Name: - Mahee Shah
Assignment-6

Section 1: Multiple Choice

1. What is the primary purpose of a firewall in a network security infrastructure?

a) Encrypting network traffic
b) Filtering and controlling network traffic
c) Assigning IP addresses to devices
d) Authenticating users for network access

Ans:- b) Filtering and controlling network traffic
Explanation:- Firewall main purpose is to monitor and control incoming and outgoing network traffic based on predefined security rules. It acts like a barrier between trusted internal network and untrusted external networks, like the internet, keeping unwanted traffic out.

2. What type of attack involves flooding a network with excessive traffic to disrupt normal operation?

a) Denial of Service (DoS)
b) Phishing
c) Spoofing
d) Man-in-the-Middle (MitM)

Ans:- a) Denial of Service (DoS)
Explanation:- DoS attack is when a attacker sends so much of traffic to the network that it cannot handle, causing it to slow down or even crash completely. This prevents legit users from accessing the services.

3. Which encryption protocol is commonly used to secure wireless network communications?

a) WEP (Wired Equivalent Privacy)
b) WPA (Wi-Fi Protected Access)
c) SSL/TLS (Secure Sockets Layer/Transport Layer Security)
d) AES (Advanced Encryption Standard)

Ans:- b) WPA (Wi-Fi Protected Access)
Explanation:- WPA is widely used to secure wireless networks by providing stronger data encryption compared to WEP. It helps protect the network from unauthorized access and ensures that only authorised users can connect.

4. What is the purpose of a VPN (Virtual Private Network) in a network security context?

a) To create a secure connection to another network over the Internet
b) To assign IP addresses to devices
c) To monitor network traffic
d) To act as a firewall for network security

Ans:- a) To create a secure connection to another network over the Internet
Explanation:- A VPN allows users to create a secure connection to another network over the Internet, which is especially useful for accessing sensitive information remotely. It encrypts the user's internet connection to ensure that the data is safe from prying eyes.

Section 2: True or False

True or False: Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.
Ans:- True
Explanation:- Patch management involves updating software and firmware to fix security issues and enhance system performance. Without regular updates, systems can become vulnerable to attacks.

True or False: A network administrator should perform regular backups of critical data to prevent data loss in the event of hardware failures, disasters, or security breaches.
Ans:- True
Explanation:- Regular backups are crucial to prevent data loss due to hardware failures, disasters, or security breaches. Backups ensure that important data can be recovered in case of any issues.

True or False: Traceroute is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.
Ans:- True

Explanation:- Traceroute is used to track the path data packets take from the source to the destination. It also measures the time it takes for packets to travel, helping diagnose network issues.

Section 3: Short Answer

8. Describe the steps involved in conducting a network vulnerabilitv Assignment.

Ans:-

1. Conducting a network vulnerabilitv assessment involve several steps.
2. First, identify the scope of the assessment by determining which systems and networks need to be tested.
3. Second, gather information about the network through techniques like scanning and probing use of **wireshark.**
4. Third, identify potential vulnerabilities by analyzing the gathered data.
5. Fourth, prioritize the vulnerabilities based on their severity and the potential impact on the network.
6. Lastly, provide recommendations for remediation and mitigation of the identified vulnerabilities.

Explanation:- A network vulnerability assessment helps identify weaknesses in the network that could be exploited by attackers. By following a structured approach, network administrators can identify and address vulnerabilities before they are exploited.

Section 4: Practical Application

9. Demonstrate how to troubleshoot network connectivity issues using the ping command.

Ans:-

1. To troubleshoot network connectivity issues using the ping command, follow these steps.
2. First, open the command prompt or terminal on your computer.
3. Next, type **`ping`** followed by the IP address or domain name of the target device or server you want to test.
4. Press Enter, and the ping command will send packets to the target and display the results.
5. If the ping is successful, you will see a reply from the target device with the round-trip time.
6. else the ping fails, you will see a request timed out message, indicating a connectivity issue.

Explanation:- The ping command is a simple yet effective tool to check if a device is reachable over the network. It helps in diagnosing connectivity problems by showing whether packets can reach the target device and how long it takes.

Section 5: Essay

10. Discuss the importance of regular network maintenance and the key tasks involved in maintaining network infrastructure.

Ans:-

1. Regular network maintenance is essential to ensure the smooth operation and security of the network.
2. Without regular maintenance, networks can become slow, unreliable, and vulnerable to attacks.
3. Key tasks in network maintenance include updating software and firmware, monitoring network performance, backing up critical data, and checking for security vulnerabilities.
4. Regular maintenance helps to identify potential issues before they become major problems and ensures that the network is always running at optimal performance.

Explanation:- Network maintenance is like taking care of a car. Just as a car needs regular oil changes and check-ups to run smoothly, a network needs regular updates, monitoring, and checks to function properly and securely.

1. Which of the following best describes the purpose of a VPN (Virtual Private Network)?

a) Encrypting network traffic to prevent eavesdropping

b) Connecting multiple LANs (Local Area Networks) over a wide area network (WAN)

c) Authenticating users and controlling access to network resources

d) Reducing latency and improving network performance

Ans:- a) Encrypting network traffic to prevent eavesdropping
Explanation:- A VPN's primary purpose is to encrypt network traffic, ensuring that data sent over the network is secure from eavesdropping and unauthorized access. It creates a secure tunnel for data to travel between the user's device and the destination network.