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

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)

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)

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

Ans:- A **VPN (Virtual Private Network)** enhances network security by **encrypting internet traffic** and establishing a **secure, private connection** between a user’s device and a remote network. This prevents unauthorized access, protects sensitive data from cyber threats, and **hides the user's IP address**, ensuring privacy and anonymity online. VPNs are commonly used for **secure remote access**, bypassing geo-restrictions, and protecting data on public Wi-Fi networks.

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:- Conducting a **network vulnerability assessment** involves the following key steps:

1. **Planning & Scoping** – Define the assessment scope, objectives, and network assets to be tested.
2. **Asset Discovery** – Identify devices, servers, and systems within the network.
3. **Vulnerability Scanning** – Use automated tools to scan for security weaknesses.
4. **Risk Analysis** – Assess the impact and severity of detected vulnerabilities.
5. **Reporting & Documentation** – Summarize findings, risks, and recommended remediation steps.
6. **Remediation & Patching** – Fix vulnerabilities by applying patches, updates, or security measures.
7. **Reassessment** – Conduct follow-up testing to ensure vulnerabilities are resolved.

Regular assessments help **identify and mitigate security risks** before they can be exploited by attackers.

Section 4: Practical Application

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

ANS:- **Troubleshooting Network Connectivity with ping**

1. **Check Internet Connectivity:**

```
ping google.com
```

   - Success: Internet is working.
   - Failure: Check router or ISP.

2. **Check Router Connection:**

```
ping 192.168.1.1
```

   - Success: Router is reachable.
   - Failure: Restart router or check cables.

3. **Check Local Network Devices:**

```
ping 192.168.1.100
```

   - Success: Device is connected.
   - Failure: Check device network settings.

4. **Check Local Network Stack:**

```
ping 127.0.0.1
```

   - Failure: Possible network adapter issue.

Next Steps:

- Restart router/computer.
- Check cables and Wi-Fi.
- Disable firewall temporarily.
- Use tracert or traceroute for deeper analysis.

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

ANS:- **Importance of Regular Network Maintenance**

Regular **network maintenance** is crucial for ensuring **security, performance, and reliability** in an organization's IT infrastructure. It helps **prevent downtime, reduce vulnerabilities, and optimize network performance**, ensuring smooth operations.

Key Tasks in Network Maintenance

1. **Updating Firmware & Software**
    - Apply security patches and updates to prevent vulnerabilities.
    - Keep network devices (routers, switches, firewalls) up to date.
2. **Monitoring Network Performance**
    - Use monitoring tools to track bandwidth usage and detect bottlenecks.
    - Analyze logs to identify potential failures or security incidents.
3. **Backing Up Network Configurations**
    - Regularly back up router, switch, and firewall configurations.
    - Store backups securely to recover quickly in case of failures.
4. **Security Audits & Vulnerability Assessments**
    - Scan for security threats and weak points.
    - Implement firewalls, intrusion detection/prevention systems (IDS/IPS).
5. **Checking Hardware Health**
    - Inspect cables, switches, and routers for physical damage.
    - Replace outdated or malfunctioning hardware to prevent failures.
6. **Managing User Access & Permissions**
    - Review and update user roles and network permissions.
    - Remove inactive accounts and enforce strong authentication policies.
7. **Testing Network Redundancy & Failover Plans**
    - Ensure backup connections and failover systems are operational.
    - Conduct disaster recovery drills to minimize downtime risks.

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