**ASSIGNMENT – 5:**

**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**

**Answer: (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)**

**Answer:** (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)**

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

**4. 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**

**Answer: (a)** Encrypting network traffic to prevent eavesdropping

|  |
| --- |
| **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.**

**Answer:** 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.**

**Answer:** 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.**

**Answer:** True

|  |
| --- |
| **SECTION 3: SHORT ANSWER** |

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

**Answer:**

* **Asset Discovery:**
  + Identify all devices and systems on the network to be scanned.
* **Scanning and Data Gathering:**
  + Run vulnerability scanning tools to detect potential weaknesses across the network, including open ports, outdated software, and misconfigurations.
* **Analysis and Prioritization:**
  + Evaluate the severity and likelihood of exploitation for each identified vulnerability, assigning priority levels based on potential impact.
* **Reporting and Remediation Plan:**
  + Generate a detailed report outlining vulnerabilities with suggested mitigation strategies and timelines for addressing them.
* **Implementation and Verification:**
  + Apply necessary security patches, configuration changes, and updates to address identified vulnerabilities, then re-scan to confirm successful remediation.

|  |
| --- |
| **SECTION 4: PRACTICAL APPLICATION** |

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

**Answer:**

**Step 1: Verify Local Network Connection**

* Open the command prompt (cmd on Windows or terminal on macOS/Linux).
* Type:
  + **ping 127.0.0.1**
  + This tests if the network adapter (loopback interface) is functioning correctly.
  + A successful response indicates that the local machine's TCP/IP stack is working.

**Step 2: Check Connectivity to the Default Gateway**

* Find the default gateway using:
  + **ipconfig # Windows**

**ifconfig # Linux/macOS (or `ip a`)**

* Ping the default gateway:
  + **ping <gateway\_IP\_address>**
  + If the response is successful, the device can communicate with the local network.
  + If it fails, check the network cables, Wi-Fi connection, or network adapter settings.

**Step 3: Test Connectivity to an External Website (e.g., Google DNS)**

* Try pinging a well-known public IP address:
  + **ping 8.8.8.8**
  + If successful, the network has internet access.
  + If it fails, there may be an issue with the ISP or firewall settings.

**Step 4: Test DNS Resolution**

* If ping 8.8.8.8 works but ping google.com fails, the issue may be with DNS.
* Test DNS resolution by pinging a domain:
  + **ping google.com**
  + If it fails, try changing the DNS server to Google’s (8.8.8.8) in network settings.

**Step 5: Analyze Results and Take Action**

* **Successful pings**: Network is working correctly.
* **Packet loss or high latency**: Network congestion or ISP issues.
* **No response from default gateway**: Local network issue (router/modem).
* **No response from external IPs**: Internet connectivity issue.

|  |
| --- |
| **SECTION 5: ESSAY** |

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

**Answer:**

Regular network maintenance is crucial for ensuring optimal network performance, minimizing downtime, protecting data security, and identifying potential issues before they become major disruptions.

**Key tasks involved in network maintenance:**

* **Monitoring network performance:**
  + Tracking network metrics like bandwidth utilization, packet loss, and latency to identify performance issues.
* **Software and firmware updates:**
  + Regularly installing the latest software patches and firmware updates to address security vulnerabilities and improve stability.
* **Hardware inspections:**
  + Checking the physical condition of network devices like routers, switches, and cables for signs of wear and tear.
* **Backup procedures:**
  + Performing regular backups of critical data to ensure data recovery in case of system failure.
* **Troubleshooting network issues:**
  + Identifying and resolving network problems like connectivity issues, slow performance, or access control issues.