**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?

**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)**

3. Which encryption protocol is commonly used to secure wireless network communications?

**b. WPA (Wi-fi Protected Access)**

4. What is the purpose of a VPN(Virtual Private Network) in a Network Security Context?

**A VPN (Virtual Private Network) is used to create a secure and encrypted connection between a user's device and a remote network over the internet. The primary purpose of a VPN in network security include.**

**Section :- 2 True or False**

**5. True -** Patch Management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

**6. True -** A network administrator should perform regular backup of critical data to prevent data loss in the event of hardware failures, disaster, or security breaches.

**7. True -** Traceoute is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.

**Section :- 3 Short**

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

A Network vulnerability assessment is a structured process used to identity, analyze, and mitigate security risks in a network.

**1. Define the Scope and Objectives**

. Identify which systems, devices, and applications need to be assessed.

. Determine the goals, such as identifying weak point, ensuring compliance, or preventing cyberattacks.

. Define the assessment boundaries (internal network, external-facing systems, cloud infrastructure, etc.).

**2. Gather Information (Reconnaissance)**

. Collect data about network assets (IP addresses, operating systems, software versions).

. Use network scanning tools like Nmap to discover live hosts, open ports, and services running on the networks.

. Identify network topology and entry points that attackers might target.

**3. Preform Vulnerability Scanning**

. Use automated Vulnerability Scanner like Nessus, OpenVAS, or Qualys to detect known security weaknesses.

. Unpatched software or outdated firmware.

. Weak Password and misconfiguration

. Open ports and unnecessary services

. Documents all identified vulnerabilities for further analysis.

A **network vulnerability assessment** is an ongoing process that helps organizations **proactively identify and fix security weaknesses** before attackers exploit them. By following these steps, businesses can **strengthen their cybersecurity posture and protect sensitive data**.

👉 **Key Takeaway:** **"Regular vulnerability assessments reduce security risks, improve compliance, and enhance overall network security."** 🔐

**Section -4 Practical - Done**

**Section 5 -**

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. Encryption Network traffic to prevent eavasbropping.**