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

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)

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)

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

Ans :- Encryption

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 Answer

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

Ans :- Steps to Conduct a Network Vulnerability Assessment

1. Define the Scope.
2. Gather Information
3. Identify Vulnerabilities
4. Analyze the Results
5. Prioritize Vulnerabilities
6. Create a Report
7. Recommend Fixes
8. Implement Remediation
9. Re-scan and Verify

Section 4: Practical Application

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

Ans : -

1. **Open Command Prompt / Terminal**
    - Press Win + R, type cmd, and press Enter.
2. **Ping the Local Host (127.0.0.1)**
    - Command: ping 127.0.0.1
    - Purpose: Checks if your own network card is working properly.
3. **Ping Your Default Gateway (Router IP)**
    - Command example: ping 192.168.1.1

- Purpose: Checks whether your device can reach the router.
- If it fails → problem is between your device and router.

4. **Ping Another Device in the Same Network**
   - Command example: ping 192.168.1.10
   - Purpose: Tests local network connectivity.
   - If response fails → device may be offline or blocked.
5. **Ping a Website or External IP**
   - Command examples:
     - ping google.com
     - ping 8.8.8.8
   - Purpose: Checks internet connectivity.
   - If local pings work but internet pings fail → internet or DNS issue.
6. **Analyze the Ping Results**
   - Reply received: Connection is working.
   - Request timed out: No response—connectivity issue.
   - High latency (ms): Slow network.
   - Packet loss: Unstable connection.
7. **Take Corrective Actions**
   - Restart router or network adapter.
   - Check cables/Wi-Fi settings.
   - Verify IP address and DNS configuration.
   - Contact ISP if external connections still fail.

Section 5: Essay

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

Ans :- Importance of Regular Network Maintenance

1. **Ensures Network Security**
   - Protects the network from viruses, malware, and cyberattacks.
   - Updates security patches and firewall rules to handle new threats.

2. **Improves Network Performance**
    - Reduces slow speed, lag, and network congestion.
    - Keeps devices and services running smoothly.
3. **Prevents Network Failures**
    - Detects issues early before they become serious.
    - Reduces downtime and avoids system crashes.
4. **Increases Reliability**
    - Ensures users can access the network without interruptions.
    - Maintains stable connectivity across all devices.
5. **Protects Important Data**
    - Regular backups prevent data loss during failures or attacks.

Key Tasks Involved in Maintaining Network Infrastructure

1. **Network Monitoring**
    - Check traffic, bandwidth usage, device status, and errors.
2. **Updating Software and Firmware**
    - Apply patches to routers, switches, firewalls, and servers.
3. **Regular Backups**
    - Take backups of critical files, configurations, and databases.
4. **Checking Hardware Components**
    - Inspect cables, routers, switches, and power supply for faults.
5. **Security Management**
    - Update firewall rules, set strong passwords, enable encryption.
    - Review access control and remove unauthorized users.
6. **Performance Testing**
    - Test network speed, latency, and device response time.
7. **Documentation Update**
    - Maintain records of network devices, IP addresses, and changes.
8. **Troubleshooting Issues**
    - Identify and fix connectivity problems quickly.