312-38 Q&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.geekcert.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 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

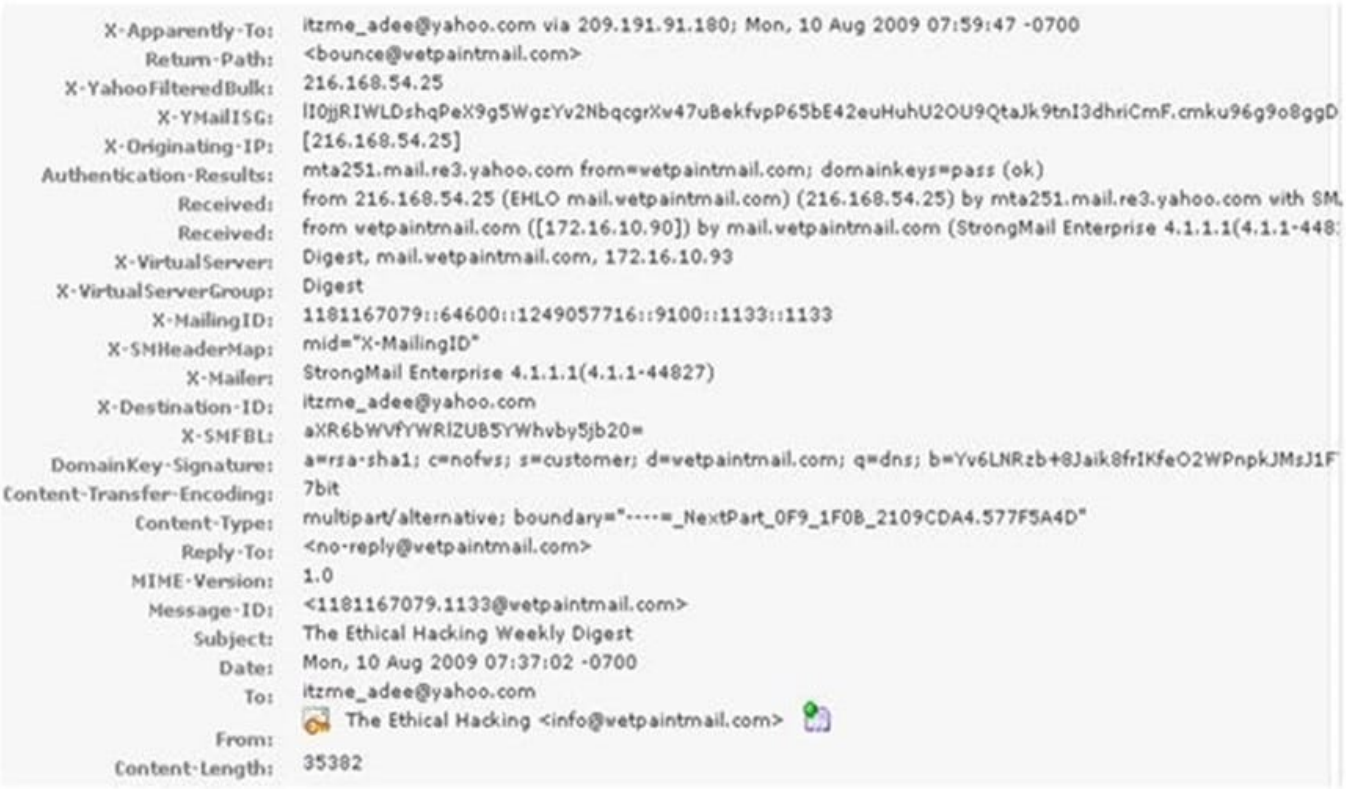
D. Bus topology

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:

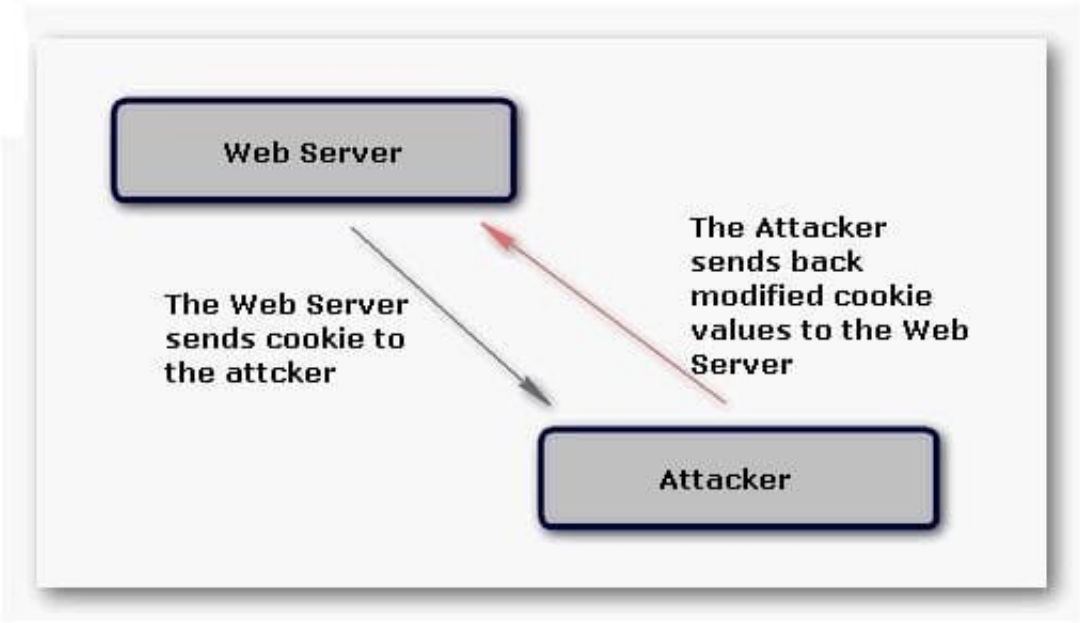
Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new 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 2

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 _____.

F. Kismet

G. Absinthe

H. THC-Scan

I. NetStumbler

Correct Answer: D

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 3

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. 802.11n

C. 802.11e

D. 802.11h

Correct Answer: C

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 4

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

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 5

Which of the following acts as a verifier for the certificate authority?

A. Registration authority

B. Certificate authority

C. Directory management system

D. Certificate Management system

Correct Answer: A