**Chauhan Abhishek**

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?
   1. Encrypting network traffic

b) Filtering and controlling network traffic

c) Assigning IP addresses to devices

d) Authenticating users for network access

**Answer:-b) Filtering and controlling network traffic**

1. What type of attack involves flooding a network with excessive traffic to disrupt Normal operation?
   * 1. Denial of Service (DoS)
     2. Phishing
     3. Spoofing
     4. Man-in-the-Middle (MitM)

**Answer:- a) Denial of Service (DoS)**

1. Which encryption protocol is commonly used to secure wireless network

Communications?

* + 1. WEP (Wired Equivalent Privacy)
    2. WPA (Wi-Fi Protected Access)
    3. SSL/TLS (Secure Sockets Layer/Transport Layer Security)
    4. D) AES (Advanced Encryption Standard)

**Answer:-b) WPA (Wi-Fi Protected Access)**

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

**Answer:-** A VPN, which stands for virtual private network, protects its users by encrypting their data and masking their IP addresses. This hides their browsing activity, identity, and location, allowing for greater privacy and autonomy

**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.

**Answer:- 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.

**Answer:- 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.

**Answer:- TRUE**

**Section 3: Short**

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

**Answer:-** A network vulnerability assessment is a systematic review of a system’s security weaknesses.

1.Planning and designing

2.Asset discovery

3.Configuration

4.Network scanning

5.Vulnerability prioritization

6.Report generati

**Section 4: Practical Application**

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

**Answer:-** The ping command is used to check if a local machine can reach a destination. Here are some other ways to troubleshoot network connectivity issues:

Traceroute:-Tracks the path of packets to identify points of latency or packet loss.

Nslookup:-Provides information about a system’s DNS server, such as its domain name and IP address.

Ipconfig:- Displays TCP/IP values, as well as information about DNS, DCHP, and gateways. Ifconfig:-Displays or sets the IP address and netmask of a network interface.

Check network indicators:-Check that all physical connections are working properly.

Contact ISP:-If the issue is related to external connectivity or the local loop, contact your ISP to check for problems or outages on their end.

**Section 5:**

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

**Answer:-**Regular network maintenance is important for keeping a network running smoothly and efficiently.

Some key tasks involved in network maintenance include:

Troubleshooting: Troubleshooting network problems and performing diagnostics

Monitoring: Monitoring network performance and using network monitoring services to identify potential issues

Updating: Updating firmware and software

Security: Reviewing network security settings, conducting vulnerability assessments, and ensuring compliance with security policies

Hardware: Inspecting and replacing hardware

Backup: Backing up critical data

Access control: Checking access control lists

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

1. Encrypting network traffic to prevent eavesdropping
2. Connecting multiple LANs (Local Area Networks) over a wide area Network (WAN)
3. Authenticating users and controlling access to network resources
4. D) Reducing latency and improving network performance

**Answer:-a) Encrypting network traffic to prevent eavesdropping**