

**Assignment : - 1**

**NAME :- JANI SIDHDHARTH V.**

**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**

The primary purpose of a firewall is to filter and control network traffic, allowing or blocking data based on predefined security rules**.**

**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)**

A Denial of Service (DoS) attack floods a network with excessive traffic to disrupt normal operation.

**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)**

WPA (Wi-Fi Protected Access) is commonly used to secure wireless network communications.

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

**Ans:-** The purpose of a VPN (Virtual Private Network) is to provide a secure, encrypted connection between devices over the internet, ensuring privacy, data protection, and safe access to network resources**.**

**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**

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

**Ans:-**

1. Gather Information: Collect network details and configurations.
2. Scan for Vulnerabilities: Use tools to detect security weaknesses.
3. Analyze Risks: Prioritize vulnerabilities based on severity and impact.
4. Document Findings: Report vulnerabilities and recommend fixes.
5. Remediate Issues: Apply patches and improve security controls.
6. Reassess: Verify fixes with follow-up scans.

**Section 4: Practical**

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

**Ans :-** To troubleshoot network connectivity using the ping command:

1. Ping Localhost: Run ping 127.0.0.1 to check if the local machine's network stack is functioning.
2. Ping Default Gateway: Ping the router's IP to verify local network connectivity.
3. Ping External IP: Ping a public IP to check internet access bypassing DNS.
4. Ping Domain Name: Ping a domain to test DNS resolution and external connectivity.
5. Analyze Results: Look for packet loss or high latency to identify issues**.**

**Section 5:**

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

**Ans:-**

Importance of Regular Network Maintenance:  
Ensures optimal performance, prevents downtime, strengthens security, and extends the lifespan of network infrastructure.

Key Tasks:

1. Update Firmware and Software: Apply patches and updates.
2. Monitor Network Performance: Use tools to track traffic and detect issues.
3. Backup Configurations: Regularly save device settings and critical data.
4. Check Hardware: Inspect cables, switches, and routers for wear.
5. Review Security: Update firewalls, anti-virus, and access controls.
6. Test Connectivity: Verify connections and troubleshoot proactively.
7. Audit Logs: Examine logs for unusual activity or errors.

**Section 5:**