Module -5 N+ - 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) Encrypt network traffic and create secure tunnel

5. 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

Section 2: True or false

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

Ans: False

7. 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

8.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

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

Ans: The steps involved in conducting a network vulnerability Assignment are described following:

- Define the Scope – Identify which systems and networks to assess.
- Gather Information – Map the network, identify devices, IPs, and services.
- Scan for Vulnerabilities – Use tools like Nessus or OpenVAS to find weaknesses.
- Analyse and Prioritize – Evaluate risks based on severity and impact.
- Report Findings – Document vulnerabilities with recommendations.
- Remediate Issues – Apply patches, fix configs, and strengthen security.
- Verify Fixes – Re-scan to confirm vulnerabilities are resolved.
- Maintain Regular Checks – Schedule ongoing assessments and monitoring.

Section 4: Practical Application

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

Ans:

- If website or host is unreachable
- Then open CMD and type ping command with website name
- If doesn’t work then type IP address of that website
- If works then it’s DNS error, correct it in DNS server
- Re check with ping command

Section 5: ESSAV

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

Ans: Regular network maintenance is important for ensuring better performance, security, and reliability of an organization.

Tasks involved Network Maintenance:

A. Monitoring & Performance Analysis
   - Use tools to track bandwidth, latency, and device health.
   - Analyse logs of network.

B. Firmware & Software Updates
   - Update routers, switches, firewalls, and servers to fix vulnerabilities.
   - Update operating systems and network management software.

C. Security Audits & Vulnerability Management
   - Conduct penetration testing and firewall rule reviews.
   - Implement intrusion detection/prevention systems (IDS/IPS).

D. Backup & Disaster Recovery
   - Regularly back up configurations.
   - Test recovery procedures to ensure business continuity.

E. Hardware Maintenance
   - Check physical devices for wear and tear.
   - Replace outdated equipment to avoid failures.

F. Traffic Management & Optimization
   - Adjust Quality of Service settings to prioritize critical applications.
   - Remove unnecessary network clutter.

G. Documentation & Change Management
   - Maintain updated network diagrams, IP allocations, and policies.
   - Track changes to avoid configuration conflicts.