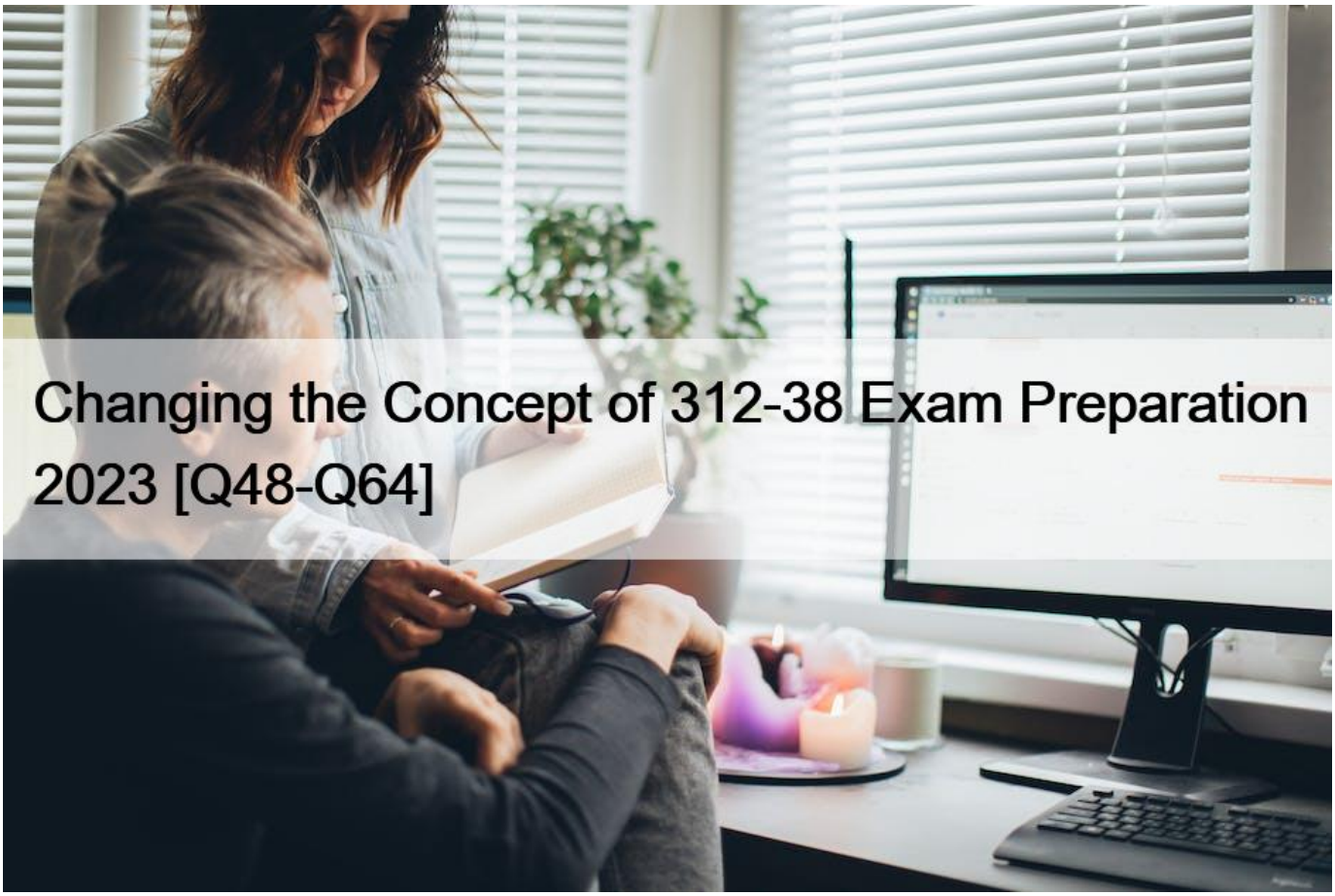
Changing the Concept of 312-38 Exam Preparation 2023 [Q48-Q64



Changing the Concept of 312-38 Exam Preparation 2023
Getting 312-38 Certification Made Easy! Get professional help from our 312-38 Dumps PDF

Topics of Certified Network Defender

Competitors should know the test themes before they start arrangement. Since it will help them in hitting the center. **ECCOUNCIL EC 312-38 exam dumps pdf** will incorporate the accompanying themes:

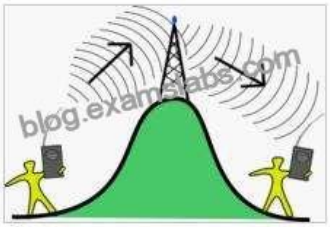
- Network Perimeter Protection- Incident Prediction- Enterprise Virtual, Cloud, and Wireless Network Protection- Application and Data Protection- Incident Response- Endpoint Protection- Network Defense Management **NEW QUESTION 48**

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?

* Gateway
* Repeater
* Network adapter
* Transceiver

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.

NEW QUESTION 49

Which of the following is a device that provides local communication between the datalogger and a computer?
* Controllerless modem
* Optical modem
* Acoustic modem
* Short haul modem

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.

NEW QUESTION 50

George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the_____.
* Archived data
* Deleted data
* Data in transit
* Backup data

NEW QUESTION 51

An employee of a medical service company clicked a malicious link in an email sent by an attacker. Suddenly, employees of the company are not able to access billing information or client record as it is encrypted. The attacker asked the company to pay money for gaining access to their dat a. Which type of malware attack is described above?
* Logic bomb
* Rootkits
* Trojan
* Ransomware

NEW QUESTION 52

Stephanie is currently setting up email security so all company data is secured when passed through email.

Stephanie first sets up encryption to make sure that a specific user’s email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?
* Usability
* Data Integrity
* Availability
* Confidentiality

NEW QUESTION 53

Which of the following IEEE standards defines the token passing ring topology?
* 802.4
* 802.5
* 802.3
* 802.7

NEW QUESTION 54

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?

* user policy
* IT policy
* None
* Group policy
* Subject-specific security

NEW QUESTION 55

Which of the following tools examines a system for a number of known weaknesses and alerts the

administrator?
* Nessus
* COPS
* SATAN
* SAINT

NEW QUESTION 56

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.
* Using WPA encryption
* Not broadcasting SSID
* Using WEP encryption
* MAC filtering the router

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.

NEW QUESTION 57

To provide optimum security while enabling safe/necessary services, blocking known dangerous services, and making employees accountable for their online activity, what Internet Access policy would Brian, the network administrator, have to choose?
* Prudent policy
* Paranoid policy
* Promiscuous policy
* Permissive policy

NEW QUESTION 58

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?
* IGMP
* ICMP
* SNMP
* BGP

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.

NEW QUESTION 59

Which of the following protocols is described as a connection-oriented and reliable delivery transport layer protocol?
* UDP
* IP
* SSL
* TCP

NEW QUESTION 60

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?
* (http = “login.pass.com”) && (http contains “SMTP”)
* (http contains “email”) && (http contains “hotmail”)
* (http contains “hotmail”) && (http contains “Reply-To”)
* (http = “login.passport.com”) && (http contains “POP3”)
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.

NEW QUESTION 61

Sam, a network administrator is using Wireshark to monitor the network traffic of the organization.

He wants to detect TCP packets with no flag set to check for a specific attack attempt. Which filter will he use to view the traffic?
* Tcp.flags==0x000
* Tcp.flags==0000x
* Tcp.flags==000×0
* Tcp.flags==x0000

NEW QUESTION 62

CORRECT TEXT

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.
demilitarized zone

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.

NEW QUESTION 63

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?
* DHCP
* ARP
* Telnet
* None
* SNMP

NEW QUESTION 64

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?
* Sliding Window
* TCP Friendly Rate Control
* Selective Acknowledgment
* Additive increase/multiplicative-decrease

312-38 Exam Crack Test Engine Dumps Training With 171 Questions:
https://www.examslabs.com/EC-COUNCIL/CertifiedEthicalHacker/best-312-38-exam-dumps.html]