, pp. 620, 622

QUESTION 710
Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The most important stages of developing computerized information systems (or any other system or software) are the early requirement gathering and design phases. If the needs of the users are not correctly determined, the system will not meet those needs. As end users will be the people using the system, they are will have the most valuable input into the system requirements definition. Inadequate user participation in defining the system's requirements can lead to a system design that does not meet the requirements of the users.

Incorrect Answers:

A: This question is asking for the BEST answer. Inadequate quality assurance (QA) tools may result in poor QA tests so floors in the system aren't recognized. However, defining the system's requirements is the most important stage of the project. If this is not done correctly, then QA testing will have no effect on the suitability of the new system.
B: Constantly changing user needs can be a hazard in a development project. However, this only has an effect if the users are involved in the design of the system. D: Inadequate project management generally leads to late or over-budget projects. Incorrectly determining the system requirements could be due to inadequate project management. However, Answer C is more specific to the cause of the problem.

QUESTION 711
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
Bottom Up Testing is an approach to integrated testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested.
With Bottom Up Testing critical modules can be tested first and the main advantage of this approach is that bugs are more easily found.

All the bottom or low-level modules, procedures or functions are integrated and then tested. After the integration testing of lower level integrated modules, the next level of modules will be formed and can be used for integration testing. This approach is helpful only when all or most of the modules of the same development level are ready. This method also helps to determine the levels of software developed and makes it easier to report testing progress in the form of a percentage.

Incorrect Answers:
A: Interface modules are located at higher levels of the software design, not at the bottom levels.
C: The major advantage of the top-down approach is that bugs are found earlier, not that confidence is achieved earlier.
D: The major functions are not located at the bottom, and would not be tested earlier.

References:
https://en.wikipedia.org/wiki/Integration_testing#Top-down_and_Bottom-up

QUESTION 712
Why do buffer overflows happen? What is the main cause?

A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory

Correct Answer: B
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
In computer security and programming buffer overflow is a type of application error. The application's lack of proper checking of parameters causes the buffer overflow.
A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety.

Incorrect Answers:
A: It is true that there is a limit of data that can be handled by a buffer, but this limit is not the cause of the overflow.
B: Buffer overflows can be exploited, but the cause is a flaw in the program. The exploitation does not cause the overflow.
D: Insufficient memory does not cause overflows. The overflow is caused by a flow in the application.

References:
Conrad, Eric, Seth Misenar and Joshua Feldman, *CISSP Study Guide*, 2nd Edition, Syngress, Waltham, 2012, p. 71

QUESTION 713
What is called the number of columns in a table?

A. Schema
B. Relation
C. Degree
D. Cardinality

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:

The number of columns in a database table (relation) is referred to as the degree.
Incorrect Answers:
A: Schema describes that structure of the database
B: A database table is also referred to as a relation.
D: Cardinality is the number of rows (tuples) in a database table (relation).

References:
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 275, 277

QUESTION 714
Which of the following would not correspond to the number of primary keys values found in a table in a relational database?

A. Degree
B. Number of tuples
C. Cardinality
D. Number of rows

Correct Answer: A
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
The degree of a table represents the number of columns in a database table. This does not correspond to the number of primary key values in a table as each row must have a unique primary key.

Incorrect Answers:
B, D: A row in a database table is referred to as a tuple. Each row or tuple must have a unique primary key. Therefore, the number of rows or tuples will correspond to the number of primary keys values found in a table.
D: Cardinality is the number of rows, also known as tuples, in a table. Each row or tuple must have a unique primary key. Therefore, the cardinality of a table will correspond to the number of primary keys values found in a table.

References:
Stewart, James, Ed Tittel and Mike Chapple, *CISSP: Certified Information Systems security Professional Study Guide*, 5th Edition, Wiley Publishing, Indianapolis, 2011, pp. 275, 277
http://databases.about.com/od/specificproducts/a/keys.htm

QUESTION 715

Java is not:

A. Object-oriented.
B. Distributed.
C. Architecture Specific.
D. Multithreaded.

Correct Answer: C
Section: Software Development Security
Explanation

Explanation/Reference:
Explanation:
JAVA was developed so that the same program could be executed on multiple hardware and operating system platforms, it is not Architecture Specific.

Incorrect Answers:
A: JAVA is object-oriented as it works with classes and objects.
B: JAVA was developed to be used in a distributed computing environment.
D: JAVA is multi-threaded that is calls to subroutines as is the case with object-oriented programming.

References:
Harris, Shon, *All In One CISSP Exam Guide*, 6th Edition, McGraw-Hill, New York, 2013, p. 1148