Assignment module 6: Network Security, Maintenance, and c 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
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

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)

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)

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

Ans-:

A VPN (Virtual Private Network) is used to create a secure and private connection over the internet. It encrypts your data and hides your real IP address, keeping your online activities safe from ISPs, and other third parties.

True or False:-

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

Ans-:True

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

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

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

1. **Define Scope & Objectives** – Identify network components to test and set security goals.

2. **Gather Network Information** – Collect details about devices, IPs, and operating systems.
3. **Identify Vulnerabilities** – Use tools like Nessus or Nmap to find security weaknesses.
4. **Analyze & Prioritize Risks** – Classify vulnerabilities as low, medium, high, or critical.
5. **Exploitation Testing (Optional)** – Test if vulnerabilities can be exploited.
6. **Document Findings** – Report issues and suggest fixes.
7. **Implement Security Fixes** – Apply patches, update software, and configure firewalls.
8. **Continuous Monitoring** – Regularly reassess security and monitor for new threats.

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

Importance of Regular Network Maintenance

Regular network maintenance is essential for ensuring **optimal performance, security, and reliability** of an organization's IT infrastructure. It helps in:

- **Preventing Downtime:** Reduces the chances of network failures and disruptions.
- **Enhancing Security:** Identifies and fixes vulnerabilities to protect against cyber threats.
- **Improving Performance:** Ensures smooth data flow and efficient network operations.

- **Reducing Costs:** Prevents costly repairs and data loss by addressing issues early.

Key Tasks in Network Maintenance

1. **Software & Firmware Updates** – Keep devices updated to fix bugs and enhance security.

2. **Data Backup & Recovery** – Regularly back up critical data to prevent loss.

3. **Performance Monitoring** – Track network speed and usage to detect slowdowns.

4. **Security Audits** – Review firewalls, access controls, and vulnerability reports.

5. **Hardware Inspection** – Check routers, switches, and cables for faults.

6. **User Access Management** – Update permissions and remove inactive accounts.