Name: Ashish kumar sahni

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

**Explain:** A firewall’s primary purpose is to filter and control incoming and outgoing network traffic based on an organization previously established security policies.

**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)

**Explain:** A Denial-of-Service attack happen when someone overload on a network or server with so much traffic that it can’t handle regular tasks, causing it to crash or slow down the network or server.

**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 Stand**

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

**Explain:** WPA is the one most people use to keep their wireless networks secure. It’s better than the older WEP.

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

**a) Encrypting network traffic to prevent eavesdropping**

**b) Filtering and blocking malicious websites**

**c) Restricting access to network resources based on user identity**

**d) Detecting and mitigating network intrusions and attacks**

**Ans: a)** Encrypting network traffic to prevent eavesdropping

**Explain:** A VPN main job is to encrypt your data so nobody can spy on what you are doing online, keeping your information private and safe.

**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 because Patch management means regularly updating your software and firmware to fix any security holes and make thing work better. Its like getting updates for your apps to keep them running smoothly and securely.

**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 a network admin should make regular backups of important data to avoid losing it if something bad happens, like a hardware failure, disaster, or security problem.

**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 because traceroute is a tool that helps track the path and measure the time it takes for data to travel from one device to another across a network.

**Section 3: Short Answer**

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

**Ans:** **1.** Plan and Scope: Decide what part of the network to check and get approval.

**2.** Gather Info: Collect details about the network, like IPs and open ports.

**3.** Scan for Vulnerabilities: Use tools to find weaknesses, like outdated software or open ports.

**4.** Manual Testing: Double-check vulnerabilities and do extra tests.

**5.** Assess Risks: Rank vulnerabilities by how dangerous they are.

**6.** Report Findings: Write a report with what you found and how to fix it.

**7.** Fix Issues: Work with the team to fix the problems.

**8.** Re-check: Scan again to make sure everything is fixed.

**9.** Monitor: Keep an eye on the network and do regular checks.

**Section 4: Practical Application**

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

**Ans: Step 1:** Open command prompt on pressing “Win+R” type ‘cmd’ and press ‘Enter’

**Step 2:** Ping the local Host to check the network interface working correctly by pinging the localhost (Loopback address). Type command ping ‘127.0.0.1’ if it successfully indicates that the TCP/IP stack is functioning correctly on your computer.

**Step 3:** Ping the Default Gateway to find the gateway IP on window type “ipconfig” or in macOS/Linux type “ifconfig” or “ip route” command is “ping (gateway IP address)”

**Step 4:** Ping an External IP address command for checking Google’s DNS server command “ping 8.8.8.8” if it successfully working connection to the internet if not the issue might be with your ISP or your network configuration.

**Step 5:** Ping a Domain Name command “ping google .com” if it successful your DNS settings are working correctly. If this fails, but the ping to 8.8.8.8 worked, there might be an issue with your DNS server.

**Step 6:** Interpreting Results

* All successful network is fine.
* fail at step 2 issue with network adapter or settings.
* Fail at step 3 possible router or local network issue.
* Fail at step 4 ISP or router issue.
* Fail at Step 5 DNS problem.

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

**Ans:** Because a network requires reliability, security, and optimal performance, regular network maintenance cannot be ignored. This will help to avoid pitfalls like downtime, improve security, guarantee optimal network performance, achieve compliance, and prolong hardware life, as well as increase scalability.

Basic tasks of network maintenance:

**Software Updates:** Upgrading of software and application of patches is done regularly.

**Monitoring:** Keeping a constant check on performance and security.

**Hardware Checks:** Checking for failures and upgrading hardware as and when necessary.

**Configuration Management:** Configurations of the network are checked and updated regularly.

**Backup and Recovery:** Backing up data regularly and testing disaster recovery plans is another critical function. Conduct known security audits and vulnerability scans, too.

**Bandwidth Management:** Traffic optimization and bandwidth management.

**Documentation:** The maintenance activities should be properly documented and the records kept in detail.

**User Training:** The best practice should also be transferred to users. Regular maintenance provides security, efficiency, and scalability of the network infrastructure.