Assignment Module-6

Que-1. What is the primary purpose of a firewall in a network security infrastructure?

Ans. B)filtering and controlling network traffic

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

Ans. A) Denial of Service(DoS)

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

Ans. WPA(Wi-fi Protected Access)

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

Ans. A VPN wraps your data in encryption and tunnels it safely from point A to point B, so eavesdroppers, ISPs, or hostile networks see noise—not meaning.

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

Ans. True

Que-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

Que-7. 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

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

Ans. 1. Define the Scope and Objectives

Set the rules of engagement.
Identify which networks, systems, and devices are in scope, along with the assessment goals. No scope = accidental outage = instant regret.

2. Asset Identification and Network Mapping

You can’t secure what you don’t know exists.
Inventory all assets—servers, routers, switches,

firewalls, endpoints—and map the network topology to understand data flow and trust boundaries.

3. Information Gathering (Reconnaissance)

Collect technical details such as:

- IP addresses
- Open ports and services
- Operating systems and versions

This builds the foundation for accurate vulnerability detection.

4. Vulnerability Scanning

Use automated tools to scan systems for:

- Missing patches
- Misconfigurations
- Known vulnerabilities (CVEs)

This step highlights weaknesses before attackers do.

5. Vulnerability Analysis and Risk Assessment

Not all vulnerabilities are equal.
Analyze scan results to assess severity, exploitability, and potential impact on the organization.

6. Validation and False-Positive Reduction

Manually verify critical findings to confirm they are real and exploitable. This avoids wasting time fixing issues that don’t exist.

7. Reporting and Documentation

Document findings in a clear report that includes:

- Identified vulnerabilities
- Risk levels
- Affected systems
- Recommended remediation steps

Good reporting turns technical risk into business language.

8. Remediation and Mitigation

Apply patches, reconfigure systems, close unnecessary ports, and implement security controls to eliminate or reduce risks.

9. Re-testing and Continuous Monitoring

Re-scan systems to confirm vulnerabilities are fixed. Security isn’t a one-time event—it’s a cycle.

Que-9. Discuss the importance of regular network maintenance and the key tasks involved in maintaining network infrastructure.

Ans. Regular network maintenance is critical to ensure availability, security, performance, and reliability of network infrastructure. Networks are living systems—left unattended, they decay, slow down, and eventually fail.