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:- b) Filtering and controlling network traffic

2. What type of attack involves flooding a network with excessive traffic to disrupt normal operation?
Ans:- a) Denial of Service (DoS)

3. Which encryption protocol is commonly used to secure wireless network communications?
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 creates a secure, encrypted tunnel between your device and the internet.

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. 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

8. Describe the steps involved in conducting a network vulnerability Assignmen
Ans:- Steps to conduct a network vulnerability assessment:

• Plan the assessment – Decide what to scan (devices, servers, etc.) and when to do it.

• Identify assets – List all systems, IPs, and software in the network.

• Scan the network – Use tools like Nessus, OpenVAS, or Nmap to find weaknesses.

• Analyze results – Check the scan report for open ports, outdated software, or misconfigurations.

• Prioritize risks – Focus first on high-risk vulnerabilities that hackers could easily exploit.

• Fix issues – Apply patches, update software, and close unnecessary ports.

• Document everything – Record what was found and how it was fixed for future tracking.

• Repeat regularly – Do assessments on a regular basis to stay secure.

Section 4: practical

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

Ans:-

Step 1: Check if your PC is working properly
Open Command Prompt and type:

ping 127.0.0.1
 This pings your own system (loopback).
 If it replies, your network adapter is working fine.

Step 2: Check connection with your router

ping 192.168.1.1
 (Use your actual default gateway IP if it’s different)

 If it replies: You're connected to the router (Wi-Fi or cable is fine).
 If it doesn’t: There might be a Wi-Fi/cable problem or IP conflict.

Step 3: Check if another device on the same network is reachable

ping 192.168.1.5
 If this works: Devices are talking to each other.
 If not: The other device may be turned off or disconnected.

Step 4: Check internet access
 Try pinging an external website:

ping google.com
 If this works: You're online!
 If it fails: You might have an issue with your ISP or DNS settings.

Step 5: Check DNS resolution

ping 8.8.8.8
 If this works but google.com didn’t, it’s likely a DNS issue.

Section 5: Long

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

Why is it important?

- Taaki network smooth chale, bina lag ke
- Security update rahe, hackers ka chance kam ho
- Problems time se mil jayein, badi dikkat banne se pehle
- Devices purane ho jayein to unko time pe replace kiya ja sake

Key Tasks jo regularly karne chahiye:

1. Updates check karo

- Router, firewall, switch ka firmware update rakho
- Taaki bugs aur security holes fix ho jayein

2. Network monitor karo

- Tools se dekho speed theek hai ya nahi
- Koi device zyada load to nahi le raha

3. Cables aur hardware check karo

- Loose ya damaged cable ho to replace karo
- Switch ya router heat ho raha ho to clean ya replace karo

4. Backups banao

- Router ke settings ya servers ka data backup
- Agar kuch bigad gaya to easily restore ho jaye

5. Security logs check karo

- Kisi ne unauthorized access ki try to nahi ki
- Firewall ya antivirus alert mila ho to usse review karo

6. Unwanted devices/users hatao

- Jo system use nahi ho raha, uska access band karo
- IP conflict ya security risk kam hote hain

7. Testing karo

- ping, tracert, etc. se connection check karo
- Har corner of network ka health verify karo

8. Sab document karo

- Kya change hua, konsa cable kahan gaya, sab likho
- Kal ko koi problem aaye to easily samjha ja sake