SY0-501.exam.130q

Number: SY0-501
Passing Score: 800
Time Limit: 120 min

SY0-501

CompTIA Security+ Certification Exam

Exam A

QUESTION 1
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

A. RTO
B. RPO
C. MTBF
D. MTTR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following types of keys is found in a key escrow?

A. Public
B. Private
C. Shared
D. Session

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

QUESTION 3
A security analyst is reviewing the following output from an IPS:

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF
Frag offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Select two.)

A. The source IP of the attack is coming from 250.19.18.22.
B. The source IP of the attack is coming from 250.19.18.71.
C. The attacker sent a malformed IGAP packet, triggering the alert.
D. The attacker sent a malformed TCP packet, triggering the alert.
E. The TTL value is outside of the expected range, triggering the alert.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Malicious traffic from an internal network has been detected on an unauthorized port on an application server.
Which of the following network-based security controls should the engineer consider implementing?

A. ACLs
B. HIPS
C. NAT
D. MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

A. DMZ
B. NAT
C. VPN
D. PAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

- All access must be correlated to a user account.
- All user accounts must be assigned to a single individual.
- User access to the PHI data must be recorded.
- Anomalies in PHI data access must be reported.
- Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.
D. Enable account lockout thresholds.

E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

Correct Answer: ACG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following encryption methods does PKI typically use to securely project keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive
D. True positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:

- New Vendor Entry – Required Role: Accounts Payable Clerk
- New Vendor Approval – Required Role: Accounts Payable Clerk
- Vendor Payment Entry – Required Role: Accounts Payable Clerk
- Vendor Payment Approval – Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

A.

New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

B.

New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

C.

New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

D.
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

A. Time-of-day restrictions
B. Permission auditing and review
C. Offboarding
D. Account expiration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. DetectiveF. Deterrent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

```
File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243
```

The administrator pulls a report from the patch management system with the following output:

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cdes283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

Given the above outputs, which of the following MOST likely happened?

A. The file was corrupted after it left the patch system.
B. The file was infected when the patch manager downloaded it.
C. The file was not approved in the application whitelist system.
D. The file was embedded with a logic bomb to evade detection.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A company has a data system with definitions for “Private” and “Public”. The company’s security policy outlines how data should be protected based on type. The company recently added the data type “Proprietary”. Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost
B. More searchable data
C. Better data classification
D. Expanded authority of the privacy officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

A. Owner
B. System
C. Administrator
D. User

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

A. Deterrent
B. Preventive
C. Detective
D. Compensating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are
MOST likely occurring? (Select two.)

A. Replay
B. Rainbow tables
C. Brute force
D. Pass the hash
E. Dictionary

Correct Answer: CE

Section: (none)
Explanation

Explanation/Reference:
QUESTION 20
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

A. LDAP
B. TPM
C. TLS
D. SSL
E. PKI

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

A. Vulnerability scanning
B. Penetration testing
C. Application fuzzing
D. User permission auditing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

A. Give the application team administrator access during off-hours.
B. Disable other critical applications before granting the team access.
C. Give the application team read-only access.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following cryptographic attacks would salting of passwords render ineffective?

A. Brute force
B. Dictionary C. Rainbow tables
D. Birthday

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Only Kerberos that can do Mutual Auth and Delegation.
https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication- overview

QUESTION 26
Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

A. RA
B. CA
C. CRL
D. CSR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

A. Buffer overflow
B. MITM
C. XSS
D. SQLi

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

A. Capture and document necessary information to assist in the response.
B. Request the user capture and provide a screenshot or recording of the symptoms.
C. Use a remote desktop client to collect and analyze the malware in real time.
D. Ask the user to back up files for later recovery.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following technologies employ the use of SAML? (Select two.)

A. Single sign-on
B. Federation
C. LDAP
D. Secure token
E. RADIUS

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

A. Privilege escalation
B. Pivoting
C. Process affinity
D. Buffer overflow
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
After a user reports slow computer performance, a system administrator detects a suspicious file, which was installed as part of a freeware software package. The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State           RpcSs [svchost.exe]
TCP   0.0.0.0:135            0.0.0.0:0              LISTENING       [svchost.exe]
TCP   0.0.0.0:445            0.0.0.0:0              LISTENING

TCP   192.168.1.10:5000      10.37.213.20           ESTABLISHED     winserver.exe
UDP   192.168.1.10:1900      *.*                                    SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

A. The scan job is scheduled to run during off-peak hours.
B. The scan output lists SQL injection attack vectors.
C. The scan data identifies the use of privileged-user credentials.
D. The scan results identify the hostname and IP address.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

A. Using salt
B. Using hash algorithms
C. Implementing elliptical curve
D. Implementing PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

A. Shared accounts
B. Preshared passwords
C. Least privilege
D. Sponsored guest

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.

B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not turned properly and reported a false positive.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.)

A. Install an X- 509-compliant certificate.
B. Implement a CRL using an authorized CA.
C. Enable and configure TLS on the server.
D. Install a certificate signed by a public CA.

E. Configure the web server to use a host header.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Select three.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP F. HTTPS
G. LDAPS

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
An auditor is reviewing the following output from a password-cracking tool:

```
user1: Password1
user2:Recovery!
user3:Alaskan10
user4:4Private
user5:PerForMance2
```

Which of the following methods did the author MOST likely use?

A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following must be intact for evidence to be admissible in court?
A. Chain of custody B.
Order of volatility
C. Legal hold
D. Preservation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

A. AES
B. 3DES
C. RSA D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44

A technician suspects that a system has been compromised. The technician reviews the following log entry:

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured to include an explicit deny rule.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46

A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.) A.

```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

```
nslookup
comptia.org
set type=MX
example.org
```

B.

C. `dig -axfr comptia.org@example.org`

D. `ipconfig/flushDNS`

```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

E.

F. `dig@example.org comptia.org`

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.)

A. To prevent server availability issues
B. To verify the appropriate patch is being installed

C. To generate a new baseline hash after patching
D. To allow users to test functionality
E. To ensure users are trained on new functionality

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

A. ISA
B. NDA
C. MOU
D. SLA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which of the following would meet the requirements for multifactor authentication?

A. Username, PIN, and employee ID number
B. Fingerprint and password
C. Smart card and hardware token
D. Voice recognition and retina scan

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

A. Separation of duties
B. Mandatory vacations
C. Background checks
D. Security awareness training

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

A. Black box
B. Regression
C. White box
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

A. Removing the hard drive from its enclosure
B. Using software to repeatedly rewrite over the disk space
C. Using Blowfish encryption on the hard drives
D. Using magnetic fields to erase the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies
D. VPN concentrators
E. Routers

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

A. FTPS

B. SFTP
C. SSL
D. LDAPS
E. SSH

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs
B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 57
A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

A. HTTPS
B. LDAPS
C. SCP
D. SNMPv3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

A. The finding is a false positive and can be disregarded
B. The Struts module needs to be hardened on the server
C. The Apache software on the server needs to be patched and updated
D. The server has been compromised by malware and needs to be quarantined.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Select two.)

A. Geofencing
B. Remote wipe
C. Near-field communication
D. Push notification services
E. Containerization

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

A. ALE
B. AV
C. ARO
D. EF
E. ROI

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

-Initial IR engagement time frame

-Length of time before an executive management notice went out -
Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A company's AUP requires:
▪ Passwords must meet complexity requirements.
▪ Passwords are changed at least once every six months. ▪
Passwords must be at least eight characters long.

An auditor is reviewing the following report:

Username	Last login	Last changed
Carol	2 hours	90 days
David	2 hours	30 days
Ann	1 hour	247 days
Joe	0.5 hours	7 days

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds
B. Account recovery
C. Password expiration

D. Prohibit password reuse

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

A. SPoF
B. RTO
C. MTBF
D. MTTR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

A. Document and lock the workstations in a secure area to establish chain of custody
B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
D. Document findings and processes in the after-action and lessons learned report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users. Which of the following types of attack is MOST likely occurring?

A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

A. steward
B. owner
C. privacy officer
D. systems administrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

A. Public
B. Hybrid
C. Community
D. Private

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A director of IR is reviewing a report regarding several recent breaches. The director complies the following statistics:
▪ Initial IR engagement time frame
▪ Length of time before an executive management notice went out ▪
Average IR phase completion

The director wants to use data to shorten the response time. Which of the following would accomplish this?

A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff

B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies
D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?
A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following differentiates a collision attack from a rainbow table attack?

A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate from being validated

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78

A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A portable data storage device has been determined to have malicious firmware.

Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A user of the wireless network is unable to gain access to the network. The symptoms are:

1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.

Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

Correct Answer: DFI
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.

Which of the following mobile device capabilities should the user disable to achieve the stated goal?

A. Device access control
B. Location based services
C. Application control
D. GEO-Tagging

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first.

Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
D. CPU cache, RAM, paging/swap files, remote logging data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.

Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer securityD. Increase application event logging

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.

Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability

B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code.

Which of the following assessment techniques is BEST described in the analyst's report?
A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are.

The controls used by the receptionist are in place to prevent which of the following types of attacks?

A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

A. ALE
B. MTTR
C. MTBF
D. MTTF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Select TWO.)

A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.

The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD
B. ECDHE
C. Diffie-Hellman
D. HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

A. Vishing
B. Impersonation
C. Spim
D. Scareware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET
/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow

Which of the following attacks is being attempted?

A. Command injection

B. Password attack
C. Buffer overflow
D. Cross-site scripting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A security team wants to establish an Incident Response plan. The team has never experienced an incident.

Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 103
A company has a data classification system with definitions for "Private" and "public". The company's security policy outlines how data should be protected based on type. The company recently added the data type "Proprietary".

Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost
B. More searchable data
C. Better data classification
D. Expanded authority of the privacy officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A security administrator is developing training for corporate users on basic security principles for personal email accounts.

Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single Qfor password recovery

B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

In order to prevent similar situations in the future, the company should improve which of the following?

A. Change management procedures
B. Job rotation policies
C. Incident response management
D. Least privilege access controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it.

Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
C. Install end-point protection on all computers that access web email

D. Create new email spam filters to delete all messages from that sender

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

A. Recovery agent
B. Ocsp
C. Crl
D. Key escrow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 108
An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection.

Which of the following AES modes of operation would meet this integrity-only requirement?

A. HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

QUESTION 110
A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

QUESTION 111
A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.
B. Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement
B. Interconnection security agreement
C. Non-disclosure agreement
D. Business process analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 114
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing
B. Main-in-the-middle
C. URL hijacking
D. Transitive access

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.
Which of the following procedures did Joe follow?

A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

A. Bcrypt
B. Blowfish
C. PGP
D. SHA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:  Login
Success [user: msmith] [Source: 10.0.12.45] [localport: 23]
at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?
A. Configure port security for logons
B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

Which of the following is required to complete the certificate chain?

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop.

Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

A. Remote wipe
B. Full device encryption
C. BIOS password
D. GPS tracking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

A. MD5
B. SHA
C. RIPEMD
D. AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files.

Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

A. Deterrence
B. Mitigation
C. Avoidance
D. Acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4
B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
D. Deny TCP from 192.168.1.10 to 172.31.67.4

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 125
The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

A. Job rotation
B. Least privilege
C. Account lockout
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
C. Using a similar wireless configuration of a nearby network
D. Inundating a target system with SYN requests

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 127
A network technician is trying to determine the source of an ongoing network based attack.

Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

A. Proxy
B. Protocol analyzer
C. Switch
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
The security administrator has noticed cars parking just outside of the building fence line.

Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls
F. Implement a warning banner

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access.

Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.

Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: