Perform a Network Vulnerability Scan with OpenVAS

Project Description: In this lab, I performed a comprehensive network vulnerability scan using OpenVAS (Open Vulnerability Assessment System). The purpose of this exercise was to identify potential security weaknesses within a simulated network environment. This document outlines the process and results of the scan while providing insights into detected vulnerabilities and mitigation strategies.

---

1. Install and Configure OpenVAS

1. **Environment Setup:**
   - I used a Kali Linux virtual machine as the platform for running OpenVAS.
   - OpenVAS was installed and initialized using the following command:

     ```
     sudo gvm-setup
     ```

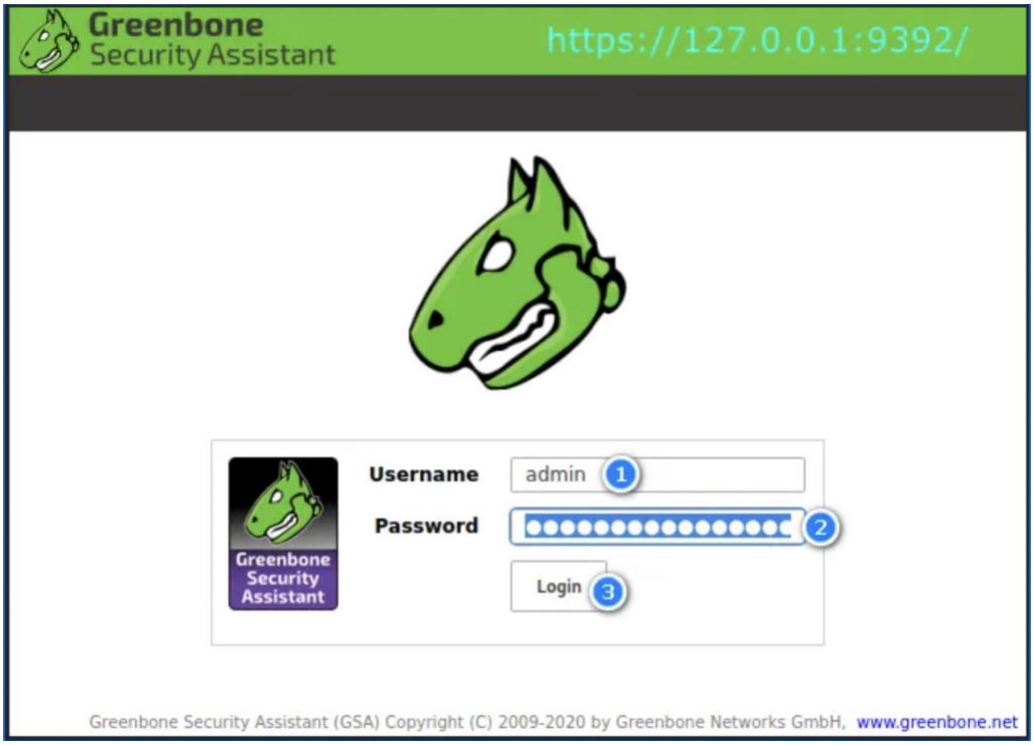
2. **Troubleshooting PostgreSQL Configuration:**
   - During the setup, I encountered an error related to PostgreSQL versions. This was resolved by:
     - Installing PostgreSQL 17.
     - Upgrading the PostgreSQL cluster with:

       ```
       sudo pg_upgradecluster 16 main
       ```

3. **Starting OpenVAS Services:**
   - The services were started with:

     ```
     sudo gvm-start
     ```

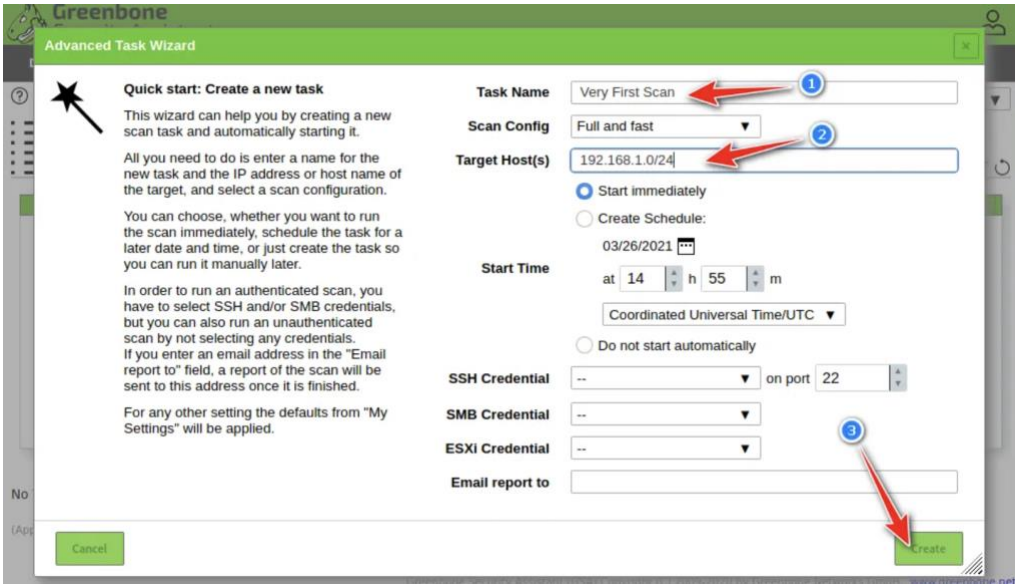
   - The web interface was accessed via https://127.0.0.1:9392.



---

2. Target Definition and Scan Configuration

1. **Defining the Target Network:**
   - The target IP range `192.168.68.0/24` was specified for the scan.
   - OpenVAS was configured to perform a comprehensive scan using its default settings.
2. **Configuring Scan Policies:**
   - Selected the **Full and Fast** policy to ensure a thorough evaluation of vulnerabilities.



---

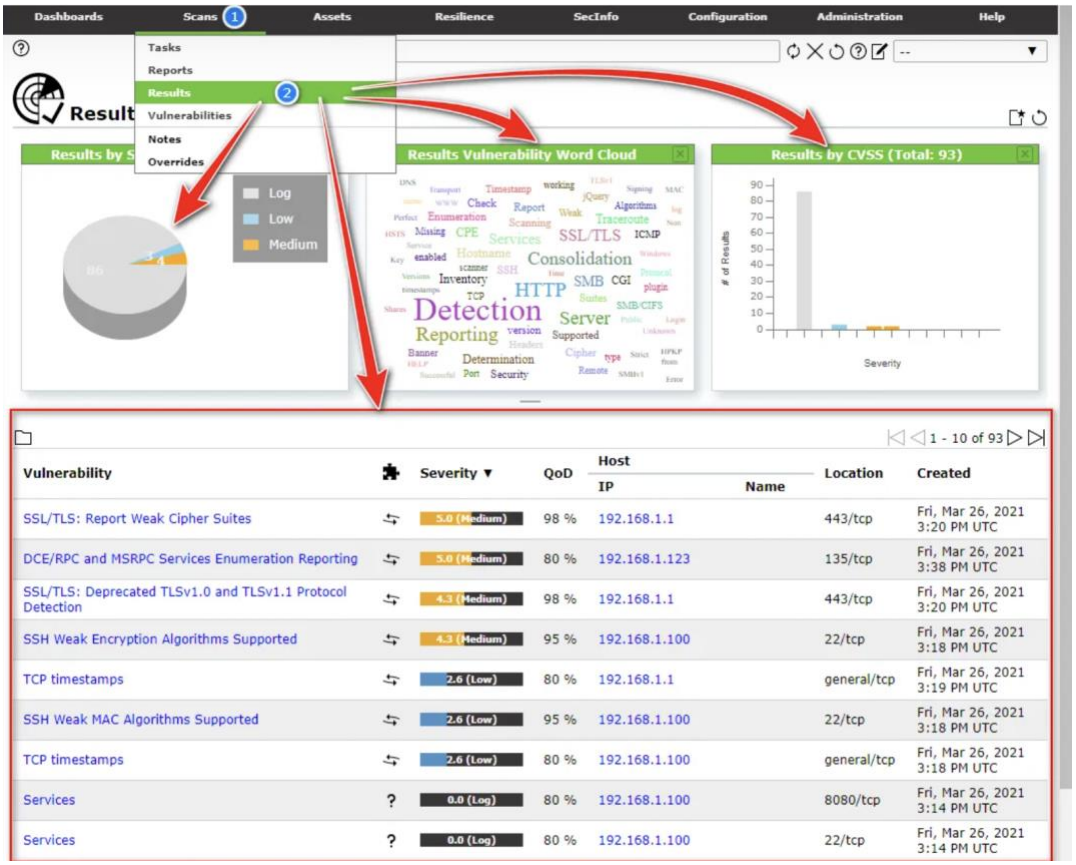
3. Executing the Scan

1. **Launching the Scan:**
   - The scan was initiated from the OpenVAS dashboard by selecting the defined target and chosen scan policy.
2. **Monitoring Progress:**
   - The scan's progress was monitored in real-time through the web interface, which provided a percentage-based completion tracker.

---

4. Results and Analysis

1. **Detected Vulnerabilities:**
   - The scan identified multiple vulnerabilities:
     - **Critical:** Unpatched CVE in Apache HTTP server.
     - **High:** Outdated versions of OpenSSH.
     - **Medium:** Misconfigured firewall rules allowing unnecessary open ports.
2. **Summary Report:**
   - A detailed report was generated, listing vulnerabilities along with their severity levels, descriptions, and potential impacts.



---

5. Mitigation Strategies

1. **Addressing Critical Vulnerabilities:**
   - Applied updates to the Apache HTTP server to address the unpatched CVE.
   - Configured automated patch management to prevent similar issues.
2. **Fixing High-Risk Issues:**
   - Updated OpenSSH to the latest secure version.
3. **Enhancing Firewall Security:**
   - Modified firewall rules to close unnecessary ports and restrict access.

---

6. Lessons Learned

- **Value of Regular Scans:**
  - Regular vulnerability scans are critical for proactive identification and mitigation of security weaknesses.
- **Importance of Timely Updates:**
  - Maintaining up-to-date software versions significantly reduces the risk of exploitation.

Summary: This lab provided hands-on experience in identifying and addressing network vulnerabilities using OpenVAS. The exercise emphasized the importance of regular scans and proactive mitigation strategies to ensure robust network security.