MODULE 6: NETWORK SECURITY,MAINTAINENECE AND TROUBLESHOOTING PROCEDURES

SECTION 1 : MCQ

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

1. . 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

1. 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)

3 (a) Which of the following best describes the purpose of a VPN (Virtual Private Network)?

a) Encrypting network traffic to prevent eavesdropping

b) Connecting multiple LANs (Local Area Networks) over a wide area network (WAN)

c) Authenticating users and controlling access to network resources

d) Reducing latency and improving network performance

ANS: **a) Encrypting network traffic to prevent eavesdropping**

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

ANS:

* **Encrypts your internet data** to keep it safe from hackers.
* **Hides your IP address** to protect your identity online.
* **Lets you use public Wi-Fi safely** (like in cafes or airports).
* **Gives remote access** to your work or home network securely.
* **Bypasses location blocks** (e.g., to access websites or content not available in your country).

**SECTION 2: TRUE OR FALSE**

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

ANS: TRUE

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

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:

1 **Define Scope**

* Decide what parts of the network to check (e.g., servers, devices, applications).

2 **Get Permission**

* Ensure you have approval to scan and test the network.

3 **Information Gathering**

* Find active devices, open ports, and running services using tools like Nmap.

4 **Scan for Vulnerabilities**

* Use scanners (like Nessus or OpenVAS) to find security weaknesses.

5 **Analyze Risks**

* Rate each vulnerability based on how serious and likely it is to be exploited.

6 **Report Findings**

* Create a clear report with issues found, risks, and how to fix them.

7 **Fix and Patch**

* Work on fixing the problems (patching, reconfiguring, etc.).

8 **Re-scan to Verify**

* Check again to make sure the issues are resolved.

9 **Regular Monitoring**

* Repeat assessments regularly to stay secure.

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

ANS:

**Open Command Prompt / Terminal**

* On Windows: Click Start → Type cmd → Press Enter.
* On Mac/Linux: Open Terminal.

**Step 1: Ping Your Own Computer (Loopback Test)**

* Type: ping 127.0.0.1  
  ✅ If replies come, your network card and TCP/IP are working.  
  ❌ If not, there's a local issue.

**Step 2: Ping Your IP Address**

* Type: ping <your IP> (e.g., ping 192.168.1.5)  
  ✅ If it works, your system is connected to the network.  
  ❌ If not, check your adapter or cable/Wi-Fi.

**Step 3: Ping Your Default Gateway (Router)**

* Type: ping <router IP> (usually something like 192.168.1.1)  
  ✅ If it replies, your PC is talking to the router.  
  ❌ If not, check the connection to the router.

**Step 4: Ping a Public IP (Bypass DNS)**

* Type: ping 8.8.8.8 (Google DNS)  
  ✅ If replies come, internet is working.  
  ❌ If it fails, issue may be with ISP or router.

**Step 5: Ping a Website (Test DNS Resolution)**

* Type: ping google.com  
  ✅ If it works, DNS is fine.  
  ❌ If this fails but Step 4 worked → DNS issue.

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

ANS:

**Regular Network Maintenance Is Important:**

* **Keeps the network running smoothly** so users don’t face frustrating slowdowns or outages.
* **Protects against hackers** by fixing security holes before they can be exploited.
* **Makes sure everything is up to date** with the latest software and firmware.
* **Helps find problems early** so they don’t turn into big headaches later.
* **Supports the business** by avoiding downtime that can cost time and money.

**You Need to Maintain a Network:**

* **Update software and firmware** on routers, switches, and firewalls regularly.
* **Check security settings** like passwords and firewall rules to keep hackers out.
* **Monitor network traffic** to spot anything unusual or slow.
* **Back up all device settings** so you can recover quickly if something breaks.
* **Test the network’s speed and connections** often to make sure it’s working well.
* **Physically inspect hardware** like cables and devices for wear or damage.
* **Keep good records** of all changes, updates, and devices in your network.