## Assignment:6

***Network Security, Maintenance, and Troubleshooting Procedures Section***

**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.

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. Traceroute 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: 1 Define scope: list in-scope networks, hosts, and services; set rules of engagement.

2 Gather information: inventory assets, OS versions, open ports, and exposures.

3 Scan: run credentialed/uncredentialed scans to detect CVEs and misconfigurations.

4 Validate & prioritize: confirm true positives and rank by severity, likelihood, and business impact.

5 Remediate: patch software/firmware, close unnecessary ports, harden configs, enforce MFA.

6 Reassess: rescan to verify fixes and ensure no regressions.

7 Report: summarize findings, evidence, risk ratings, and remediation status.

**Section 4: Practical Application**

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

Answer: 1 Check local TCP/IP stack: ping 127.0.0.1 (loopback) — validates IP stack.

2 Check own interface: ping — confirms NIC and local firewall.

3 Check default gateway: ping — verifies LAN reachability.

4 Check internet by IP: ping 8.8.8.8 — tests external reachability bypassing DNS.

5 Check DNS resolution: ping google.com — ensures DNS works.

6 Interpret results: timeouts suggest filtering or down links; 'host unreachable' indicates routing issues; packet loss/high latency points to congestion or bad cabling/Wi-Fi.

**Section 5: Essay**

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

Answer: Regular network maintenance keeps systems secure, reliable, and fast. Threats and bugs change constantly; without routine care, small issues—an unpatched device, a misconfigured firewall rule, a failing cable—can escalate into outages or breaches. Consistent maintenance reduces downtime, improves user experience, and lowers long term costs by catching problems early. Key tasks include:

(1) Patch management for operating systems, firmware on routers/switches/APs, and critical apps.

(2) Configuration management—back up device configs, use version control, and standardize baselines.

(3) Monitoring and alerting—track availability, bandwidth, latency, and security logs to detect anomalies quickly.

(4) Security hardening—enforce least privilege, MFA, network segmentation/VLANs, strong Wi Fi (WPA2/WPA3), and updated EDR/antivirus.

(5) Capacity and performance reviews—analyze utilization trends, QoS needs, and WiFi coverage to prevent bottlenecks.

(6) Regular vulnerability assessments and remediation cycles.

(7) Documentation—up to date topology maps, IP addressing plans, and asset inventories.

(8) Backup and recovery—periodic full/incremental backups and restore testing for both data and device configurations.

Together, these practices create a feedback loop: monitoring reveals risks, assessments quantify them, remediation reduces exposure, and documentation ensures repeatability.

Organizations that schedule monthly reviews and quarterly audits typically experience fewer incidents, faster recovery times, and better compliance with standards.

In short, maintenance is not a one time project but an ongoing process that sustains network health and business continuity.