**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)**

**Section 2: True or false**

**True or False: Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.**

**🡪**True

**True or False: 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

**True or False: 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 Answer**

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

🡪1. Define Scope and Objectives: Identify the systems, networks, and applications that need to be assessed.

2. Asset Inventory: List all network devices, servers, and software that need to be tested.

3. Identify Vulnerabilities: Use vulnerability scanning tools (like Nessus or OpenVAS) to find weaknesses in the network.

4. Risk Assessment: Evaluate the potential impact and likelihood of each vulnerability being exploited.

5. Reporting: Document the findings, provide recommendations, and assign priorities for remediation.

6. Remediation: Address identified vulnerabilities through patches, configuration changes, or other security measures.

7. Retesting: After remediation, retest the network to ensure vulnerabilities have been effectively mitigated.

**Section 4: Practical Application**

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

**🡪**To troubleshoot network connectivity issues using the ping command:

1. Open Command Prompt/Terminal: On a Windows machine, press Win + R, type cmd, and hit Enter. On Linux/macOS, open Terminal.
2. Ping Localhost: Type ping 127.0.0.1 or ping localhost to check if the network stack is functioning properly. If successful, it confirms that the computer’s networking is working.
3. Ping Default Gateway: Type ping [Gateway IP] (e.g., ping 192.168.1.1) to verify if the device can communicate with the router.
4. Ping External Website: Type ping www.google.com to test internet connectivity. A successful response confirms the device can reach the internet.
5. Analyze Results: If any of these pings fail, it indicates where the issue might lie (local machine, router, internet, etc.).

**Section 5: Essay**

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

**🡪**Regular network maintenance is essential for ensuring the reliability, security, and optimal performance of a network infrastructure. Networks are the backbone of modern businesses, and downtime can lead to significant losses in productivity, revenue, and data integrity. Maintenance helps prevent issues before they escalate, ensuring seamless operations.

**Key tasks involved in maintaining network infrastructure**:

1. **Monitoring Network Performance**: Regular monitoring of bandwidth usage, traffic patterns, and device health ensures issues are identified early.
2. **Patch Management**: Keeping software and firmware up to date with the latest security patches prevents exploitation of vulnerabilities.
3. **Backup and Disaster Recovery**: Regularly backing up critical data and having a disaster recovery plan in place ensures data integrity during emergencies.
4. **Security Audits and Updates**: Regular security checks, vulnerability assessments, and updating firewall rules and anti-malware tools ensure protection against cyber threats.

**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**