*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?*

*ANS. Filtering and controlling network traffic*

*2.* *What type of attack involves flooding a network with excessive traffic to disrupt normal operation?*

*ANS. Denial of Service (DoS)*

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

*ANS. WPA (Wi-Fi Protected Access)*

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

*ANS. Encrypting network traffic to prevent eavesdropping*

*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.*

*Ans: 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.*

*Ans: 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.*

*Ans: True .*

*Section 3: Short Answer*

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

*ANS. Conducting a network vulnerability assessment involves several critical steps aimed at identifying, analyzing, and mitigating security risks within a network. Here’s a structured approach:*

*1.Planning and Scoping*

*- Define Objectives Determine the purpose of the assessment (e.g., compliance, security enhancement).*

*- Scope the Assessment: Decide which systems, devices, and network segments will be tested. Clarify the rules of engagement and obtain necessary permissions.*

*2. Information Gathering (Reconnaissance)*

*- Passive Reconnaissance: Gather information about the network, like IP ranges, domain names, and services, without directly interacting with the network.*

*- Active Reconnaissance: Conduct direct probes like network scans to map out the network architecture and detect active devices, open ports, and running services.*

*3. Vulnerability Scanning*

*- Use automated tools (e.g., Nessus, OpenVAS) to scan for known vulnerabilities in the network infrastructure, including software versions, misconfigurations, and unpatched systems.*

*4. Manual Testing*

*- Perform manual validation to identify vulnerabilities that automated tools may miss. This includes checking for logic flaws, improper access controls, and configuration errors.*

*5. Vulnerability Analysis*

*- Analyze the identified vulnerabilities to determine their potential impact. This includes understanding the severity, potential exploitation, and the business context.*

*6. Exploitation (Optional)*

*- If within the assessment scope, simulate attacks on identified vulnerabilities to determine if they can be successfully exploited. This is often done in penetration testing engagements.*

*7. Reporting*

*- Document Findings: Create a detailed report highlighting the discovered vulnerabilities, their severity, potential impact, and recommended mitigations.*

*-Risk Prioritization:Rank vulnerabilities based on their risk level, often using frameworks like CVSS (Common Vulnerability Scoring System).*

*8.Remediation Recommendations*

*- Provide actionable recommendations to fix the identified vulnerabilities, such as applying patches, reconfiguring systems, or implementing additional security controls.*

*9. Review and Reassessment*

*- After remediation, conduct a follow-up assessment or a review to ensure that the identified vulnerabilities have been properly addressed and no new issues have emerged.*

*10. Continuous Monitoring*

*- Implement ongoing monitoring strategies to detect and respond to emerging vulnerabilities. This could include periodic scans, updating systems, and threat intelligence monitoring.*

*Tools and Techniques Involved*

*- Network Scanners: Nmap, Wireshark.*

*- Vulnerability Scanners: Nessus, OpenVAS.*

*- Exploitation Frameworks: Metasploit, Burp Suite.*