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
```

Start the service if it's not running:

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

Enable the service to run at startup:

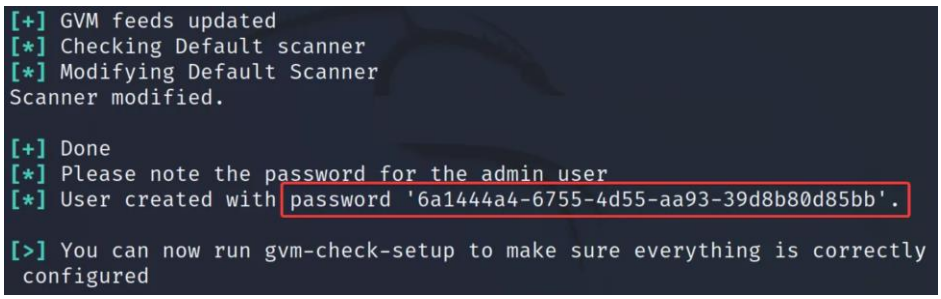
```
$ sudo systemctl enable redis-server@openvas.service
```

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.

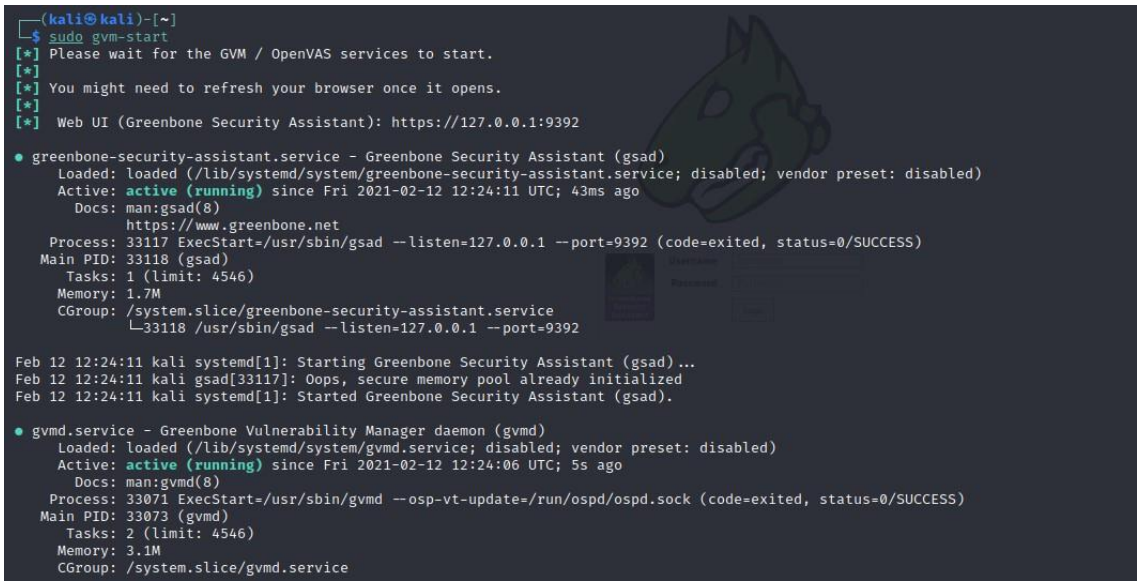


Starting and Stopping OpenVAS

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



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
```

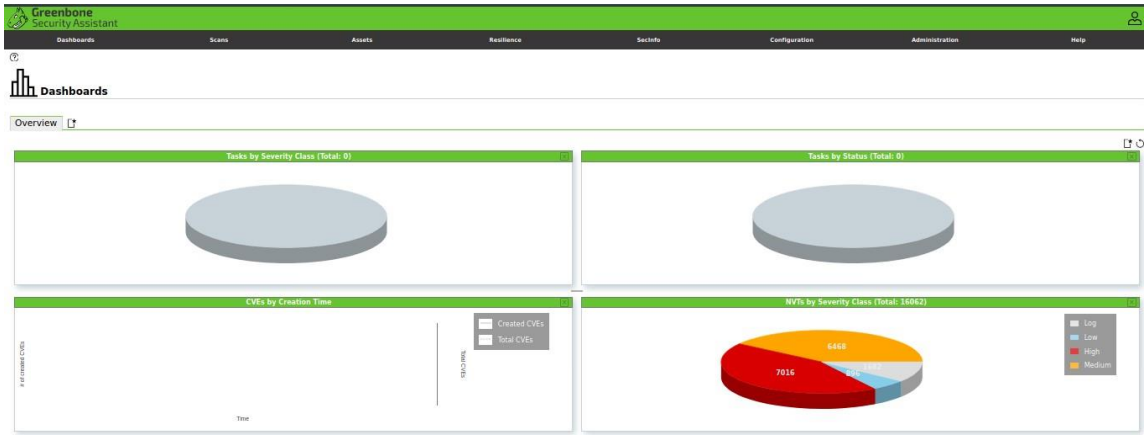
NOTE: Depending on the version you have installed, you may need to use the gvm command other than OpenVAS.

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.

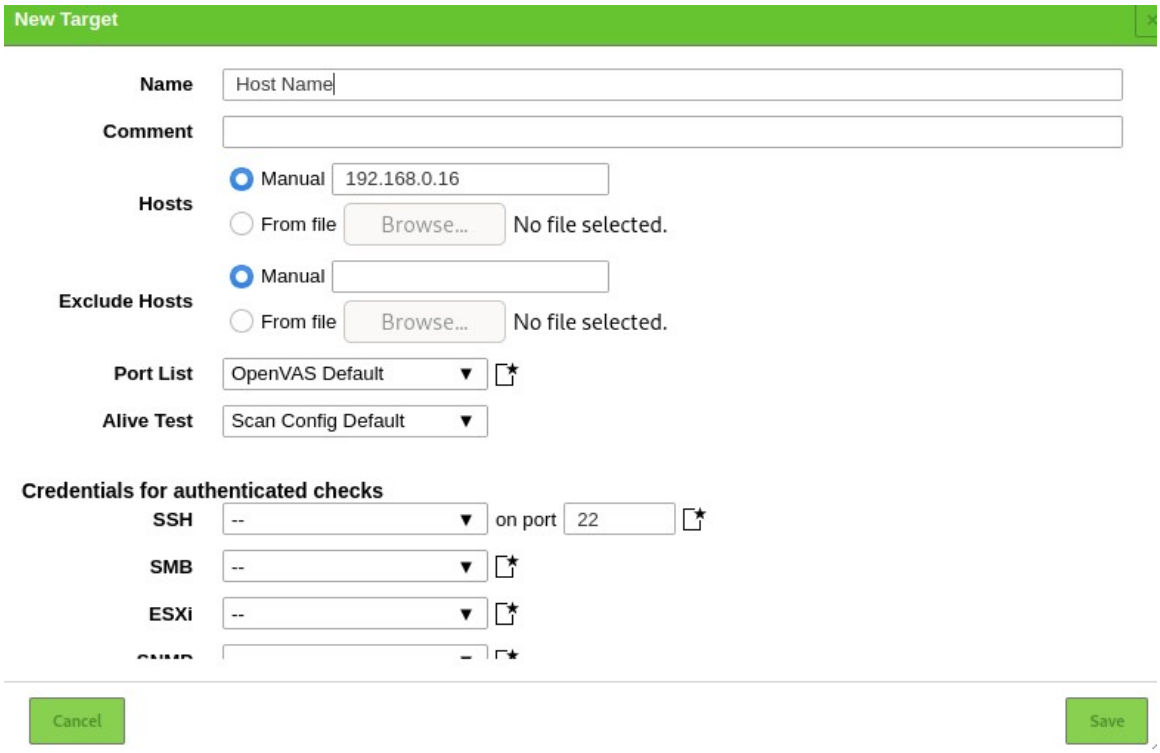
Add Target

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.



Creating a Scan Task

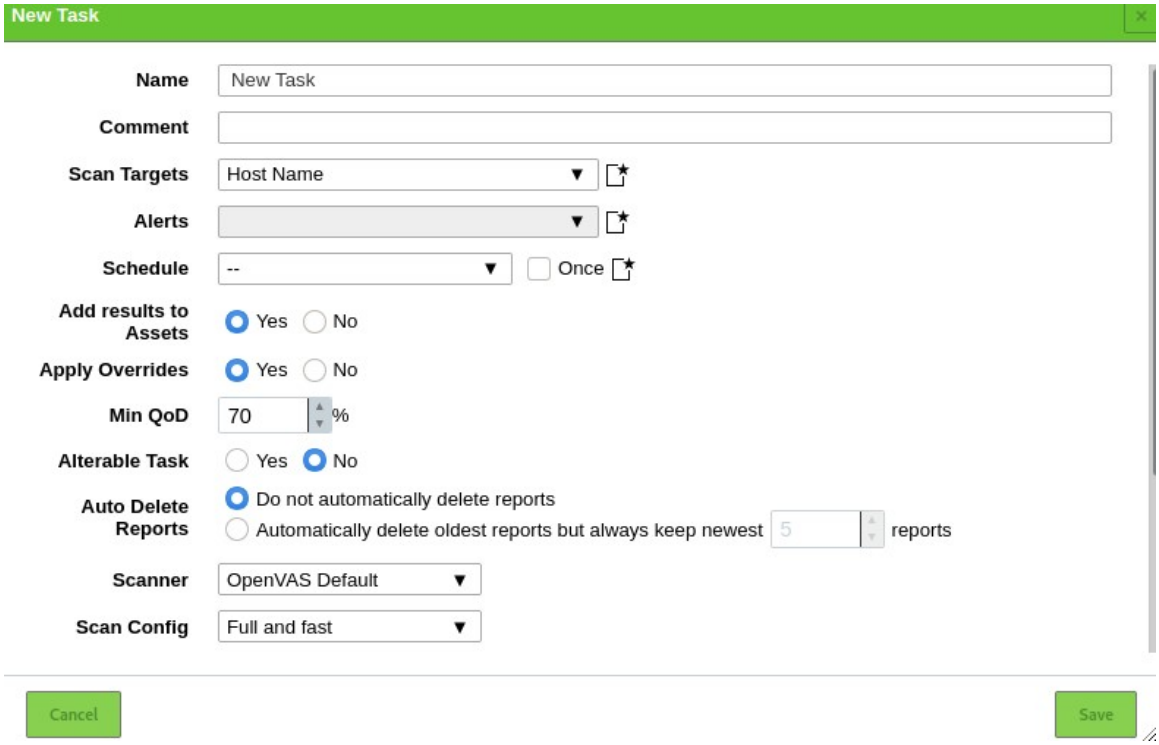
Let us now proceed to create a scan task. A task in OpenVAS (Greenbone) defines the target(s) you want to be scanned and the required scanning parameters. For the sake of simplicity, we will use the default scan options.

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

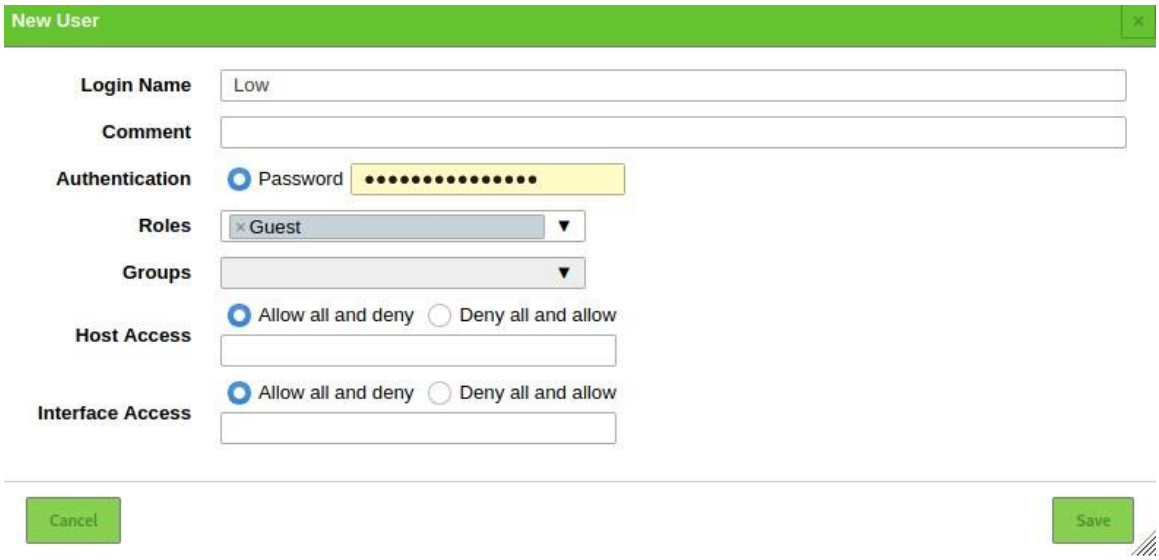
Use the default settings and click on Create.



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

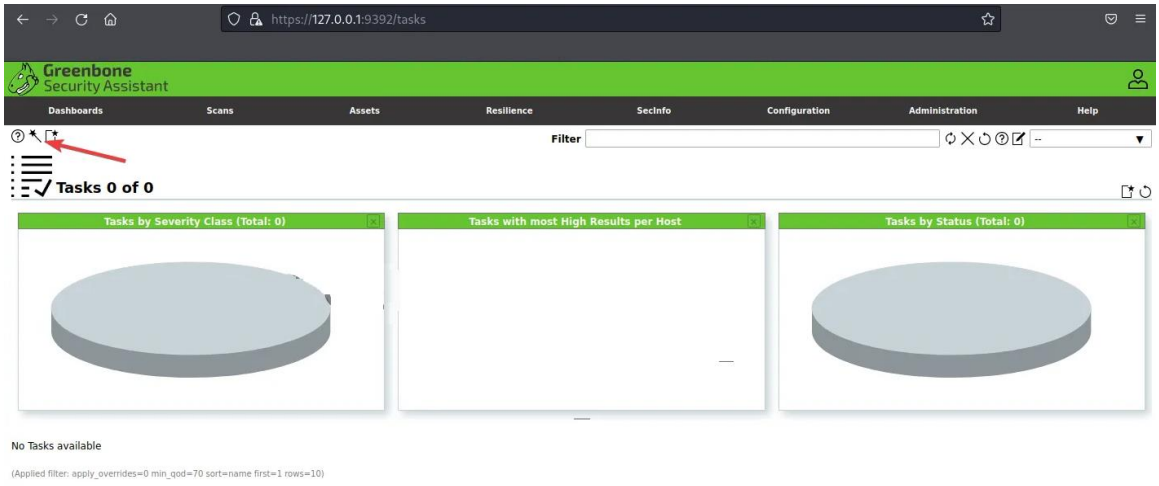
Adding Users

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:



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/`