**Name: - Abhishek Kumar**

**Assignment 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?

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:** A firewall main job is to allow safe data and block harmful data in a network.

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:** A DoS attack overloads a network with traffic so that normal services stop working.

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 used to secure Wi-Fi communications.

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

**Ans:** A VPN provides secure and private communication over a public network (like the Internet).

**Section 2: True or false**

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

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

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

**Section 3: Short**

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

**Ans:**

1. Planning – Decide what to test in the network.
2. Gather Information – Collect details about systems and devices.
3. Scanning – Use tools to find open ports and weaknesses.
4. Find Vulnerabilities – Match results with known problems.
5. Check Risk – See which problems are serious.
6. Report – Write results and give suggestions.
7. Fix – Apply patches and updates.
8. Re-testing – Test again to confirm fixed.

**Section 4: Practical Application**

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

**Ans:**

1. Open Command Prompt/Terminal
2. Type ping command – Example: ping google.com or ping 0.0.0.0 .
3. Check Reply:

* If you see Reply from ... with time values → Connection is OK.
* If you see Request timed out or Destination unreachable → There is a problem.

1. Understand the problem:

* If local IP fails → Problem is with your device or network card.
* If router IP fails → Problem is with router.
* If outside IP/website fails → Problem is with Internet connection.

**Section 5: Essay**

10. Discuss the importance of network documentation in the context of building and managing networks.

**Ans:** Network documentation means keeping written records of network design, devices, IP addresses, configurations, and policies.

**Importance:**

1. Easy Management – Helps administrators understand and manage the network better.
2. Quick Troubleshooting – Problems can be solved faster because all details are available.
3. Future Planning – Useful when upgrading or expanding the network.
4. Security – Helps in tracking devices and applying correct security policies.
5. Teamwork – Different admins can work easily if proper records are available.

1. 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.

**Reason:** VPN encrypts data so no one can read or steal it while traveling over the internet.