312-38Q&As

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

A. Verification

B. Mitigation

C. Remediation

D. Assessment

Correct Answer: C

QUESTION 2

Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm\\'s partners have asked that a secure wireless network be implemented in the office so employees can move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment. What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?

A. The IEEE standard covering wireless is 802.9 and they should follow this.

B. 802.7 covers wireless standards and should be followed

C. They should follow the 802.11 standard

D. Frank and the other IT employees should follow the 802.1 standard.

Correct Answer: C

QUESTION 3

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

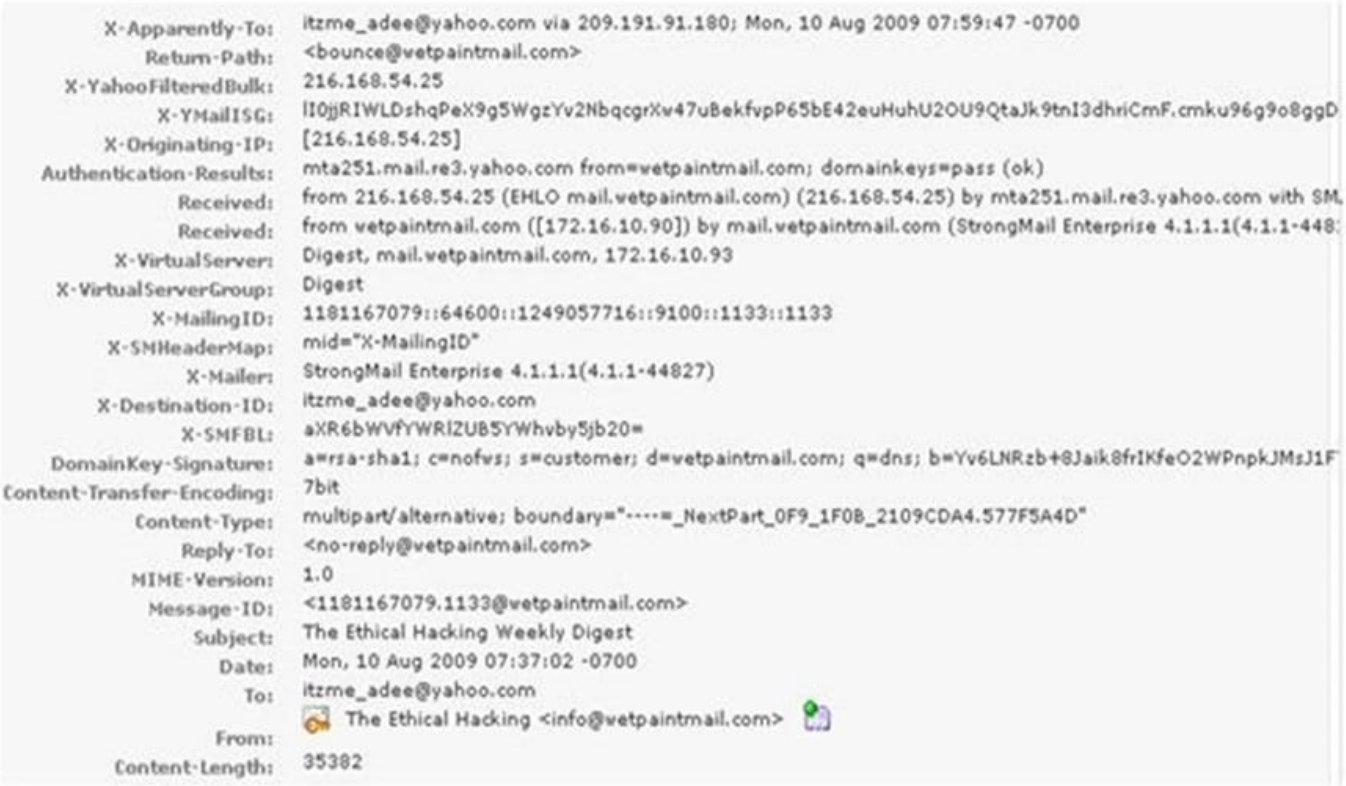
D. Bus topology

Correct Answer: B

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:

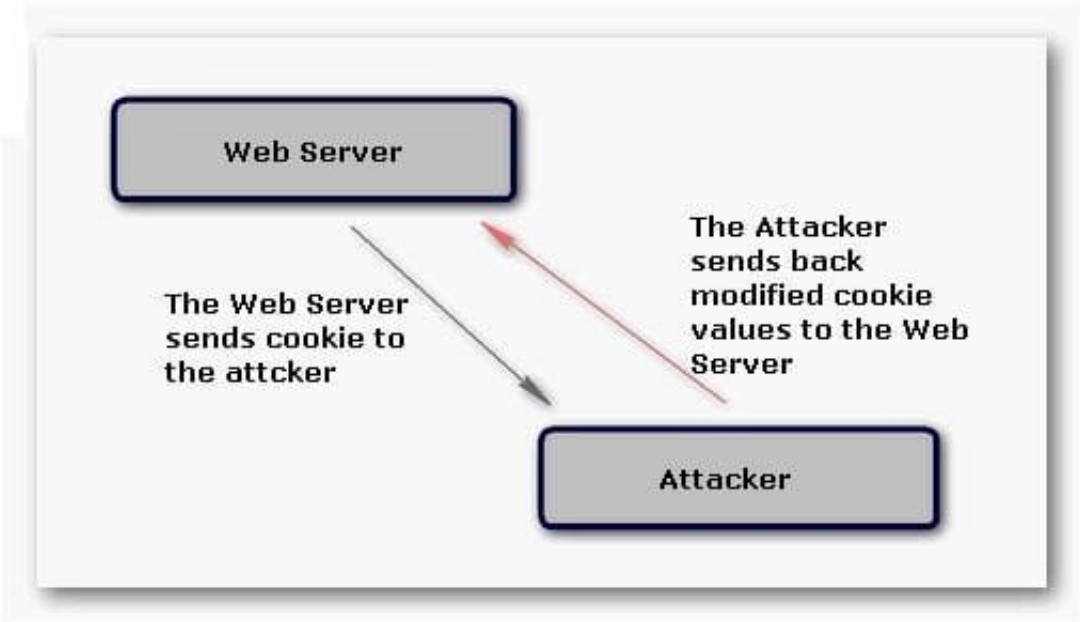
Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new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

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:

1.	Implement	i.	Applies tailoring guidance and supplemental controls as needed
2.	Authorize	ii.	Determines security control effectiveness
3.	Categorize	iii.	Determines risk to organizational operations and assets
4.	Select	iv.	Sets security controls within an enterprise architecture
		v.	Defines criticality of information system according to potential worst-case

QUESTION 4

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

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 5

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

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 6

Which of the following is true regarding any attack surface?

A. Decrease in vulnerabilities decreases the attack surface

B. Increase in vulnerabilities decreases the attack surface

C. Decrease in risk exposures increases the attack surface

D. Decrease in vulnerabilities increases the attack surface

Correct Answer: A

QUESTION 7

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

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 8

Jason has set a firewall policy that allows only a specific list of network services and denies everything else. This strategy is known as a _____.

A. Default allow

B. Default access

C. Default accept

D. Default deny

Correct Answer: D

QUESTION 9

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

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 10

Which BC/DR activity works on the assumption that the most critical processes are brought back from a remote location first, followed by the less critical functions?

A. Recovery

B. Restoration

C. Response

D. Resumption

Correct Answer: A

QUESTION 11

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

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 12

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

QUESTION 13

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

QUESTION 14

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

A. 802.11r

B. 802.11e

C. 802.11a

D. 802.11b

Correct Answer: A

QUESTION 15

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