312-38$^{\text{Q\&As}}$

Certified Network Defender (CND)

QUESTION 1

Which of the following IEEE standards operates at 2.4 GHz bandwidth and transfers data at a rate of 54 Mbps?

A. 802.11r

B. 802.11n

C. 802.11g

D. 802.11a

Correct Answer: C

QUESTION 2

Disaster Recovery is a

A. Operation-centric strategy

B. Security-centric strategy

C. Data-centric strategy

D. Business-centric strategy

Correct Answer: C

QUESTION 3

Which of the following helps in blocking all unauthorized inbound and/or outbound traffic?

A. IDS

B. IPS

C. Sniffer

D. Firewall

Correct Answer: D

QUESTION 4

James was inspecting ARP packets in his organization\\'s network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating. Which type of attack is James analyzing?

A. ARP Sweep

B. ARP misconfiguration

C. ARP spoofinq

D. ARP Poisioning

Correct Answer: A

QUESTION 5

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 6

A company wants to implement a data backup method that allows them to encrypt the data ensuring its security as well as access it at any time and from any location. What is the appropriate backup method that should be implemented?

A. Cloud backup

B. Offsite backup

C. Hot site backup

D. Onsite backup

Correct Answer: A

QUESTION 7

Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?

A. Scans and probes

B. Malicious Code

C. Denial of service

D. Distributed denial of service

Correct Answer: B

QUESTION 8

Fill in the blank with the appropriate term. is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.

Correct Answer: Banner grabbing

Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. An intruder however can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits. Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat. For example, one could establish a connection to a target host running a Web service with netcat, then send a bad html request in order to get information about the service on the host: [root@prober] nc www.targethost.com 80 HEAD / HTTP/1.1 HTTP/1.1 200 OK Date: Mon, 11 May 2009 22:10:40 EST Server: Apache/2.0.46 (Unix) (Red Hat/Linux) Last-Modified: Thu, 16 Apr 2009 11:20:14 PST ETag: "1986-69b-123a4bc6" Accept-Ranges: bytes Content-Length: 1110 Connection: close Content-Type: text/html The administrator can now catalog this system or an intruder now knows what version of Apache to look for exploits.

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

Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy setting this?

A. AllSigned

B. Restricted

C. RemoteSigned

D. Unrestricted

Correct Answer: A

QUESTION 11

With which of the following forms of acknowledgment can the sender be informed by the data receiver about all segments that have arrived successfully?

A. Block Acknowledgment

B. Negative Acknowledgment

C. Cumulative Acknowledgment

D. Selective Acknowledgment

Correct Answer: D

Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options: The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted". Answer option A is incorrect. Block Acknowledgment (BA) was initially defined in IEEE 802.11e as an optional scheme to improve the MAC efficiency. IEEE 802.11n capable devices are also referred to as High Throughput (HT) devices. Instead of transmitting an individual ACK for every MPDU, multiple MPDUs can be acknowledged together using a single BA frame. Block Ack (BA) contains bitmap size of

64*16 bits. Each bit of this bitmap represents the status (success/ failure) of an MPDU. Answer option B is incorrect. With Negative Acknowledgment, the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly that may need to be retransmitted. Answer option C is incorrect. With Cumulative Acknowledgment, the receiver acknowledges that it has correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

QUESTION 12

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?

A. (http = "login.pass.com") andand (http contains "SMTP")

B. (http contains "email") andand (http contains "hotmail")

C. (http contains "hotmail") andand (http contains "Reply-To")

D. (http = "login.passport.com") andand (http contains "POP3")

Correct Answer: C

Adam will use (http contains "hotmail") andand (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.

QUESTION 13

Which of the following is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing?

A. Logical Link Control

B. Token Ring network

C. Distributed-queue dual-bus

D. CSMA/CA

Correct Answer: C

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 14

Which of the following attacks is a class of brute force attacks that depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations?

A. Phishing attack

B. Replay attack

C. Birthday attack

D. Dictionary attack

Correct Answer: C

A birthday attack is a class of brute force attacks that exploits the mathematics behind the birthday problem in probability theory. It is a type of cryptography attack. The birthday attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations. Answer option D is incorrect. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities. A dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list (from a pre-arranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries, or simple, easily-predicted variations on words, such as appending a digit. Answer option A is incorrect. Phishing is a type of internet fraud attempted by hackers. Hackers try to log into system by masquerading as a trustworthy entity and acquire sensitive information, such as, username, password, bank account details, credit card details, etc. After collecting this information, hackers try to use this information for their gain. Answer option B is incorrect. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

QUESTION 15

Which of the following is a physical security device designed to entrap a person on purpose?

A. Mantrap

B. Trap

C. War Flying

D. War Chalking

Correct Answer: A