

Security System and Products

Lecturer:

Dr Hamidreza Bagheri

York St John University
2024 - 2025



GVM/OpenVAS

GVM/OpenVAS

GVM (Greenbone Vulnerability Manager), earlier known as OpenVAS (Open Vulnerability Assessment System), is an open-source [vulnerability scanner](#) used to [identify vulnerabilities in remote systems, servers, and applications](#).

OpenVAS is a [penetration testing framework](#) whose collection of tools allows you to scan and test systems for known vulnerabilities. It is an [endpoint scanning application](#) and [web application](#) used to [identify and detect vulnerabilities](#). It is widely used by companies as part of their [risk mitigation](#) solutions to quickly identify gaps in their production and even development servers or applications. This is not a complete solution, but it can help you fix common security vulnerabilities that may not be discovered. OpenVAS consists of:

- A database comprised of results and configurations
- Executable scanner applications that run Vulnerability Tests (VT) against target systems
- Greenbone Vulnerability Manager Daemon (GVMD)
- Greenbone Security Assistant (GSA) with Greenbone Security Assistant Daemon (GSAD)
- A collection of network vulnerability tests

Installing OpenVAS

Before installing OpenVAS, the first thing we need to do is ensure your system is up to date.

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo apt-get dist-upgrade
```

Or

```
$ sudo apt update && sudo apt upgrade && sudo apt dist-upgrade
```

Once you have your system up to date, we can install OpenVAS.

Note that the Kali team always changes the situation regarding OpenVAS in different distribution. In other words, [you sometimes probably see OpenVAS pre-installed](#), and in some other distribution, it's not.

To install it, do the following:

```
$ sudo apt-get install openvas
```

Check the redis service that comes installed with OpenVAS:

To check the status:

```
$ sudo systemctl status redis-server@openvas.service
```

```
(kali@kali)-[~]
$ sudo systemctl status redis-server@openvas.service
o redis-server@openvas.service - Advanced key-value store (openvas)
   Loaded: loaded (/lib/systemd/system/redis-server@.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: http://redis.io/documentation,
           man:redis-server(1)
```

Start the service if it's not running:

```
$ sudo systemctl start redis-server@openvas.service
```

Enable the service to run at startup:

```
$ sudo systemctl enable redis-server@openvas.service
```

```
(kali@kali)-[~/Desktop]
$ sudo systemctl enable redis-server@openvas.service
Created symlink /etc/systemd/system/multi-user.target.wants/redis-server@openvas.service → /lib/systemd/system/redis-server@.service.
```

Having installed OpenVAS successfully, you will have access to the setup script. Launch it to configure OpenVAS for first-time use:

```
$ sudo gvm-setup
```

This is going to take a long time.

Remember to **note down the password** generated during the setup process as you will require it later.

```
[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '6a1444a4-6755-4d55-aa93-39d8b80d85bb'.

[>] You can now run gvm-check-setup to make sure everything is correctly
configured
```

Starting and Stopping OpenVAS

If you have OpenVAS configured properly, you can run it by executing the command:

```
$ sudo gvm-start
```

This command should launch the OpenVAS service and open the browser. You can manually navigate to the web interface using the default listening ports. This command should launch the services listening on port 9390 and 9392

```
(kali@kali)~$ sudo gvm-start
[*] Please wait for the GVM / OpenVAS services to start.
[*] You might need to refresh your browser once it opens.
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-02-12 12:24:11 UTC; 43ms ago
     Docs: man:gsad(8)
           https://www.greenbone.net
   Process: 33117 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
  Main PID: 33118 (gsad)
    Tasks: 1 (limit: 4546)
   Memory: 1.7M
   CGroup: /system.slice/greenbone-security-assistant.service
           └─33118 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

Feb 12 12:24:11 kali systemd[1]: Starting Greenbone Security Assistant (gsad)...
Feb 12 12:24:11 kali gsad[33117]: Oops, secure memory pool already initialized
Feb 12 12:24:11 kali systemd[1]: Started Greenbone Security Assistant (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-02-12 12:24:06 UTC; 5s ago
     Docs: man:gvmd(8)
   Process: 33071 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
  Main PID: 33073 (gvmd)
    Tasks: 2 (limit: 4546)
   Memory: 3.1M
   CGroup: /system.slice/gvmd.service
```

Troubleshooting Errors

Installing OpenVAS on older versions of Kali Linux may result in some errors. Here are some possible ways of fixing possible errors:

Install PostgreSQL or SQLite3 database

```
$ sudo apt-get install postgresql
$ sudo service postgresql start
$ sudo apt-get install sqlite3
$ sudo service sqlite3 start
```

Next, use gvm commands:

```
$ sudo apt install gvm -y
$ sudo gvm-setup
$ sudo gvm-feed-update
$ sudo gvm-start
```

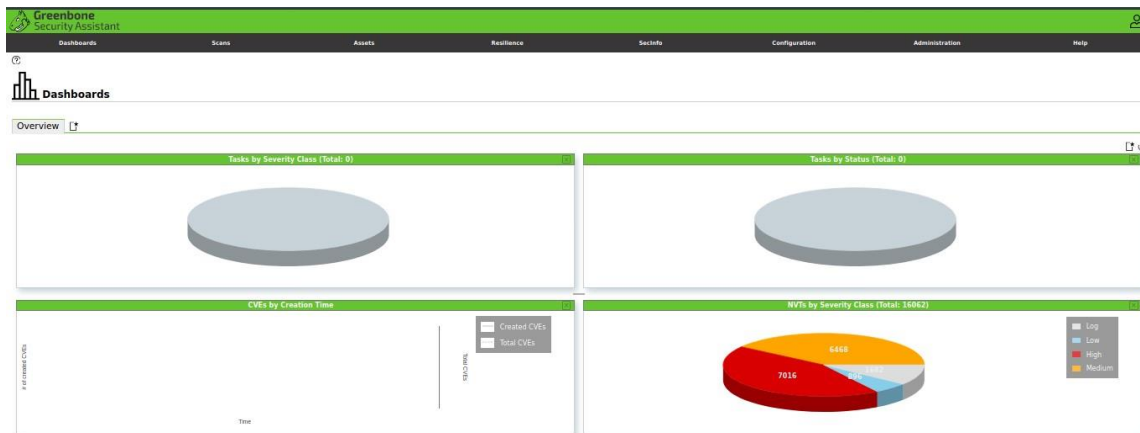
NOTE: Depending on the version you have installed, you may need to use the gvm command other than OpenVAS.

Accessing OpenVAS Web UI

Using the GSA features, you can access the OpenVAS web UI from your local machine. You will need to have OpenVAS running to access the interface.

Open your browser and navigate to `http://localhost:9392`

Use the `username: admin` & `password` generated in the setup process.



Note: If you forgot your password, use the following command to set a new one.

```
$ sudo gvmd - user=admin - new-password=YourPasswd
```

Once you log in, you should have access to OpenVAS web UI (Greenbone), which you can configure to suit your needs.

Add Target

The first step to using the Security Assistant is to add targets. Navigate to the “Configuration” menu and select “Targets”.

On the top left corner, select a blue icon to start adding targets. Doing that will launch a dialogue window that allows you to add information about the target, such as:

- Target Name
- The IP address

Once you add all the relevant information about the target, you should see it listed in the targets section.

New Target

Name

Host Name

Comment

Hosts

☒ Manual

192.168.0.16

☐ From file

Browse...

No file selected.

Exclude Hosts

☒ Manual

☐ From file

Browse...

No file selected.

Port List

OpenVAS Default

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

--

on port

22

SMB

--

ESXi

--

SNMP

--

Cancel

Save

Creating a Scan Task

Let us now proceed to create a scan task. A task in OpenVAS (Greenbone) defines the target(s) you want to be scanned and the required scanning parameters. For the sake of simplicity, we will use the default scan options.

Navigate to “Scans” sections and select Tasks in the dropdown menu. Click on the icon on the left-hand side to create a new task.

That will launch a window allowing you to provide all relevant information for a scanning task.

- Task name
- Scan target
- Schedule

Use the default settings and click on Create.

New Task

Name

New Task

Comment

Scan Targets

Host Name

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70

%

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Cancel

Save

To run a task, click on the Play icon on the bottom left of the task list.

Adding Users

OpenVAS allows you to add various users and assign various roles to them. To add a user or role, navigate to the administration section and click on users. Select the new icon and add the user information:

New User

Login Name

Low

Comment

Authentication

☒ Password

Roles

☒ Guest

Groups

Host Access

☒ Allow all and deny ☐ Deny all and allow

Interface Access

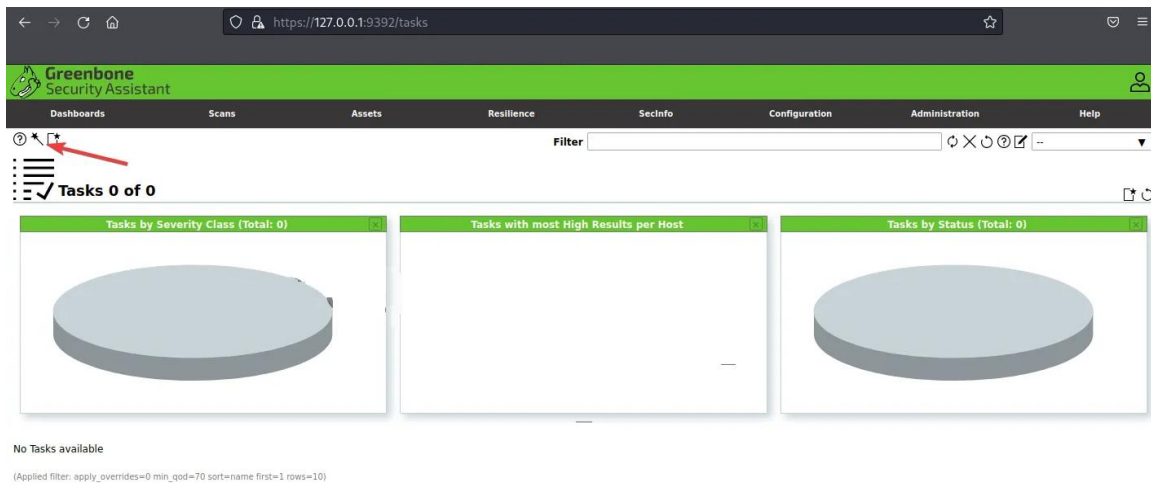
☒ Allow all and deny ☐ Deny all and allow

Cancel

Save

Running your first Scan

Now it's time to run our first scan. Here is an example of how to run your first scan.



Now you can enter either a single IP, a whole subnet, a range of IP Addresses, or a domain. This will start a default-depth scan. Depending on the scale of the Network you want to scan this can take from a few minutes up to several hours or even days if the network is large enough and you choose a deep scan.

References

- V. Nestler, Wm. Conklin, G. White, M. Hirsch, Principles of Computer Security: CompTIA Security+™ and Beyond Lab Manual, 2nd Edition, McGraw-Hill
- Gus Khawaja, Kali Linux Penetration Testing Bible, Wiley.
- <https://linuxhint.com/install-openvas-kali-linux/>