

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.

Greenbone
Advanced Task Wizard

Quick start: Create a new task
This wizard can help you by creating a new scan task and automatically starting it.
All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.
You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.
In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.
If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.
For any other setting the defaults from "My Settings" will be applied.

Task Name Very First Scan (1)

Scan Config Full and fast (2)

Target Host(s) 192.168.1.0/24 (2)

☒ Start immediately
☐ Create Schedule:
03/26/2021 at 14 h 55 m
Coordinated Universal Time/UTC
☐ Do not start automatically

SSH Credential -- on port 22
SMB Credential --
ESXi Credential -- (3)

Email report to --

Cancel Create

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.

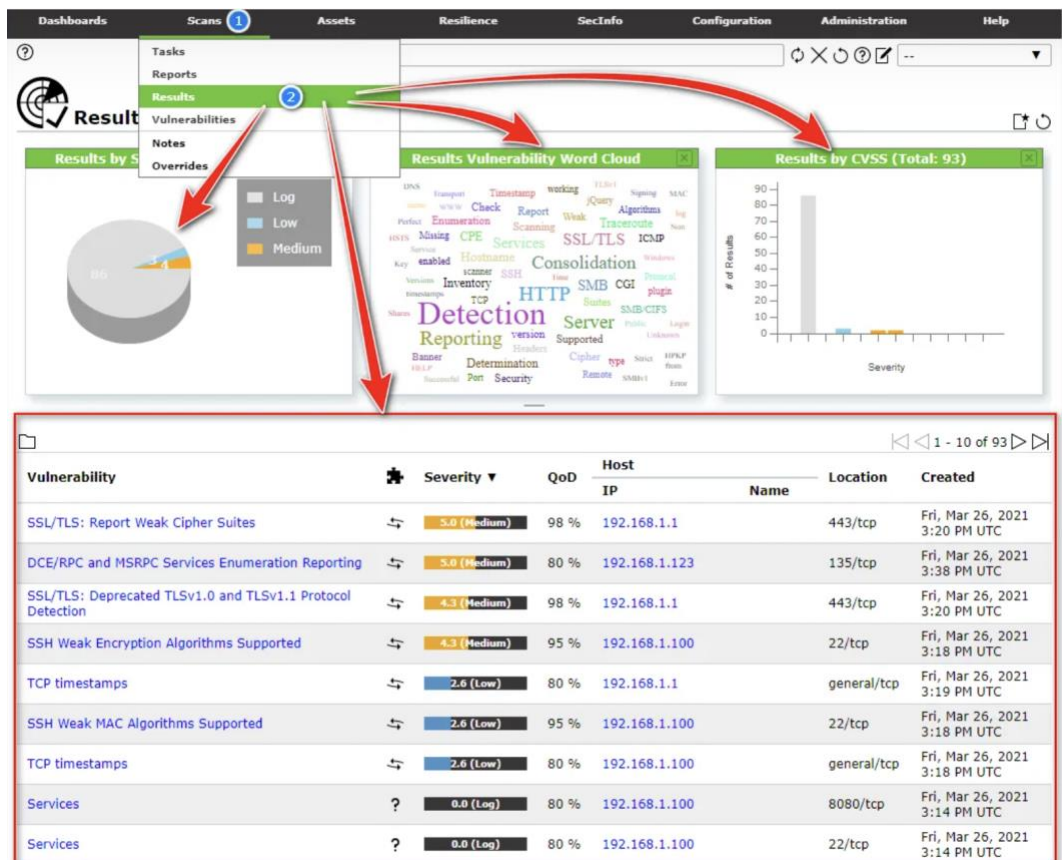
4. Results and Analysis

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.