Module – 6 : Network Security, Maintenance, and Troubleshooting Procedures

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

Ans. b) Filtering and controlling network traffic

Reason : Firewall's primary purpose is to monitor, filter, and control incoming and outgoing network traffic based on predefined security rules.

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)

Ans. a) Denial of Service(DoS)

Reason : DoS floods the network with traffic to disrupt services.

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)

Ans. b) WPA(Wi-Fi Protected Access)

Reason : WPA is the standard encryption protocol for securing wireless network communications.

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

Ans. Purpose of VPN is to provide a secure, encrypted connection over an untrusted network, ensuring privacy, data protection and safe remote access.

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

Ans. True

Reason : Patch management ensures systems stay protected from unknown vulnerabilities and run efficiently by applying updates to software, applications, and firmware.

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.

Ans. True

Reason : Regular backups protect critical data from loss due to hardware failures, cyberattacks, or disasters, ensuring business continuity.

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

Reason : Traceroute helps track the path data packets take across networks and measures delays at each hop.

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

Ans. **Steps :**

1) Define the scope and objectives of the assessment to know what needs testing.
2) Collect details about devices, IP ranges, and services running in the network.
3) Use tools to detect open ports, outdated softwares, and misconfiguration.
4) Review scan results and classify vulnerabilities based on severity.
5) Test selected vulnerabilities safely to confirm if they can be exploited.
6) Document findings, risks, and impacts in a clear, structured report.
7) Apply fixes such as patches, configuration changes, or closing unused services.
8) Re-scan the network to verify that vulnerabilities are resolved.

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

Ans. **Steps :**

1) Open command prompt to run the network tests.
2) Use ping <IP Address> to check connectivity with a router or local device, shows confirm local network is working.
3) Ping 8.8.8.8 to test internet connectivity, shows that internet is reachable.
4) Check for packet loss, response time, or unreachable message to identify issues.
5) Fix problems by restarting devices, checking cables, or verifying IP/firewall settings.

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

Ans. **Importance :**

- Regular network maintenance is essential to ensure reliability, security and optimal performance of a network.
- Helps prevent unexpected downtime, reduces the risk of cyberattacks and keeps hardware and software functioning efficiently.

Key Tasks :

- Continuously track bandwidth, latency, and device health to detect issues early.
- Apply patches and updates to fix vulnerabilities and improve stability.
- Ensure critical data and device settings are regularly backed up for recovery.
- Inspect cables, routers, switches, and servers for malfunction.
- Review firewall rules, antivirus, and access controls to prevent unauthorized access.
- Maintain records of configurations, changes, and issues for troubleshooting and audits.