Section 1: Multiple Choice

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

infrastructure? Answer:- b) Filtering and controlling network traffic

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

Answer:- a) Denial of Service (DoS)

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

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

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

security context? Answer:-a) Encrypting network traffic to prevent

eavesdropping

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.

Answer:-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.

Answer:-True

7.Trace route is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.

Answer:-True

Section 3: Short Answer

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

Answer:-

Planning C Scope Definition: Identify the network assets to be assessed and set the objectives.

Information Gathering: Collect details about the network architecture, systems, and software in use.

Vulnerability Scanning: Use tools like Nessus, OpenVAS, or Qualys to scan the network for known vulnerabilities.

Analysis C Risk Evaluation: Analyze detected vulnerabilities, prioritize them based on severity, and assess their impact.

Reporting C Documentation: Generate a report outlining the vulnerabilities, risks, and possible mitigation strategies.

Remediation C Follow-up: Implement fixes such as patching, configuration changes, or security policy updates, followed by another assessment to ensure resolution.

Section 4: Practical Application

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

Answer:-The ping command is used to test the connectivity between two network devices.

Step 1: Open Command Prompt (Windows) or Terminal (Linux/macOS).

Step 2: Type ping <destination_IP_or_domain> and press Enter. Example: ping 8.8.8.8

Step 3: Analyze the response:

Reply received: The destination is reachable.

Request timed out: The destination is unreachable, indicating a possible network issue. Unknown host: DNS resolution issue.

Step 4: If there is packet loss, troubleshoot further using tracert or nslookup.

Step 5: Check network cables, router, firewall rules, and IP configuration (ipconfig /all or ifconfig).

Section 5: Essay

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

Answer:-
Ensures network security by applying patches and updates.
Improves performance by reducing network congestion.
Prevents downtime and enhances reliability.
Helps in early detection of security threats.
Ensures compliance with industry standards and regulations.

Key Tasks Involved in Network Maintenance:

Regular Updates C Patching: Keep firmware, OS, and security software up to date.
Monitoring C Logging: Use tools like Wireshark, Nagios, or SolarWinds for real-time monitoring.
Backup C Recovery: Regularly back up critical data to avoid data loss.
Security Audits C Vulnerability Assessments: Conduct routine security checks.
Performance Optimization: Optimize bandwidth usage and network traffic.
Hardware Inspection: Check routers, switches, and servers for wear and tear.