Get The Most Updated 312-38 Dumps To Certified Ethical Hacker Certification [Q101-Q118

Get The Most Updated 312-38 Dumps To Certified Ethical Hacker Certification EC-COUNCIL Certified 312-38 Dumps Questions Valid 312-38 Materials

The EC-Council 312-38 test is the required exam for obtaining the Certified Network Defender certification. This certificate covers the individuals' skills in detecting, responding, and protecting against threats on networks. The candidates interested in this path are required to demonstrate their understanding of data transfer, software technologies, and network technologies. They should be able to use their skills to evaluate the subject material and understand the specific software that should be automated.
This certification exam evaluates the applicants' competence in various network defense fundamentals, network security application controls, as well as perimeter appliances, protocols, and VPNs. To succeed in the test, you should also have knowledge of firewall configurations, secure IDS, network traffic signature intricacies, vulnerability, and analysis scanning.

NEW QUESTION 101

Which of the following standards defines Logical Link Control (LLC)?
* 802.2
* 802.3

* 802.5
* 802.4

NEW QUESTION 102

Which of the following is a physical security device designed to entrap a person on purpose?
* Mantrap
* Trap
* War Flying
* War Chalking

NEW QUESTION 103

Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver?
* Hping
* SuperScan
* Netstat
* Nmap

NEW QUESTION 104

Which of the following commands can be used to disable unwanted services on Debian, Ubuntu and other Debian-based Linux distributions?
* # chkconfig [service name]off
* # chkconfig [service name] -del
* # service [service name] stop
* # update-rc.d -f [service name] remove

NEW QUESTION 105

Which of the following types of RAID is also known as disk striping?
* RAID 0
* RAID 2
* RAID 1
* RAID 3

NEW QUESTION 106

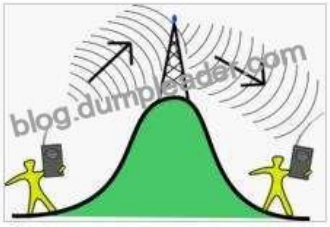
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses 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.
* Dsniff
* Cain
* Libnids
* LIDS

NEW QUESTION 107

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 108

Which encryption algorithm h used by WPA5 encryption?
* RC4.TKIP
* RC4
* AES-GCMP 256
* AES-CCMP

NEW QUESTION 109

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

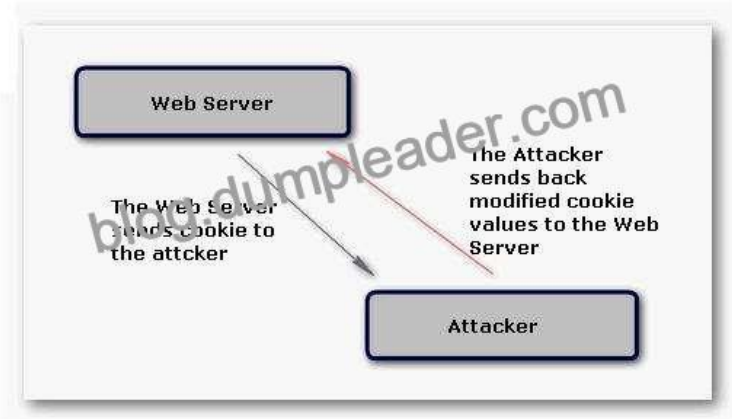
ItemPrice1=1

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?
* Computer-based social engineering
* Man-in-the-middle attack
* Cookie poisoning
* Cross site scripting

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.

NEW QUESTION 110

Identify the network topology where each computer acts as a repeater and the data passes from one computer to the other in a single direction until it reaches the destination.

* Ring

* Mesh
* Bus
* Star

NEW QUESTION 111

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?
* PSAD
* Hping
* NetRanger
* Nmap

NEW QUESTION 112

CORRECT TEXT

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.
CSMA

/CA

Explanation:

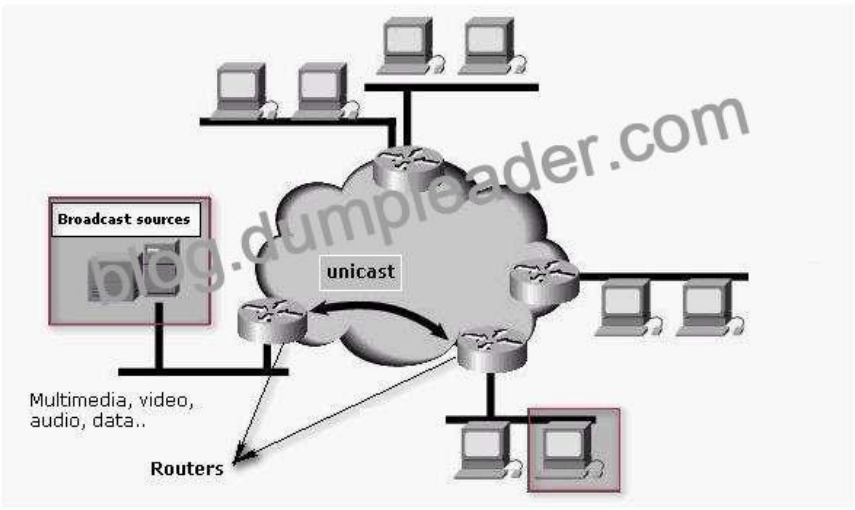
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is an access method used by wireless networks (IEEE 802.11). In this method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel. If the channel is sensed 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.

NEW QUESTION 113

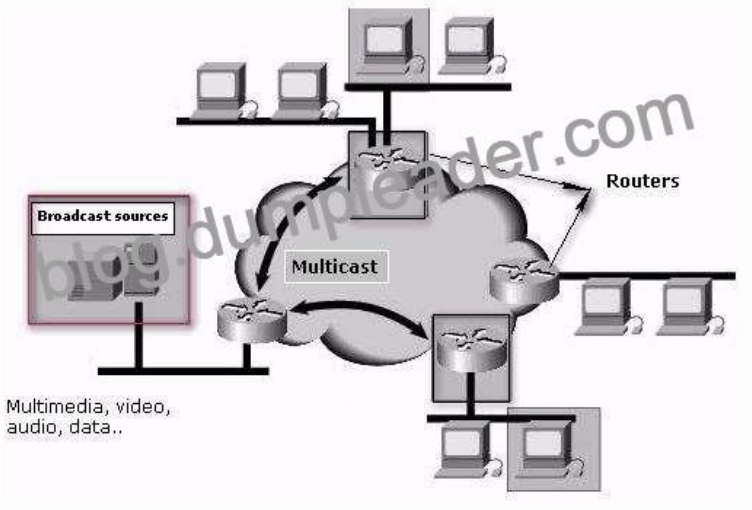
Which of the following types of transmission is the process of sending one bit at a time over a single transmission line?
* Unicast transmission
* Serial data transmission
* Multicast transmission
* Parallel data transmission
In serial data transmission, one bit is sent after another (bit-serial) on 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:



NEW QUESTION 114

Docker provides Platform-as-a-Service (PaaS) through _____ and delivers containerized software packages.
* Server-level virtualization
* Network-level virtualization
* OS-level virtualization
* Storage-level virtualization

NEW QUESTION 115

Michelle is a network security administrator working at a multinational company. She wants to provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across organizations networks without being slowed down and also wants to enable easy and secure sharing of information between devices within an enterprise. Based on the above mentioned requirements, which among the following solution should Michelle implement?

* MEM
* MAM
* MCM
* MDM

NEW QUESTION 116

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.
security

NEW QUESTION 117

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”)

NEW QUESTION 118

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

* access to information
* none
* integrity
* authentication
* confidence