Greenbone (OpenVAS) Vulnerability Scan

Contents

Time required: 120 minutes

Why Greenbone

Setup Greenbone (formerly OpenVAS) on Kali Linux to scan a target system for vulnerabilities. This assignment aims to help understand basic vulnerability scanning, identifying security weaknesses, and interpreting scan results.

NOTE: Before starting the assignment, please look at **Part 4: Create a Report**. You will want to take screenshots as you go through this tutorial.

Why?

This assignment will give essential hands-on experience with vulnerability management, a core aspect of cybersecurity. By working with Greenbone on Kali Linux, you will learn to configure and execute scans, analyze results, and make risk-based recommendations—skills that are key for identifying and prioritizing vulnerabilities in real-world systems.

1. **Proficiency with Vulnerability Scanning Tools**
    a) Gain familiarity with OpenVAS, a leading open-source tool, being able to operate more effectively in professional cybersecurity environments.
2. **Real-World Security Analysis Skills**
    a) Learn to interpret scan results, prioritize vulnerabilities, and document findings in a structured report—a necessary skill for clear communication with technical and non-technical audiences.
3. **Critical Thinking and Problem Solving**
    a) By analyzing data and making recommendations, you strengthen your ability to assess security issues critically and provide actionable solutions.
4. **Professional and Ethical Foundations**
    a) This assignment reinforces cybersecurity best practices, emphasizing ethical scanning, proper authorization, and the importance of scope and professionalism.
5. **Certification and Career Preparation**
    a) The experience aligns with entry-level certifications and prepares for future roles, enhancing both technical capabilities and readiness for industry challenges.

This assignment helps build technical confidence, professional communication skills, and ethical awareness, equips you with essential tools for a successful career in cybersecurity.

Part 1: Install Greenbone

OS: Kali Linux

1. Open a terminal session.
2. Update Kali Linux. We must do this to make sure that Greenbone has the latest PostgreSQL server and other needed components are up to date.

```
sudo apt update
sudo apt upgrade
```

3. Install Greenbone.

```
sudo apt install gvm
```

4. Initialize Greenbone with the setup command (this may take several minutes as it downloads feeds and configures settings):

```
# This will take some time.
# You may receive an error at this stage.
sudo gvm-setup
# Copy the very long admin password to a text file. You are going to want to copy and paste this very long password, not type it in.
```

5. If you do not receive an error at this stage, go to Finish GVM Installation

GVM Setup PostgresSQL Port Error

You may encounter this error of PostgresSQL did not set the default port propertly

```
-ERROR: No postgresql version uses the port 5432/tcp
-ERROR: libgvmd needs postgresql 16 to use the port 5432
-ERROR: use pg_upgradecluster to update your postgresql cluster
```

This link gives further information and where I found the solution that follows. The following steps should resolve the issue.

https://stackoverflow.com/questions/77905813/error-no-postgresql-version-uses-the-port-5432-tcp

The following steps should resolve the issue.

1. List the pg clusters.

```
# List the pg clusters
pg_lsclusters
```

2. If you see only one version 17 cluster, you can continue to the next step.

NOTE: If you see more than one, follow these steps.

```
# Stop the Postgres version 16 service
sudo pg_ctlcluster 16 main stop
sudo pg_dropcluster 16 main
```

3. Find and edit the configuration file.

```
# Show the configuration file location
sudo -u postgres psql -c 'SHOW config_file'

# This is the location I got. Yours may be different.
# Edit the configuration file
sudo nano /etc/postgresql/17/main/postgresql.conf
```

4. Edit the configuration file. Change the port to the standard port: 5432

```
# - Connection Settings -

#listen_addresses = 'localhost'         # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*'
for all
                                        # (change requires restart)
port = 5432                             # (change requires restart)
max_connections = 100                   # (change requires restart)
#reserved_connections = 0               # (change requires restart)
#superuser_reserved_connections = 3     # (change requires restart)
```

5. Restart the PostgreSQL system service.

```
sudo systemctl restart postgresql
```

6. Run the setup command again.

```
# This will take some time
sudo gvm-setup
# Copy the very long admin password to a text file. You are going to want to
copy and paste this very long password, not type it in.
```

Continue Greenbone Setup

Check to make sure your setup is good. This should succeed without any errors

```
sudo gvm-check-setup
```

Verify Greenbone Installation

1. Run the following commands to make sure everything is up to date.

```
# Stop the greenbone service.
sudo gvm-stop
# Update the feeds, this will take some time.
sudo greenbone-feed-sync
```

2. Verify that the Greenbone service is running.

```
sudo gvm-start
```

3. Open a browser in Kali Linux → go to https://localhost:9392
4. You will get a security warning as we are using a private certificate.
5. Click **Advanced** → **Accept the Risk and Continue**.
6. Log in with the admin credentials created during setup.
7. If you did not save the credentials during set, use the following command to reset the admin password to admin.

```
sudo -E -u _gvm gvmd --user=admin --new-password=admin
```

8. Verify that you have access to the Greenbone dashboard, where you'll conduct and monitor scans.

Part 2: Configure and Perform a Vulnerability Scan

Targets: Possible targets for your vulnerability scan: Anything on your local network, your local computer, firewall, lab.wncc.net. lab.wncc.edu, any device in D1.

1. **Add a Target for Scanning**
    - In the Greenbone dashboard, navigate to **Configuration > Targets**.
    - Click the **New Target** button to set up a target for the scan.
    - Enter a name for the target (e.g., "Test Server").
    - In the **Hosts** field, enter the IP address or host name of the target machine you'll be scanning (use a test machine on a local network or virtual machine for this purpose).
    - Click **Save**.
2. **Create a New Task**

NOTE: It may take some time for Greenbone to synchronize the downloaded information. Let Kali Linux run and go to another assignment. You will notice that the disk activity icon is blinking. You will know it is complete when you have choices under Scan Config.

- Go to **Scans > Tasks** and click **New Task**.
- Enter a name for the task (e.g., "Initial Scan").
- For the **Scan Targets** option, select the target you created earlier.

- Under **Scan Config**, choose **Full and fast** (this is a general scan with a balance of speed and thoroughness).
- Click **Save** to create the task.

3. **Run the Vulnerability Scan**
   - Find the task you created in **Scans > Tasks**.
   - Click the **play** button next to the task to start the scan.
   - The scan may take some time to complete, depending on the target system's size and configuration.

Part 3: Analyze the Scan Results

1. **View Scan Results**
   - Once the scan is complete, go to **Scans > Reports**.
   - Click on the most recent report to view detailed results of the scan.
2. **Identify Vulnerabilities**
   - Review the vulnerabilities found, categorized by severity (e.g., High, Medium, Low).
   - Select a high-severity vulnerability to analyze in more detail.
3. **Document Findings**
   - For each vulnerability you select, note down:
     - Vulnerability name and description.
     - CVE identifier (if available).
     - Suggested remediation steps.

Part 4: Create a Report

1. **Summarize Findings**
   - Write a brief summary of the scan results, including:
     - Number of vulnerabilities by severity.
     - Description of notable vulnerabilities.

2. **Recommendations**
    - Based on the identified vulnerabilities, provide general security recommendations (e.g., software updates, configuration changes).
    - Include specific remediation steps for the high-severity vulnerability you analyzed.
3. **Deliverables**
    - Submit a report that includes:
        - Screenshots of key steps (setting up OpenVAS, configuring the scan, viewing results).
        - Summary of findings
        - A detailed analysis of one high-severity vulnerability.
        - Recommendations for improving the security of the target system.

Rubric

- **Setup and Configuration** (10 points): Properly installed and set up Greenbone.
- **Scanning Process** (20 points): Successfully configured and executed a vulnerability scan.
- **Analysis of Results** (30 points): Correctly identified and explained vulnerabilities, especially a high-severity issue.
- **Reporting and Recommendations** (30 points): Report is well-organized, includes screenshots, and provides clear remediation steps.

Assignment Submission

Attach the completed report document to the assignment in Blackboard.