|  |  |  |
| --- | --- | --- |
| **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   **Answer =** b) 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)   **Answer =** a) Denial of Service (DoS). |
| **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)   **Answer**= b) WPA (Wi-Fi Protected Access). |
| **4. What is the purpose of a VPN (Virtual Private Network) in a network security context?**  **Answer** = In a network security context, the purpose of a VPN (Virtual Private Network) is to encrypt data and provide secure remote access, ensuring privacy and protection of sensitive information when communicating over the internet. | |



**Section 2: Tr**

**ue or false**

**True**: Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

**True:** A network administrator should perform regular backups of critical data to prevent data loss in the event of hardware failures, disasters, or security breaches.

**True:** Traceroute is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.



**Section 3: Short Answer**

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

**Answer =**

 Planning and Scoping: Define the scope and objectives.

 Information Gathering: Collect network details.

 Vulnerability Scanning: Use automated tools to find vulnerabilities.

 Manual Testing: Verify and find additional issues.

 Penetration Testing: Simulate attacks to assess impact.

 Analysis and Reporting: Prioritize vulnerabilities and document findings.

 Remediation: Fix identified vulnerabilities.

 Verification: Ensure fixes are effective.

 Documentation and Reporting: Compile a comprehensive report.

 Ongoing Monitoring: Continuously monitor and reassess security.

**Section 4: Practical Application**

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

1. Answer= **Open Command Prompt:**
   * On a Windows device, press Win + R, type CMD, and hit Enter.
2. **Ping a website:**
   * Type ping www.example.com and press Enter.
   * This sends packets to the website and waits for a response. If you receive replies, it means the network can reach the website.
3. **Ping an IP Address:**
   * Type ping 8.8.8.8 (Google's public DNS) and press Enter.
   * If you receive replies, it confirms that your network can reach the internet.
4. **Ping Your Router:**
   * Type ping 192.168.1.1 (or your router's IP address) and press Enter.
   * This checks the connection between your device and your router. If you receive replies, the local network is functioning.
5. **Analyse the Results:**
   * If you see "Request timed out" or "Destination host unreachable," there might be a problem with your network connection.
   * Check the round-trip time (in milliseconds) for high latency or packet loss.
6. **Next Steps:**
   * If there's no response, check your network cables, restart your router, or contact your ISP.
   * You can also try other troubleshooting steps, such as resetting your network adapter or using the Windows Network Troubleshooter.

**Section 5:**

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

**Answer= Importance of Regular Network Maintenance:**

1. Enhanced Performance: Regular maintenance helps to identify and resolve performance issues, ensuring that the network runs smoothly and efficiently.
2. Increased Security: By keeping software and hardware up-to-date with the latest patches and updates, regular maintenance helps protect against vulnerabilities and cyber threats.
3. Improved Reliability: Regular checks and updates can prevent unexpected network failures and reduce downtime, ensuring that the network is always available when needed.
4. Cost Savings: Proactive maintenance can detect potential issues before they become major problems, saving on costly repairs and replacements.
5. Compliance: Regular maintenance ensures that the network complies with industry standards and regulations, avoiding potential legal and financial penalties.

**Key Tasks Involved in Maintaining Network Infrastructure:**

1. Monitoring and Analysis: Continuously monitor network performance and traffic patterns to identify and address any issues promptly.
2. Software Updates and Patch Management: Regularly update firmware, operating systems, and applications to protect against security vulnerabilities and enhance performance.
3. Hardware Maintenance: Inspect and maintain network hardware, such as routers, switches, and servers, to ensure they are functioning optimally and replace any faulty components.
4. Backup and Disaster Recovery: Implement and regularly test backup and disaster recovery plans to ensure data integrity and quick recovery in case of a network failure or data loss.
5. Security Management: Perform routine security audits, update firewalls, and implement intrusion detection and prevention systems to safeguard the network from threats.
6. Documentation and Inventory Management: Maintain accurate documentation of network configurations, hardware inventory, and maintenance activities to streamline troubleshooting and future planning.