[Q96-Q114 Accurate & Verified 2022 New 312-38 Answers As Experienced in the Actual Test!

Accurate & Verified 2022 New 312-38 Answers As Experienced in the Actual Test!
312-38 Certification Sample Questions certification Exam

Career Opportunities

The EC-Council 312-38 exam equips the professionals with the fundamental knowledge and skills in networking concepts. Without a doubt, earning the Certified Network Defender certification has a lucrative career outlook. Some of the positions that the certified individuals can consider include IT Administrators, Network Technicians, Data Analysts, Network Administrators, and Network Engineers, among others. The average remuneration for these titles is $94,000 per annum.

QUESTION 96

A network designer needs to submit a proposal for a company, which has just published a web portal for its clients on the internet. Such a server needs to be isolated from the internal network, placing itself in a DMZ.

Faced with this need, the designer will present a proposal for a firewall with three interfaces, one for the internet network, another for the DMZ server farm and another for the internal network. What kind of topology will the designer propose?

* Screened subnet
* Multi-homed firewall
* Bastion host
* DMZ, External-Internal firewall

QUESTION 97

What is the range for private ports?

* 49152 through 65535
* 1024 through 49151
* Above 65535
* 0 through 1023

QUESTION 98

Which of the following is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies?
* Gateway
* Router
* Bridge
* Switch

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 99

Which of the following is a mandatory password-based and key-exchange authentication protocol?
* PPP
* CHAP
* VRRP
* DH-CHAP

QUESTION 100

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

* Aircrack

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 101

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

* Adding a second power supply unit
* Performing regular backup of the server
* Adding one more same sized disk as mirror on the server
* Implementing cluster servers’ facility
* Encrypting confidential data stored on the server

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

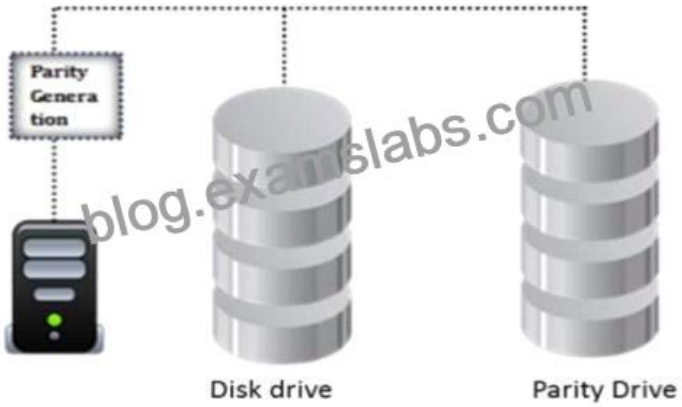
QUESTION 102

What is used for drawing symbols in public places following techniques of advertising an open Wi-Fi network?

* wardriving
* None
* spam
* war call
* warchalking

QUESTION 103

Identify the minimum number of drives required to setup RAID level 5.



Multiple
* 3
* 4
* 2

QUESTION 104

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.
* ToneLoc
* Wingate
* THC-Scan
* NetStumbler
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 105

Which of the following wireless networks provides connectivity over distance up to 20 feet?
* WMAN
* WPAN
* WLAN
* WWAN
Explanation

QUESTION 106

The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

* You should run the up2date -d -f -u command
* You should run the up2data -u command
* You should run the WSUS -d -f -u command.
* You should type the sysupdate -d command

QUESTION 107

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?

* Nmap
* Hping
* NetRanger
* PSAD

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 108

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

* Closed
* Closing
* Close-wait

* Fin-wait-1

QUESTION 109

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?
* Transport layer
* Link layer
* Internet layer
* Application layer

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 110

What is the range for registered ports?
* 1024 through 49151
* 0 through 1023
* Above 65535
* 49152 through 65535

QUESTION 111

Which of the following attack surface increase when you keep USB ports enabled on your laptop unnecessarily?
* Human attack surface
* Network attack surface
* Physical attack surface
* Software attack surface

QUESTION 112

Which of the following is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing?
* Logical Link Control
* Token Ring network
* Distributed-queue dual-bus
* CSMA/CA

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 113

Rick has implemented several firewalls and IDS systems across his enterprise network. What should he do to effectively correlate all incidents that pass through these security controls?
* Use firewalls in Network Address Transition (NAT) mode
* Implement IPsec
* Implement Simple Network Management Protocol (SNMP)
* Use Network Time Protocol (NTP)

QUESTION 114

Which of the following tools examines a system for a number of known weaknesses and alerts the administrator?
* Nessus
* COPS
* SATAN
* SAINT

Final Thoughts

With the recent technological advancements, computer networks are no longer the simple connection of servers and systems managed by network administrators they used to be. They are complex infrastructures that have reduced the globe to a small village. But with this comes the consistent threat of digital attacks. To evade such incidents, most of the independent certification vendors such as the EC-Council are moving ahead of time to create certification paths to validate security experts who can act as the last line of defense against security incidents. Well, if getting a job in this path makes sense to you, check out the EC-Council Certified

Network Defender designation alongside 312-38 evaluation. Simply put, it is a rewarding career track, to say the least.

Certification Topics of 312-38 Exam PDF Recently Updated Questions:
https://www.examslabs.com/EC-COUNCIL/CertifiedEthicalHacker/best-312-38-exam-dumps.html]