|  |  |  |
| --- | --- | --- |
| **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 2. Filtering and controlling network traffic 3. Assigning IP addresses to devices 4. Authenticating users for network access   **Ans.** Filtering and controlling network traffic. |
| 2. 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)   **Ans.** (Dos) Denial of Servicex |
| 3. 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. AES (Advanced Encryption Standard)   **Ans.** WPS (Wi-Fi Protected Access) |
| 4. What is the purpose of a VPN (Virtual Private Network) in a network security context?  **Ans.** VPN is a network that provide secure and protect user privacy and also used different location. | |

**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

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

**Ans.**

1. Planning: Define objectives, scope the assessment, and gather network info.
2. Gathering: Map the network, inventory assets, and collect public info on vulnerabilities.
3. Scanning: Use tools (like Nessus or OpenVAS) to scan for known vulnerabilities and check manually for missed issues.
4. Assessment: Prioritize vulnerabilities by severity, likelihood, and impact.
5. Exploitation: Test for exploitability of vulnerabilities using ethical hacking methods.
6. Reporting: Document findings on vulnerabilities, severity, and remediation. Provide evidence and prioritize actions.
7. Remediation: Apply patches, reconfigure systems, strengthen security, and implement controls to reduce risks.
8. Retesting: Confirm vulnerabilities are fixed and conduct regression testing to avoid new vulnerabilities.
9. Continuous Monitoring: It will ensure ongoing surveillance and regular evaluations for proactive security.

**Section 3: Short**

**Section 4: Practical Application**

|  |  |
| --- | --- |
|  | 9. Demonstrate how to troubleshoot network connectivity issues using the ping command. |
|  | **Ans.** In troubleshooting network connectivity issues using this ping command. It is an ping command is a common TCP/IP command used connectivity issues. With the use of ping command, it check the connectivity. Here is the steps from which we can the connectivity of the device or server.  **Steps:**   1. Open Command Prompt. 2. Write text field and then enter the ping IP of the Device or Server. 3. Type the IP address or Domain name of the device or server. 4. And review the ping results. | |

#### Section 5:

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. Reducing latency and improving network performance

**Ans.** Encrypting network traffic to prevent eavesdropping

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 for ensuring that a network operates efficiently, securely, and reliably. It helps prevent issues before they become major problems, the enhances network performance, and ensures that the infrastructure is up-to-date with current technologies.

* **Key Tasks in Network Maintenance:**

1. **Software Updates and Patching:**

**Operating System and Firmware:** Keeping the operating systems of routers, switches, firewalls, and other network devices up-to-date is crucial.

**Security Updates**: Regularly update security software, including antivirus, firewalls, and intrusion detection/prevention systems (IDS/IPS), to protect against new threats.

1. **Backup and Recovery Planning:**

**Data Backup**: Regularly back up important network configurations, settings, and user data.

**Disaster Recovery Plan**: Test disaster recovery procedures to ensure that data can be recovered and that the network can quickly resume normal.

1. **Network Monitoring:** Use tools to constantly monitor network traffic, bandwidth usage, and device performance. Monitoring tools help detect performance.

**Network Analytics**: Analyzing trends in network traffic, such as congestion or bandwidth spikes, can help optimize resource allocation and prevent issues.

1. **Hardware Maintenance:**

**Physical Inspection:** Regularly inspect and clean networking hardware e.g., routers, switches, cables.

**Hardware Upgrades**: Over time, older devices may become outdated. Regular maintenance network hardware needs to be upgraded to meet increased capacity demands.

1. **Network Configuration Management:**

**Change Management:** Carefully document and control any changes made to the network.

**Configuration Backups:** Regularly back up configurations of network devices.

1. **Security Audits and Assessments:**

**Penetration Testing:** Regularly test the network’s defenses by simulating attacks to identify weak points.

**Access Control**: Review user access permissions and authentication mechanisms to ensure that only authorized individuals have access to critical network resources.

1. **Traffic Analysis and Optimization:**

**Bandwidth Management:** Ensure that network traffic is balanced efficiently across the network. Identify any areas where bandwidth is being overused and optimize data flow.

1. **Documentation and Reporting:** Maintain detailed records of network configurations, maintenance activities, performance logs, and security incidents.
2. **Incident Management and Troubleshooting:** Regularly test the network’s response to common issues (e.g., slow speeds, connectivity drops, hardware failures).