Module 5: 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

b) Filtering and controlling network traffic

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)

a) Denial of Service (DoS)

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)

b) WPA (Wi-Fi Protected Access)

4. What is the purpose of a VPN (Virtual Private Network) in a network security context?
a)
network traffic to prevent eavesdropping
b) Filtering and blocking malicious websites
c) Restricting access to network resources based on user identity
d) Detecting and mitigating network intrusions and attacks
Encrypting

a) Encrypting network traffic to prevent eavesdropping

Section 2: True or False

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

Answer: True

6. 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.

Answer: True

7. 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.

Answer: True

Section 3: Short Answer

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

Identify network assets (devices, servers, routers).

Scan the network using vulnerability scanning tools.

Identify security weaknesses and open ports.

Analyze risks and their impact on the network.

Apply security patches and configuration fixes.

Document findings and monitor the network regularly.

Section 4: Practical Application

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

Open Command Prompt.

Type `ping 127.0.0.1` to test TCP/IP stack.

Type `ping <gateway IP>` to test local network connectivity.

Type `ping 8.8.8.8` to test internet connectivity.

Type `ping www.google.com` to test DNS resolution.

Analyze replies or packet loss to identify the issue.

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 to ensure security, performance, and reliability of network infrastructure. It helps prevent failures, reduce downtime, and protect against cyberattacks.

Key maintenance tasks include updating firmware and software patches, monitoring network traffic, checking hardware health, managing backups, and reviewing security policies. Regular maintenance also involves checking logs, testing backups, and verifying firewall and antivirus updates.

Proper network maintenance improves system stability, enhances security, and ensures smooth communication between devices, making it critical for any organization.