Vendor: EC-Council

Exam Code: 312-38

Exam Name: EC-Council Certified Network Defender Certification Exam

Version: DEMO

QUESTION 1
Which of the following DDoS attacks overloads a service by sending inundate packets?

A. Network-centric attack
B. Application-centric attack
C. Web-centric attack
D. System-centric attack

Answer: A
Explanation:
In the context of DDoS (Distributed Denial of Service) attacks, a network-centric attack is one that targets the network layer of a system's architecture. This type of attack aims to overload a service by inundating it with a flood of packets, which can be achieved through methods like ICMP floods or UDP floods. These attacks consume the bandwidth of the targeted site, effectively saturating it with traffic and preventing legitimate traffic from being processed.

QUESTION 2
John, who works as a team lead in Zen Technologies, found that his team members were accessing social networking sites, shopping sites and watching movies during office hours. He approached the network admin to block such websites. What kind of network security device can be used to implement John's decision?

A. Firewall
B. Internet Content Filter
C. Proxy server
D. Network Protocol Analyzer

Answer: B
Explanation:
An Internet Content Filter is the most appropriate network security device for John's situation. It is designed to block access to specific categories of websites, such as social networking and video streaming sites, which are not related to work. This aligns with the objectives of the EC-Council's Certified Network Defender (CND) program, which includes understanding and implementing various network security controls and devices to protect the network from unauthorized access and misuse.

QUESTION 3
Which encryption algorithm does S/MIME protocol implement for digital signatures in emails?

A. Rivest-Shamir-Adleman encryption
B. Digital Encryption Standard
C. Triple Data Encryption Standard
D. Advanced Encryption Standard

Answer: A
Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol implements the Rivest-Shamir-Adleman (RSA) encryption algorithm for digital signatures in emails. Digital signatures are a key component of S/MIME, providing authentication, message integrity, and non-repudiation. RSA is a widely used public-key cryptosystem that facilitates secure data transmission and is known for its role in digital signatures. It works on the principle of asymmetric cryptography, where a pair of keys is used: a public key, which is shared openly, and a private key, which is kept secret by the

owner. In the context of S/MIME, the sender's email client uses the sender's private key to create a digital signature, and the recipient's email client uses the sender's public key to verify the signature.

QUESTION 4
On which of the following OSI layers does the Pretty Good Privacy (PGP) work?

A. Application
B. Data Link
C. Network
D. Transport

Answer: A
Explanation:
Pretty Good Privacy (PGP) is an encryption program that provides confidentiality, integrity, and authentication for data communication. PGP operates at the Application layer of the OSI model. This is because it is used to encrypt and decrypt texts, emails, files, directories, and whole disk partitions and to enhance the security of email communications. PGP provides these services by utilizing cryptographic privacy and authentication through a hybrid approach that combines symmetric and asymmetric encryption, which is implemented at the Application layer.

QUESTION 5
Identify the firewall technology that monitors the TCP handshake between the packets to determine whether a requested session is legitimate.

A. Packet Filtering Firewall
B. Stateful Multilayer Inspection
C. Circuit Level Gateway
D. Network Address Translation

Answer: B
Explanation:
Stateful Multilayer Inspection firewalls monitor the state of active connections and determine which network packets to allow through the firewall. They are designed to inspect the TCP handshake, which is the initial connection setup process between two hosts in a network. By monitoring this handshake, the firewall can determine whether a requested session is legitimate. This technology allows the firewall to not only filter packets based on predefined rules but also to ensure that the packets are part of an established and approved connection.

QUESTION 6
What is the IT security team responsible for effectively managing the security of the organization's IT infrastructure, called?

A. Grey Team
B. Red Team
C. Blue Team
D. Yellow Team

Answer: C
Explanation:
In the context of cybersecurity, the Blue Team refers to the group responsible for defending an

organization's IT infrastructure. This team's primary focus is on internal security measures, maintaining defensive protocols, and ensuring that the organization's systems and data are protected against cyber threats. They are tasked with the effective management of security controls, incident response, and the overall maintenance of the organization's cybersecurity posture.

QUESTION 7
Identify the attack where an attacker manipulates or tricks people into revealing their confidential details like bank account information, credit card details, etc.?

A. Social Engineering Attacks
B. Port Scanning
C. DNS Footprinting
D. ICMP Scanning

Answer: A
Explanation:
The attack described in the question is a Social Engineering Attack. This type of attack involves manipulating or deceiving people into divulging confidential information such as bank account details, credit card numbers, and other sensitive data. Social engineering attacks exploit human psychology rather than technical hacking techniques to gain access to systems, networks, or physical locations, or for financial gain. Attackers may use various tactics such as phishing, pretexting, baiting, or tailgating to trick individuals into providing the information they seek1.

QUESTION 8
An IT company has just been hit with a severe external security breach. To enhance the company's security posture, the network admin has decided to first block all the services and then individually enable only the necessary services. What is such an Internet access policy called?

A. Prudent Policy
B. Permissive Policy
C. Promiscuous Policy
D. Paranoid Policy

Answer: D
Explanation:
The Paranoid Policy is a type of Internet access policy that is characterized by initially blocking all services and then selectively enabling only those that are necessary. This approach is often taken as a security measure following a severe external breach, as it allows the network administrator to ensure that only essential and secure services are accessible, minimizing potential vulnerabilities.

QUESTION 9
Which of the following standards does a cloud service provider has to comply with, to protect the privacy of its customer's personal information?

A. ISO/IEC 27018
B. ISO/IEC 27019
C. ISO/IEC 27020
D. ISO/IEC 27021

Answer: A
Explanation:
ISO/IEC 27018 is a code of practice for cloud service providers that handle personally identifiable information (PII). It provides a framework for protecting the privacy of PII in the cloud, consistent with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. This standard is particularly relevant for cloud service providers needing to demonstrate they have implemented effective privacy controls to protect their customers' data. The adoption of ISO/IEC 27018 by a cloud service provider is a strong indication of compliance with privacy laws and regulations, ensuring the protection of personal information in the cloud.

QUESTION 10
A stateful multilayer inspection firewall combines the aspects of Application level gateway, Circuit level gateway and Packet filtering firewall. On which layers of the OSI model, does the Stateful multilayer inspection firewall works?

A. Network, Session & Application
B. Physical & application
C. Session & network
D. Physical, session & application

Answer: A
Explanation:
A stateful multilayer inspection firewall operates across multiple layers of the OSI model, specifically the Network, Session, and Application layers. It combines the features of packet filtering, circuit-level gateway, and application-level gateway firewalls. This type of firewall inspects the state and context of network traffic, ensuring that all packets are part of a known and valid session. It can make decisions based on the connection state as well as the contents of the traffic, providing a thorough inspection across these layers.

QUESTION 11
The SOC manager is reviewing logs in AlienVault USM to investigate an intrusion on the network. Which CND approach is being used?

A. Preventive
B. Reactive
C. Retrospective
D. Deterrent

Answer: B
Explanation:
The SOC manager reviewing logs in AlienVault USM to investigate an intrusion is employing a reactive approach. This approach is characterized by actions taken in response to an event or incident that has already occurred. In this context, the SOC manager is analyzing the logs to understand the intrusion after it has been detected, which is a form of reactive security measure.

QUESTION 12
An organization's web server was recently compromised triggering its admin team into action to defend the network. The admin team wants to place the web server in such a way that, even if it is attacked, the other network resources will be unavailable to the attacker. Moreover, the network monitoring will easily detect the future attacks. How can the admin team implement this plan?

A. They can place the web server outside of the organization in a remote place
B. They can remove the web server from their organization
C. They can place it in a separate DMZ area behind the firewall
D. They can place it beside the firewall

Answer: C
Explanation:
Placing the web server in a separate Demilitarized Zone (DMZ) behind the firewall is a security best practice that allows an organization to isolate its public-facing services from the internal network. This setup ensures that if the web server is compromised, the attacker would not have direct access to the internal network resources. Additionally, the DMZ provides a controlled environment where network traffic to and from the web server can be monitored effectively, facilitating the detection of any future attacks. The firewall serves as a barrier, with specific rules that only allow necessary communication to and from the DMZ, thereby enhancing the overall security posture of the organization.

QUESTION 13
Daniel works as a network administrator in an Information Security company. He has just deployed an IDS in his organization's network and wants to calculate the false positive rate for his implementation. Which of the following formulae can he use to so?

A. False Negative/False Negative+True Positive
B. False Positive/False Positive+True Negative
C. True Negative/False Negative+True Positive
D. False Negative/True Negative+True positive

Answer: B
Explanation:
The false positive rate is a measure used to evaluate the performance of an IDS (Intrusion Detection System). It is calculated by dividing the number of false positives (FP) by the sum of false positives and true negatives (TN). The formula is:
False Positive Rate=FP+TNFP
This formula helps in determining how often the IDS incorrectly classifies an event as a threat, which is actually benign. A lower false positive rate indicates a more accurate IDS.

QUESTION 14
Which of the following attack signature analysis techniques are implemented to examine the header information and conclude that a packet has been altered?

A. Context-based signature analysis
B. Content-based signature analysis
C. Atomic signature-based analysis
D. Composite signature-based analysis

Answer: D
Explanation:
Composite signature-based analysis is a technique used in intrusion detection systems to examine multiple attributes or behaviors over time to identify potential threats. This method can analyze packet headers to detect anomalies that may indicate a packet has been altered. It looks at a series of packets or fragments to determine if they are part of a legitimate session or if they have been manipulated as part of an attack, such as overlapping fragments which cannot be reassembled properly. This approach is more comprehensive than atomic signature-based

analysis, which examines single events or packets in isolation, and provides a more contextual understanding compared to context-based or content-based analyses.

QUESTION 15

Patrick wants to change the file permission of a file with permission value 755 to 744. He used a Linux command chmod [permission Value] [File Name] to make these changes. What will be the change in the file access?

A. He changed the file permission from rwxr-xr-x to rwx-r--r--
B. He changes the file permission from rwxr-xr-x to rw-rw-rw-
C. He changed the file permission from rw------- to rw-r--r--
D. He changed the file permission from rwxrwxrwx to rwx------

Answer: A
Explanation:
In Linux file permissions, the numerical value 755 represents the permissions rwxr-xr-x, where `r' stands for read, `w' for write, and `x' for execute. The first digit `7' corresponds to the file owner's permissions, allowing read, write, and execute. The second and third digits `5' and `5' correspond to the group and others' permissions, allowing read and execute. Changing the permission to 744 changes the group and others' permissions to read only (r-), removing the execute permission.

QUESTION 16

David, a network and system admin, encrypted all the files in a Windows system that supports NTFS file system using Encrypted File Systems (EFS). He then backed up the same files into another Windows system that supports FAT file system. Later, he found that the backup files were not encrypted. What could be the reason for this?

A. EFS could only encrypt the files that follow NTFS
B. FAT files cannot be encrypted
C. EFS is not the encryption system used in Windows
D. Copied files loses their encryption

Answer: A
Explanation:
The Encrypting File System (EFS) is a feature of the NTFS file system that provides encryption at the file system level. It is designed to work specifically with NTFS and does not support the FAT file system. When files encrypted with EFS are copied or backed up to a volume that uses the FAT file system, the encryption is lost because FAT does not support EFS encryption. This is why David found that the backup files were not encrypted after transferring them to a system that supports the FAT file system.

QUESTION 17

Wallcot, a retail chain in US and Canada, wants to improve the security of their administration offices. They want to implement a mechanism with two doors. Only one of the doors can be opened at a time. Once people enter from the first door, they have to be authorized to open the next one. Failing the authorization, the person will be locked between the doors until an authorized person lets him or her out. What is such a mechanism called?

A. Mantrap
B. Physical locks
C. Concealed detection device

D. Alarm system

Answer: A
Explanation:
The apt-get command is a powerful and free package management utility for Debian-based Linux distributions. It is used for handling packages and is utilized to install, update, and remove software on Debian systems. The apt-get command is the recommended tool for doing upgrades from one Debian GNU/Linux release to another, as it effectively manages dependencies and ensures that all necessary changes are made during an upgrade.

QUESTION 18
Which wireless networking topology setup requires same channel name and SSID?

A. Ad-Hoc standalone network architecture
B. Infrastructure network topology
C. Hybrid topology
D. Mesh topology

Answer: B
Explanation:
In an infrastructure network topology, all wireless devices communicate through an access point/base station. The access point serves as the central transmitter and receiver of wireless radio signals. Mainstream wireless APs support the configuration of the same channel name (frequency) and SSID (Service Set Identifier) to facilitate seamless communication between devices. This setup is essential for devices to identify and connect to the correct network, especially in environments where multiple networks may overlap.

QUESTION 19
Which component of the data packets is encrypted in Transport mode encryption of an IPsec server?

A. Payload
B. Header
C. Header and Payload
D. Encryption is not used in IPsec server

Answer: A
Explanation:
In Transport mode encryption of an IPsec server, only the payload of the data packet is encrypted. This mode is designed to encrypt the message within an IP packet, while the header remains unencrypted. Transport mode is used for end-to-end communication between a client and a server, where the server can interpret the headers to route the packet to the correct application or process.

QUESTION 20
Which of the following network security protocols protects from sniffing attacks by encrypting entire communication between the clients and server including user passwords?

A. TACACS+
B. RADIUS
C. CHAP

D. PAP

Answer: A
Explanation:
TACACS+ (Terminal Access Controller Access-Control System Plus) is a network security protocol that provides centralized authentication for users who are attempting to gain access to the network. It is designed to protect against sniffing attacks by encrypting the entire packet, which includes both the authentication credentials and the subsequent communication after the credentials have been accepted. This encryption ensures that sensitive information such as user passwords is not transmitted in plain text where it could be intercepted by unauthorized individuals. Unlike RADIUS, which only encrypts the password, TACACS+ encrypts the entire authentication process, providing a higher level of security.

QUESTION 21
Which of the following Wireshark filters allows an administrator to detect SYN/FIN DDoS attempt on the network?

A. tcp.flags==0x003
B. tcp.flags==0X029
C. TCP.flags==0x300
D. tcp.dstport==7

Answer: B
Explanation:
The correct Wireshark filter to detect a SYN/FIN DDoS attempt is tcp.flags==0X029. This filter is designed to capture packets where both the SYN and FIN flags are set, which is an unusual combination and indicative of a SYN/FIN attack. In a typical three-way TCP handshake, the SYN and FIN flags are not set in the same TCP segment. A SYN flag is used to initiate a connection, and a FIN flag is used to politely close a connection. Therefore, seeing both flags set in the same packet suggests a possible SYN/FIN DDoS attack.

QUESTION 22
What should a network administrator perform to execute/test the untrusted or untested programs or code from untrusted or unverified third-parties without risking the host system or OS?

A. Application Whitelisting
B. Application Blacklisting
C. Deployment of WAFs
D. Application Sandboxing

Answer: D
Explanation:
Application sandboxing is a security technique that allows untrusted or untested programs or code to be executed in a separate, restricted environment known as a sandbox. This environment is isolated from the host system and operating system, ensuring that any potential malicious behavior contained within the code cannot affect the host. It's a way to test and execute third-party applications without risking the integrity or security of the main system. Sandboxing provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory, which prevents the programs from affecting other processes and data on the host system.

QUESTION 23
In what type of IoT communication model do devices interact with each other through the internet, primarily using protocols such as ZigBee, Z-Wave, or Bluetooth?

A. Back-End Data-Sharing Model
B. Device-to-Gateway Model
C. Device-to-Cloud Model
D. Device-to-Device Model

Answer: D
Explanation:
In the context of IoT communication models, the Device-to-Device (D2D) model refers to the direct interaction between devices without the need for intermediary devices or services. This model is characterized by the use of protocols such as ZigBee, Z-Wave, or Bluetooth, which are designed to facilitate direct communication between devices in close proximity. These protocols are commonly used in home automation, where devices like sensors, lights, and locks need to communicate with each other to perform their functions effectively.

QUESTION 24
Identify the network topology in which the network devices are connected such that every device has a point-to-point link to all the other devices.

A. Star Topology
B. Hybrid Topology
C. Mesh Topology
D. Bus Topology

Answer: C
Explanation:
The network topology where every device is connected to every other device through a point-to-point link is known as Mesh Topology. In this arrangement, devices have a dedicated link to each other, ensuring a unique path for data to travel between any two devices. This setup enhances the reliability of the network, as there are multiple paths for data transfer, and if one link fails, the system can continue to operate using alternative paths. Mesh topology is characterized by its robustness and is commonly used in applications where reliability is critical, such as military communications and internet service provider networks.

QUESTION 25
Which mobile-use approach allows an organization's employees to use devices that they are comfortable with and best fits their preferences and work purposes?

A. BYOD
B. COPE
C. COBO
D. CYOD

Answer: A
Explanation:
The mobile-use approach that allows an organization's employees to use devices they are comfortable with and that best fit their preferences and work purposes is Bring Your Own Device (BYOD). This approach offers the most flexibility for employees, as they can bring and use their personal devices for work-related activities. It is a popular choice for companies that wish to

provide a flexible work environment and cater to the diverse preferences of their employees123.

QUESTION 26
What can be the possible number of IP addresses that can be assigned to the hosts present in a subnet having 255.255.255.224 subnet mask?

A. 62
B. 30
C. 14
D. 126

Answer: B
Explanation:
A subnet with a mask of 255.255.255.224 (or /27 in CIDR notation) allows for 32 IP addresses in total. However, the first address is reserved for the network address, and the last is reserved for the broadcast address. This leaves 30 usable IP addresses for hosts within the subnet.

QUESTION 27
Which of the following is an example of Indicators of Attack?

A. Malware
B. Signatures
C. Exploits
D. Remote code execution

Answer: C
Explanation:
Indicators of Attack (IOAs) are behaviors or actions that suggest an attacker's intent to compromise a system. Unlike Indicators of Compromise (IOCs), which are evidence that an attack has already occurred, IOAs focus on the detection of attack attempts before they can cause harm. Exploits are a prime example of IOAs because they are tools or techniques used to take advantage of vulnerabilities in systems, often before any actual damage is done. This can include exploiting security holes, system weaknesses, or software bugs to gain unauthorized access or perform unauthorized actions.

QUESTION 28
USB ports enabled on a laptop is an example of____

A. System Attack Surface
B. Network Attack Surface
C. Physical Attack Surface
D. Software attack Surface

Answer: C
Explanation:
The term "attack surface" refers to the sum of all possible points where an unauthorized user can try to enter data to or extract data from an environment. The enabled USB ports on a laptop are considered a part of the physical attack surface because they allow for physical interaction with the device. This includes the potential for unauthorized devices to be connected, which could be used to compromise security, such as through the introduction of malware or the unauthorized copying of sensitive data.