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?

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: A VPN creates a secure, encrypted tunnel between a user's device and a remote server, hiding data from unauthorized access, especially on public networks.

Section 2: True or false

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

Ans: True

2.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

3. 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

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

Ans: Steps for Network Vulnerability Assessment:

1. Define scope — Identify all devices, systems, and assets to be assessed.
2. Gather information — Collect network diagrams, IP ranges, and system details.
3. Scan for vulnerabilities — Use tools like Nessus or OpenVAS to scan all systems.
4. Analyze results — Review scan reports to identify weaknesses and threats.
5. Prioritize risks — Rank vulnerabilities by severity (critical, high, medium, low).
6. Remediate — Patch, update, or configure systems to fix identified vulnerabilities.
7. Re-scan and verify — Confirm that vulnerabilities have been resolved.
8. Document and report — Record findings and recommendations for future reference.

Section 4: Practical Application

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

Ans: Troubleshooting with Ping Command:

- Basic ping: ping [destination IP/hostname] — Tests basic connectivity and measures response time.
- Check for packet loss: Review the summary — any lost packets indicate network issues.
- Ping the default gateway: ping [gateway IP] — If it fails, the problem is on the local network.

- Ping the DNS server: ping [DNS IP] — Checks if name resolution is working.
- Ping an external site: ping google.com — If local pings work but this fails, the issue is with routing or DNS.
- Continuous ping: ping -t [IP] (Windows) or ping [IP] (Linux) — Monitors for intermittent drops.
- Interpret results: High latency or timeouts point to congestion or hardware faults; complete failure indicates no route or firewall blocking.

Section 5: Essay

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

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

Ans: Regular network maintenance ensures the network remains secure, efficient, and reliable. Without it, performance degrades, vulnerabilities grow, and the risk of breaches increases.

Key tasks include:

- Software and firmware updates — Patching devices closes security holes and improves stability.
- Backup management — Regular backups ensure data recovery after failures or attacks.
- Performance monitoring — Tools like SNMP or network analyzers detect bottlenecks and slowdowns early.
- Security audits — Vulnerability scans and penetration tests identify and fix weaknesses before attackers exploit them.

- Hardware inspection — Checking cables, switches, and routers prevents physical failures.
- Log review — Analyzing system and security logs helps detect unusual activity or intrusions.
- Documentation updates — Keeping network diagrams and records current aids in faster troubleshooting.
- Access control review — Ensuring only authorized users have appropriate access reduces insider threat risks.