-NAME : - DISHA PRAJAPATI

# Assignment Module 6

# Network Security, Maintenance, and Troubleshooting Procedures

## Section 1: Multiple Choice

1. What is the primary purpose of a firewall in a network security infrastructure?
2. Encrypting network traffic
3. Filtering and controlling network traffic
4. Assigning IP addresses to devices
5. Authenticating users for network access

ANS :- b) Filtering and controlling network traffic

* Filters and controls network traffic to prevent unauthorized access.

1. What type of attack involves flooding a network with excessive traffic to disrupt normal operation?
2. Denial of Service (DoS)
3. Phishing
4. Spoofing
5. Man-in-the-Middle (MitM)

ANS :- a) Denial of Service (DoS)

* Disrupts services by flooding a network with excessive traffic.

1. 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)

* WPA is more secure than WEP and uses stronger encryption (TKIP/AES).

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

ANS :- A VPN provides secure and private communication over a public network (like the Internet).

## Section 2: True or False

1. True or False:

Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

ANS:- True

1. 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

1. 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

## Section 3: Short Answer

1. Describe the steps involved in conducting a network vulnerability Assignment.

ANS:-

1. **Planning** – Decide what part of the network to test.
2. **Information Gathering** – Collect device, IP and service details, using tools like Nmap
3. **Scanning** – check open ports & running services
4. **Vulnerability Detection** – Identify possible security weaknesses.
5. **Analysis** – Check which issues are most risky.
6. **Reporting** – Write down all findings in a report.
7. **Remediation** – Give solutions and fix the problems.

## Section 4: Practical Application

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

ANS:-

**Troubleshooting with Ping Command**

1. ping 127.0.0.1 → Check TCP/IP stack.
2. ping <own IP> → Verify NIC.
3. ping <gateway IP> → Test router connection.
4. ping <LAN device IP> → Check LAN communication.
5. ping 8.8.8.8 → Verify internet.
6. ping google.com → Test DNS resolution.

If ping fails, it shows where the connectivity breaks.

## Section 5: Essay

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

ANS:-

Regular network maintenance is very important to keep the network **secure, fast, and reliable**. It helps to prevent failures, reduce downtime, and protect data from security threats.

**Importance:**

* Keeps network performance smooth.
* Protects against cyber-attacks and vulnerabilities.
* Reduces chances of system crashes and downtime.
* Increases the life of network devices.

**Key Tasks in Maintenance:**

* **Updating software and firmware** – to fix bugs and security issues.
* **Monitoring network traffic** – to detect unusual activities.
* **Regular backups** – to prevent data loss.
* **Checking hardware devices** – routers, switches, cables, etc.
* **Patching vulnerabilities** – applying security patches.
* **Testing connectivity** – ensuring all devices communicate properly.

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

* VPN secures data by encrypting it, so hackers cannot read or steal information.