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?
a) Encrypting network traffic
b) Filtering and controlling network traffic
c) Assigning IP addresses to devices
d) Authenticating users for network access

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

3. 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)

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

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. =**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. = **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. =**True**

Section 3: Short

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

1. Define the Scope and Objectives

- Identify which systems, devices, and network segments will be assessed.
- Set goals such as checking for weak passwords, outdated software, open ports, or misconfigurations.
- Obtain permission and approval before starting the assessment.

2. Collect Network Information (Reconnaissance)

- Gather details about the network, such as IP ranges, devices, services, and operating systems.
- Use tools like Nmap, ipconfig, or traceroute to map the network.
- Understand how data flows and which systems are critical.

3. Identify Network Vulnerabilities

Use automated scanners and manual checks to find weaknesses, such as:

- Unpatched software
- Open or unnecessary ports
- Weak encryption
- Default passwords
- Misconfigured firewalls or routers

  Tools commonly used: Nessus, OpenVAS, Qualys, Nmap scripts.

4. Analyze and Prioritize Vulnerabilities

- Determine how severe each vulnerability is (critical, high, medium, low).
- Prioritize based on potential impact and likelihood of exploitation.
- Focus first on vulnerabilities that expose critical systems.

5. Develop and Implement Remediation Steps

- Install security patches and updates.
- Close unused ports and disable unnecessary services.
- Improve password policies and access controls.
- Reconfigure network devices and firewalls.
- Apply encryption where needed.

6. Verify and Re-Test

- After fixing issues, perform a re-scan to ensure vulnerabilities are resolved.
- Confirm that no new issues were introduced during remediation.

7. Document the Findings and Recommendations

- Record all vulnerabilities found, their severity, and steps taken to fix them.
- Provide recommendations for improving long-term security.
- Submit the final report to management or instructors.

Section 4: Practical Application

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

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

- Press Windows + R, type cmd, and press Enter.

2. Ping the Local Network Adapter (Loopback Test)

Command:

ping 127.0.0.1

Purpose:

- Checks whether the network card and TCP/IP stack are functioning properly.
- If this fails → network adapter or driver problem.

3. Ping Your Own IP Address

Command:

ping <your_IP_address>

Example:

ping 192.168.1.10

Purpose:

- Confirms the computer is correctly configured with an IP address.
- If this fails → IP configuration issue.

4. Ping the Default Gateway (Router)

Command:

ping <gateway_IP>

Example:

ping 192.168.1.1

Purpose:

- Checks if your device can reach the router.
- If this fails → problem with router, cabling, or your device's network interface.

5. Ping an External IP Address

Command:

ping 8.8.8.8

(Google DNS server)

Purpose:

- Confirms the device can reach the internet.
- If this fails but gateway ping works → problem with ISP or modem.

6. Ping a Website (DNS Test)

Command:

ping google.com

Purpose:

- Tests DNS resolution.
- If IP ping works but website ping fails → DNS server issue.

7. Analyze Ping Results

Look for:

- Replies → connection OK
- Request timed out → no response
- High latency → slow network
- Packet loss → unstable connection

Section 5: Essay

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

1. Ensures Network Reliability and Uptime

Regular checks help detect issues early, preventing network failures and minimizing downtime for users and business operations.

2. Improves Network Performance

Maintenance helps remove bottlenecks, optimize bandwidth usage, and ensure devices like routers, switches, and servers run smoothly.

3. Enhances Network Security

With ongoing maintenance, administrators can:

- Apply security patches
- Update firmware
- Review firewall rules
- Detect potential threats

This prevents malware, hacking attempts, and unauthorized access.

4. Supports Scalability and Future Growth

Documentation and regular assessments help plan upgrades and expansions, ensuring the network can handle future needs.

5. Reduces Repair Costs

Identifying problems early prevents major failures that require expensive repairs or replacements.

6. Improves User Satisfaction

A well-maintained network means fewer slowdowns, fewer outages, and a better experience for employees or customers.

Key Tasks Involved in Network Maintenance

1. Updating Software and Firmware

- Install OS updates
- Update router/switch firmware
- Patch security vulnerabilities

2. Monitoring Network Performance

- Use tools to check bandwidth usage, latency, and device health
- Identify slow connections or overloaded devices

3. Checking and Replacing Hardware

- Inspect cables, switches, routers, and access points
- Replace damaged or aging components
- Ensure proper cooling and power supply

4. Reviewing Security Settings

- Update firewall rules
- Check access control lists (ACLs)
- Review user permissions
- Ensure antivirus and security tools are active

5. Backing Up Configuration Files

- Save router and switch configurations
- Backup firewalls, servers, and critical system settings
- Helps restore the network after failure

6. Managing IP Addressing and DHCP

- Verify DHCP server functionality
- Ensure proper IP allocation
- Remove unused or conflicting IP assignments

7. Testing Connectivity

- Use tools like ping, traceroute, and network analyzers
- Ensure internal and external connectivity is stable

8. Maintaining Documentation

- Update network diagrams
- Record changes, device details, and configurations
- Helps troubleshooting and future planning