# module 6: Network Security, Maintenance, and Troubleshooting Procedures

# Section 1: Multiple Choice Assignment

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

ANS : b) Filtering and controlling network traffic

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

ANS : a) Denial of Service (DoS)

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

ANS : b) WPA (Wi-Fi Protected Access)

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

ANS : Purpose of a VPN (Virtual Private Network) in a network security context are :

* Encrypting data for privacy and protection from eavesdropping.
* Securing remote access to private networks.
* Masking IP addresses to bypass geographic restrictions.
* Ensuring safe communication over public or untrusted networks.

# Section 2: True or false

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

ANS : True

6. 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

7. 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

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

ANS : Steps involved in Network Vulnerability Assessment:

1. Define Scope: Identify goals and systems to assess.
2. Gather Information: Collect details about the network and devices.
3. Scan for Vulnerabilities: Use tools to detect security gaps.
4. Prioritize Risks: Rank vulnerabilities by impact and likelihood.
5. Remediate Issues: Fix high-priority vulnerabilities.
6. Document Findings: Create a report with recommendations.
7. Repeat Regularly: Conduct periodic assessments to ensure security.

# Section 4: Practical Application

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

ANS : Steps to Troubleshoot with ping:

1. Ping Localhost: ping 127.0.0.1 – Check if the local system's network stack is working.
2. Ping Default Gateway: ping <gateway\_IP> – Verify connection to the router.
3. Ping External IP: ping 8.8.8.8 – Test internet connectivity (bypasses DNS).
4. Ping Website: ping www.google.com – Check DNS resolution and internet access.
5. Analyze Results:
   * Success: Replies with low latency.
   * Failure: Indicates issues like no route, DNS, or hardware problems.

# Section 5:

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

ANS : Importance of Regular Network Maintenance:

* Prevents Problems: Keeps the network running smoothly and avoids downtime.
* Boosts Security: Protects the network from cyber threats.
* Improves Speed: Helps the network work faster and more efficiently.
* Increases Lifespan: Makes network equipment last longer.

Key Tasks:

1. Update Software: Fix bugs and improve security.
2. Monitor Traffic: Keep an eye on network activity to spot issues.
3. Back Up Data: Regularly back up data to avoid loss.
4. Check Hardware: Inspect and replace faulty equipment.
5. Review Security: Check for security weaknesses.
6. Manage Settings: Ensure network settings are correct and up-to-date.

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

ANS : a) Encrypting network traffic to prevent eavesdropping