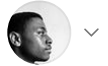


Open in app ↗



# How to Install OpenVAS



Daniel Iwugo

Published in InfoSec Write-ups

5 min read · 5 days ago



Listen



Share

... More



# OpenVAS

Open Vulnerability Assessment Scanner

OpenVAS | Credit: [www.openvas.com](https://www.openvas.com)

If you're starting off in cybersecurity you may have heard of vulnerability scanners. A vulnerability scanner is a software or program that identifies security vulnerabilities or weaknesses in a system, application or network. It's used by both attackers and defenders to figure out the security posture of the target system.

In this article, you'll learn how to install a vulnerability scanner called OpenVAS, an offshoot of Nessus. OpenVAS is an open-source framework and vulnerability scanner extensively used for identifying and evaluating security vulnerabilities in computer systems and networks.

So without further adieu, let's jump in 🤖.

## Requirements

1. A Computer with at least 4GB RAM and 20GB Storage
2. A stable internet connection
3. A Linux OS (Debian or Ubuntu LTS)

#### 4. A lot of patience ⌚

### Important Concept: Containers

There are two ways to install OpenVAS:

1. From the source
2. Using Docker Containers

Installing from the source can be quite tasking and could even end up still not working in the end (Trust me, I've been there 🤔). However, using a docker container makes the process simple and almost seamless.

A docker container is a lightweight, standalone, executable software package that includes everything needed to run an application, including the code, runtime environment, system tools, and libraries. This allows the application in the container to be deployable almost anywhere.

We don't really need to get into the specifics of things but basically think of it like a Lego set and its box. The Lego set is your application and the box is the container. The box contains the instructions and pieces you need to build the structure.

Likewise, the container has everything you need for deploying your application anywhere. And because it's so versatile, you can create multiple containers to deploy multiple applications without putting much strain on your hardware.

Now that you have an idea of how containers work, let's look at how to install OpenVAS using them.

### Installation Steps

We'll start off by opening up a terminal and installing curl and docker.io.

```
sudo apt install curl docker.io
```

Next, install docker.compose

```
sudo apt install python3 python3-pip
python3 -m pip install --user docker-compose
```

Now we need to add the current user to the `docker` user group so you can use containers. Type in the following.

```
sudo usermod -aG docker $USER && su $USER
```

Logout and log back in for the changes to be applied to your system.

We need to create a directory for the docker compose file. A compose file contains instructions to setup the container, just like instructions for the Lego set. Let's create a directory to put it in.

```
export DOWNLOAD_DIR=$HOME/greenbone-community-container && mkdir -p $DOWNLOAD_DIR
```

**Note:** The download directory in this tutorial is `/home/<user>/greenbone-community-container`. If you restart your computer at any point during the setup, the `DOWNLOAD_DIR` variable will lose its value. In such cases, replace `DOWNLOAD_DIR` with `./greenbone-community-container` in the commands.

Let's download the actual compose file.

```
cd $DOWNLOAD_DIR && curl -f -L <https://greenbone.github.io/docs/latest/_static/docker-compose-22.4.yml -o docker-compose.yml
```

```
(mercury@pluto)-[~]
$ cd $DOWNLOAD_DIR && curl -f -L https://greenbone.github.io/docs/latest/_static/docker-compose-22.4.yml -o docker-compose.yml
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left  Speed
100 4296 100 4296 0 0 771 0 0:00:05 0:00:05 --:--:-- 929
```

## Downloading the Docker Compose file | Credit: Mercury

Once that's done, we can now setup (pull) the actual containers for OpenVAS. Feel free to pull up an episode of Phineas and Ferb while waiting for the downloads 🍌.

```
docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edit
```

```
(mercury@pluto)-[~/greenbone-community-container]
$ docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edition up -d
Creating network "greenbone-community-edition_default" with the default driver
Creating volume "greenbone-community-edition_gpg_data_vol" with default driver
Creating volume "greenbone-community-edition_scap_data_vol" with default driver
Creating volume "greenbone-community-edition_cert_data_vol" with default driver
Creating volume "greenbone-community-edition_data_objects_vol" with default driver
Creating volume "greenbone-community-edition_gvmd_data_vol" with default driver
Creating volume "greenbone-community-edition_psql_data_vol" with default driver
Creating volume "greenbone-community-edition_vt_data_vol" with default driver
Creating volume "greenbone-community-edition_notus_data_vol" with default driver
Creating volume "greenbone-community-edition_psql_socket_vol" with default driver
Creating volume "greenbone-community-edition_gvmd_socket_vol" with default driver
Creating volume "greenbone-community-edition_ospd_openvas_socket_vol" with default driver
Creating volume "greenbone-community-edition_redis_socket_vol" with default driver
Pulling vulnerability-tests (greenbone/vulnerability-tests):...
latest: Pulling from greenbone/vulnerability-tests
71d064a1ac7d: Pull complete
3948fedfef90: Extracting [=====>] 45.12MB/61.12MB
2b29019d021d: Download complete
```

Pulling the OpenVAS containers | Credit: Mercury

And now, we can start the containers. It should take a few minutes.

```
docker-compose -f $DOWNLOAD_DIR/docker-compose.yml -p greenbone-community-edit
```

```
Status: Downloaded newer image for greenbone/gvm-tools:latest
Creating greenbone-community-edition_pg-gvm_1 ... done
Creating greenbone-community-edition_cert-bund-data_1 ... done
Creating greenbone-community-edition_scap-data_1 ... done
Creating greenbone-community-edition_gpg-data_1 ... done
Creating greenbone-community-edition_mqtt-broker_1 ... done
Creating greenbone-community-edition_redis-server_1 ... done
Creating greenbone-community-edition_vulnerability-tests_1 ... done
Creating greenbone-community-edition_notus-data_1 ... done
Creating greenbone-community-edition_data-objects_1 ... done
Creating greenbone-community-edition_report-formats_1 ... done
Creating greenbone-community-edition_dfn-cert-data_1 ... done
Creating greenbone-community-edition_notus-scanner_1 ... done
Creating greenbone-community-edition_gvmd_1 ... done
Creating greenbone-community-edition_gsa_1 ... done
Creating greenbone-community-edition_ospd-openvas_1 ... done
Creating greenbone-community-edition_gvm-tools_1 ... done
```

Starting the Containers | Credit: Mercury

To open up the web interface for OpenVAS, run the command below.

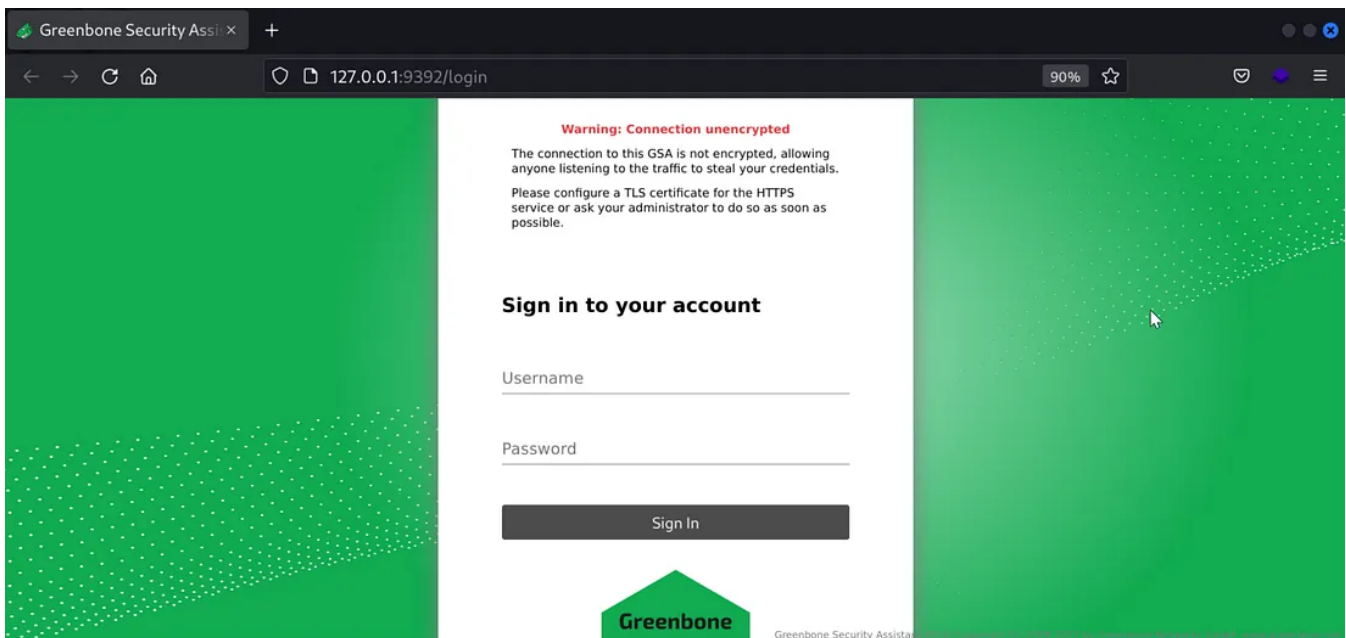
```
xdg-open "<http://127.0.0.1:9392>" 2>/dev/null >/dev/null &
```

Alternatively, you could open up Firefox and type in the following.

```
<http://127.0.0.1:9392>
```

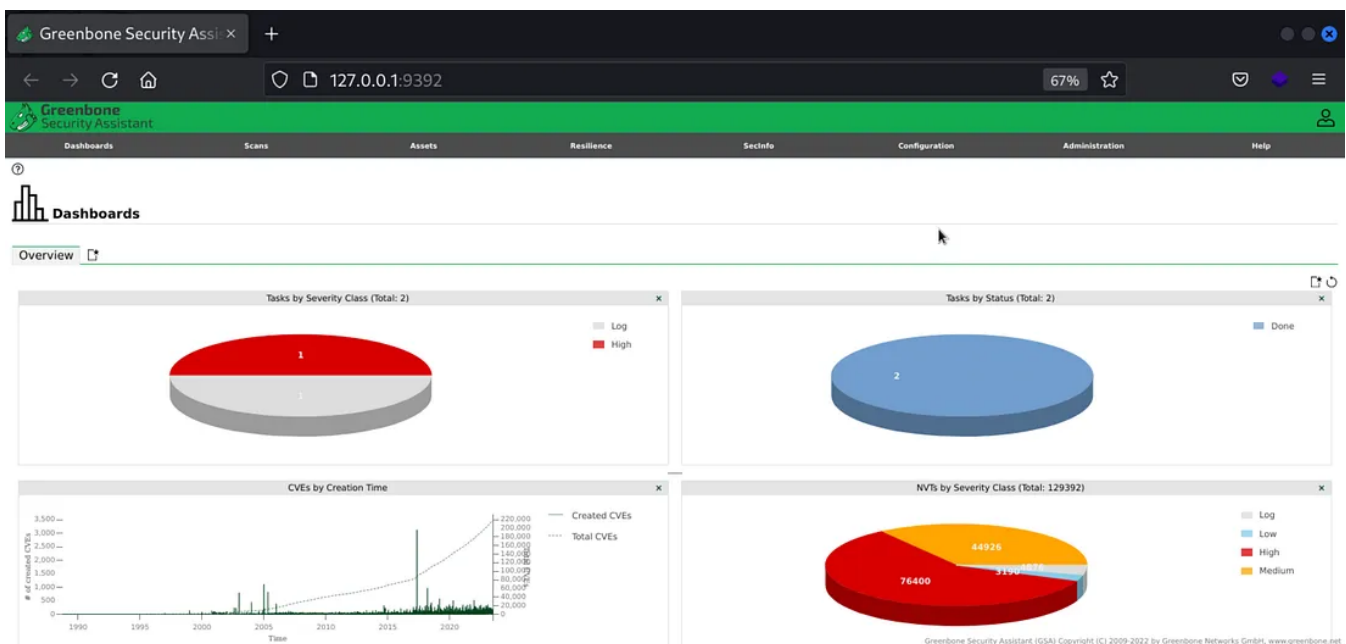
An interface just like the one below should pop up.





The OpenVAS login page | Credit: Mercury

The default username and password are `admin` and `admin` respectively. This is insecure so you might want to change them later.

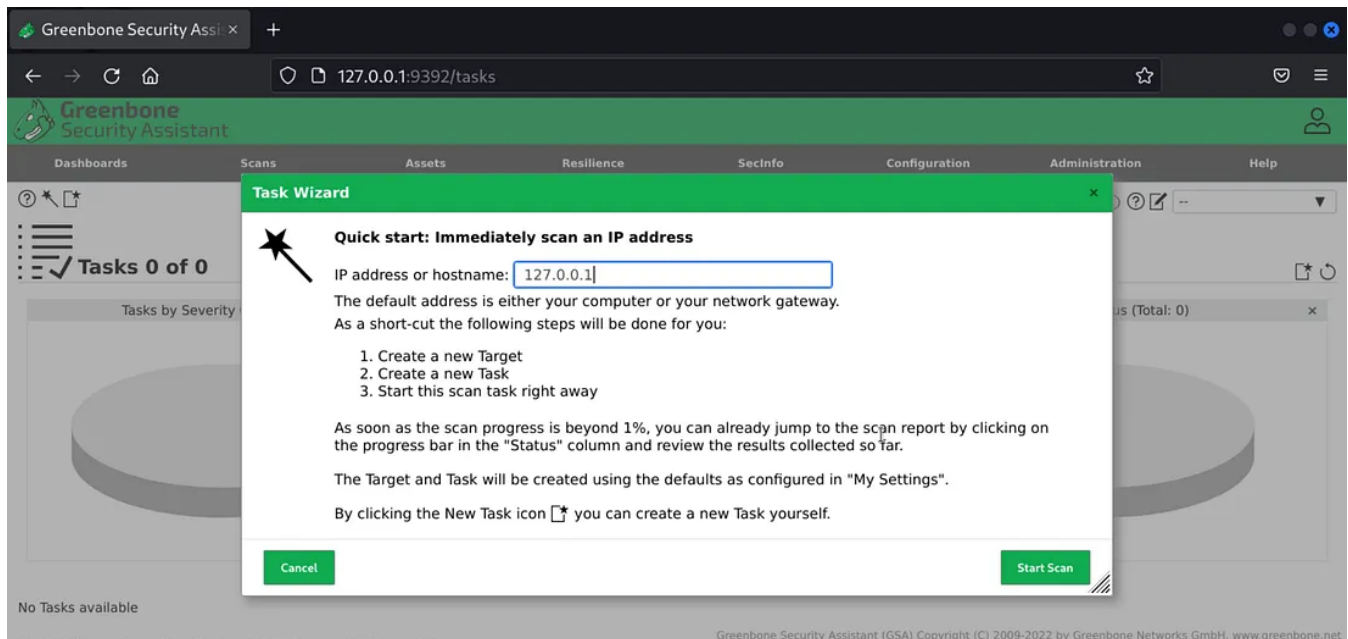


The OpenVAS Dashboard | Credit: Mercury

I've already run a few scans so my dashboard looks a bit different. Nevertheless, you should see something similar to the image above.

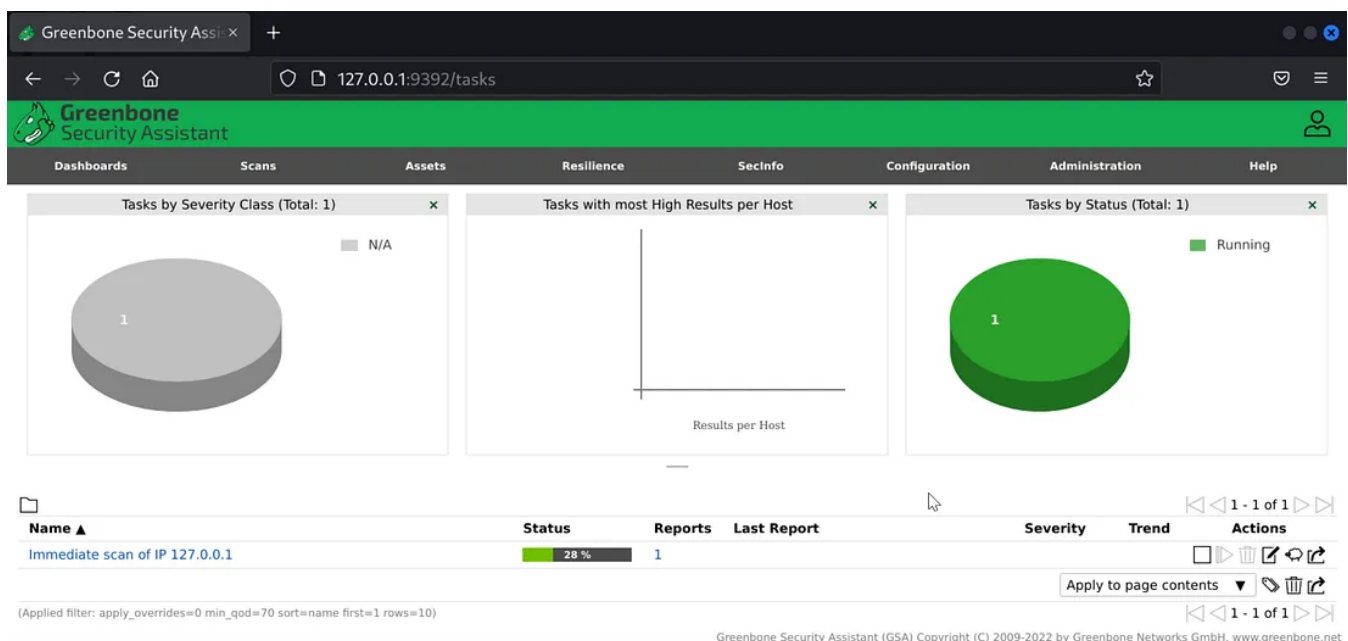
It's important to note that the scanner won't work immediately until all components are loaded. You can check this in the Feed Status under the Administration Tab. Depending on your hardware resources, it might take about 30 mins to a few hours (You might want to pull up another episode 🧐 🍉).

Once the feeds are updated, the column should show current on all tabs. Now to verify everything is working, we need to run a scan on our local host. Go to the Dashboard and click on the Wand icon at the top left to run a quick scan.



The Task Wizard | Credit: Mercury

Put the address 127.0.0.1 and hit 'Start Scan'.



Running a task scan | Credit: Mercury

If your Status bar goes past the 1% mark, give yourself a pat on the back. You have successfully installed OpenVAS 🍷 🍷 .

To stop the containers, run the following command.

```
docker-compose -f ./greenbone-community-container/docker-compose.yml -p greenbo
```

For more information, check out [Greenbone's documentation](#) or watch [this video](#).

## Conclusion

OpenVAS can be quite frustrating and time taking to install. However, once you know how to do it, you can carry out vulnerability scanning on various systems (and without paying a dime 🏛️). As always, use hacking tools for appropriate purposes and don't scan infrastructure you aren't legally allowed to.

Happy Hacking 🧐.

Cybersecurity

Vulnerability Assessment

Openvas

Open Source

Mercurysnotes



Edit profile

## Written by Daniel Iwugo

112 Followers · Writer for InfoSec Write-ups

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet. All my articles can be found here: [flipboard.com/@elementmerc](https://flipboard.com/@elementmerc)

---

More from Daniel Iwugo and InfoSec Write-ups