# Installing OpenVAS on Kali Linux


OpenVAS Installation

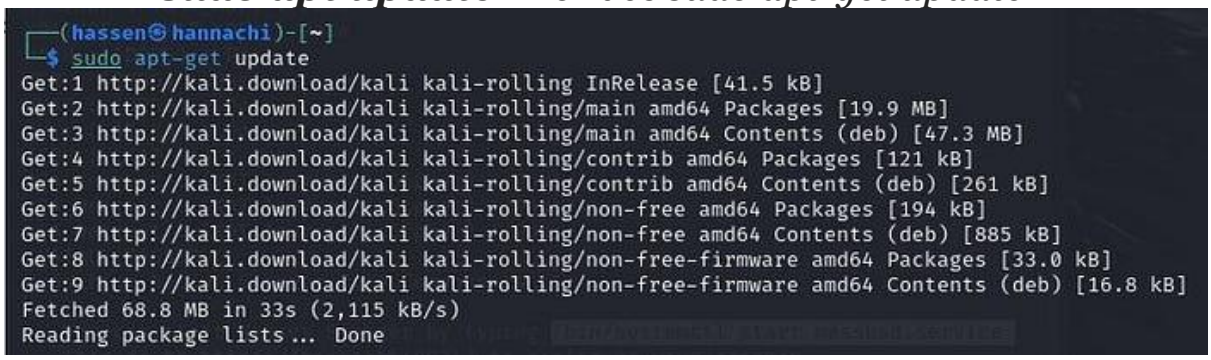

**OpenVAS**, an endpoint scanning application and web application used to identify and detect vulnerabilities. It is widely used by companies as part of their risk mitigation solutions to quickly identify gaps in their production and even development servers or applications. This is not a complete solution, but it can help you fix common security vulnerabilities that may not be discovered.

The condition of Greenbone mode is open (APEVALV) from infected chemistry (GVM) of the quality of the storage and the GitHub area. it is used in the Greenbone Security Manager device and is a comprehensive scan. An engine that runs an advanced and constantly updated Network Vulnerability Test Package (NVT).

## Prepare Kali Linux for the installation of OpenVAS

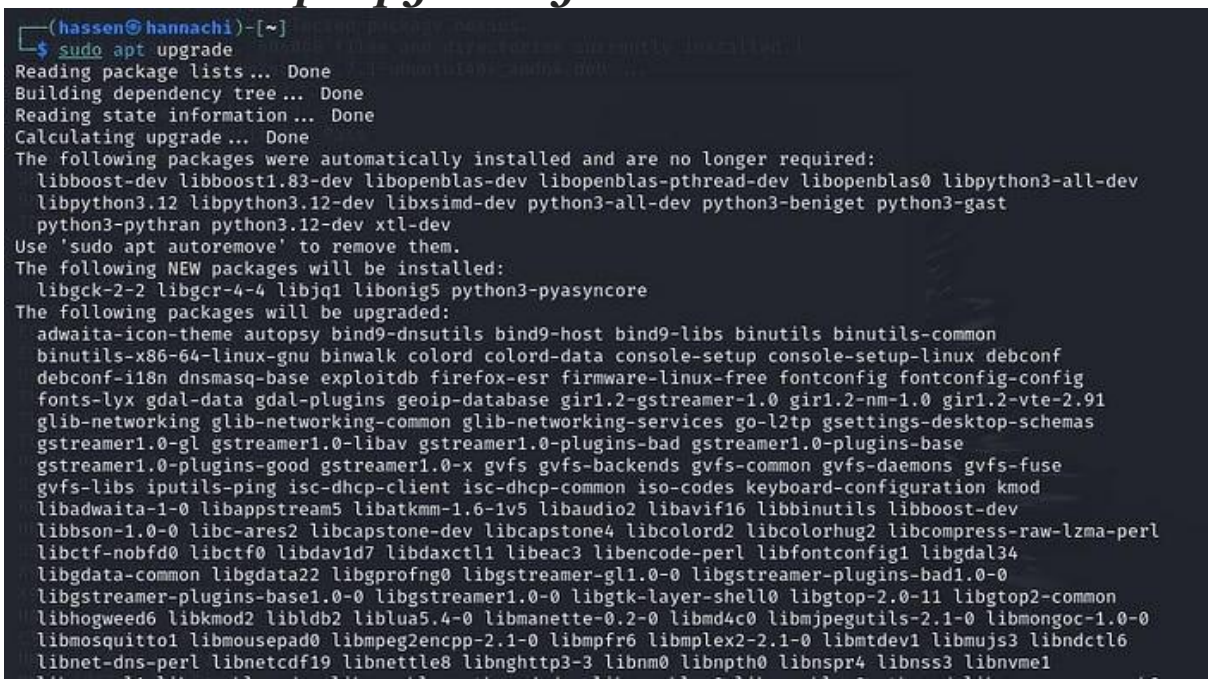
Unless you have already done so, make sure that the ***Kali Linux is up to date*** and ***install the latest Kali Linux***. You automatically download the latest rules, create admin users, and start the various services. Depending on bandwidth and computer resources, this may take a while.

- ***sudo apt update*** — or use *sudo apt-get update*



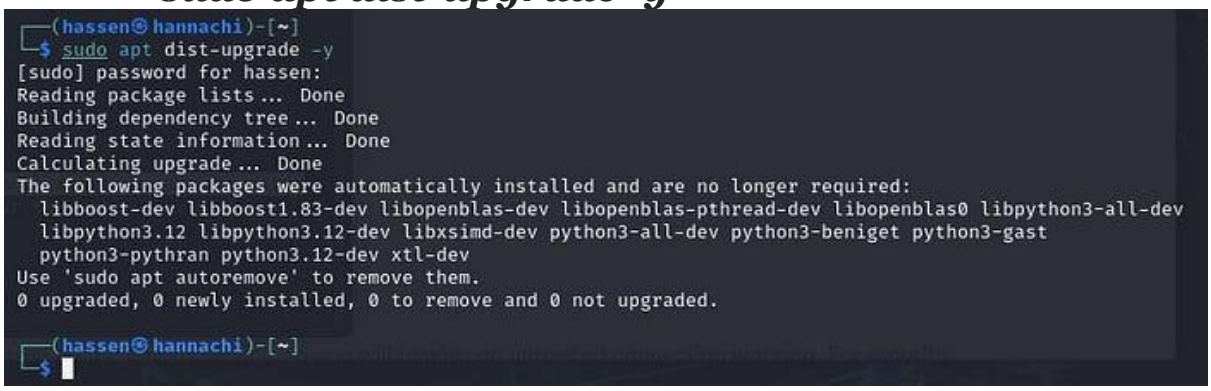

sudo apt-get update

- ***sudo apt upgrade -y***




sudo apt upgrade

- ***sudo apt dist-upgrade -y***




sudo apt dist-upgrade -y

## Installing OpenVAS on Kali Linux

To install Openvas and its dependencies on our Kali Linux system run the following command:

- ***sudo apt install openvas***

***or*** use

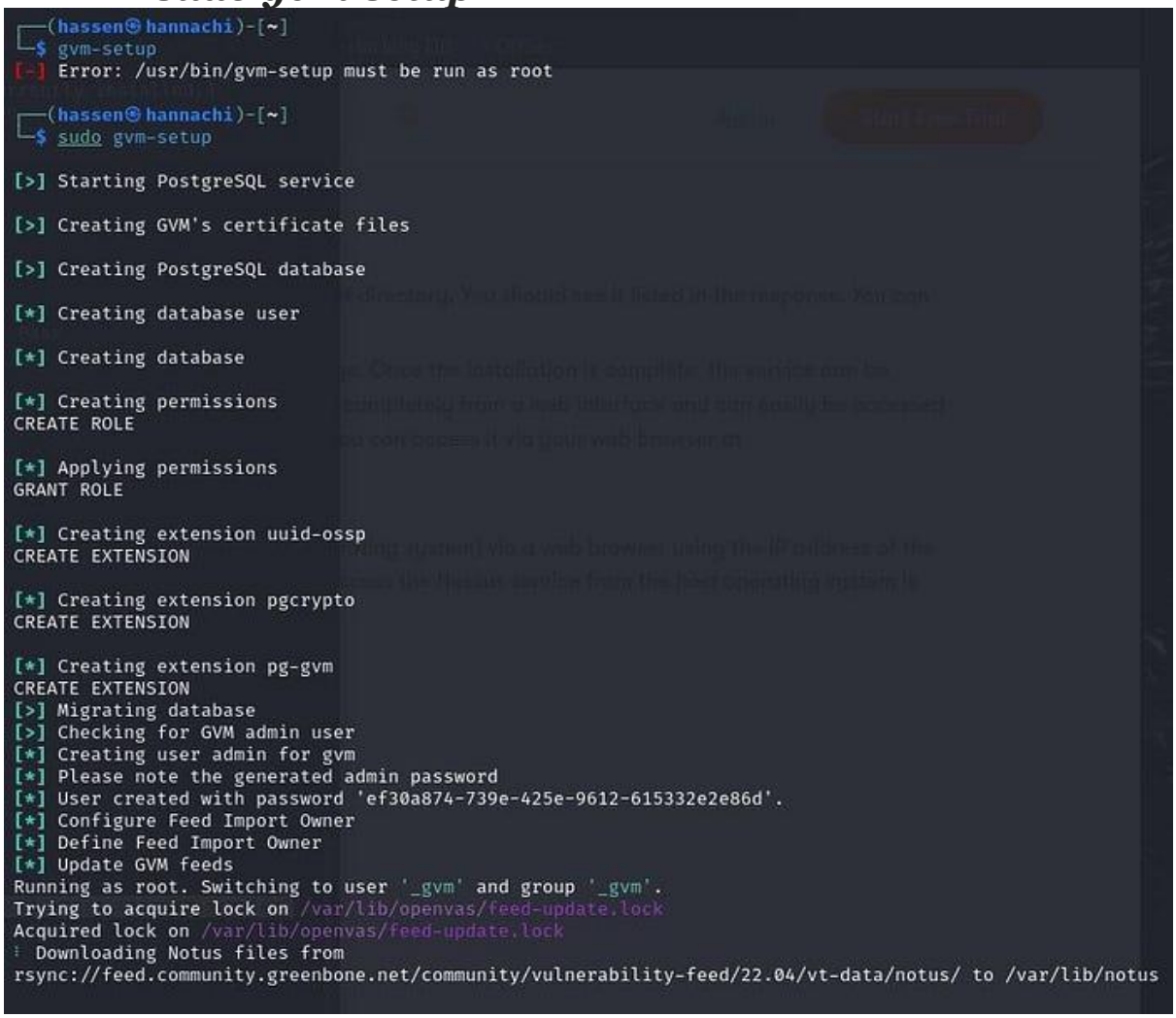
- ***sudo apt install gvm***


sudo apt install openvas

The next step is to run the installer, which will configure OpenVAS and download various *network vulnerability tests* (NVT) or signatures. Due to a large number of NVTs (*50.000+*), the setting process may take some time and consume a lot of data.

Run the following command to start the setup process:

- ***sudo gvm-setup***




sudo gvm-setup

The `gvm-setup` command will take a **long time** to download all the vulnerabilty definitions (*Notus files, NASL files, SCAP data, CRET-Bund data, gvmd data*).

***Hint***: OpenVAS will also set up an ***admin account*** and automatically generate a ***password*** for this account which is displayed in the last section of the setup output.

### Password reset

Did you forget to note down the password? You can change the admin password using the following commands:

- ***sudo gvmd --user=admin --new-password=passwd***

***No***te: *if you don't rest the automatically generated admin credentials [password], make sure to safe a copy as you will need it later for login.*


update admin user password***sudo runuser -u _gvm — gvmd — create-user=admin2 — new-password=12345***

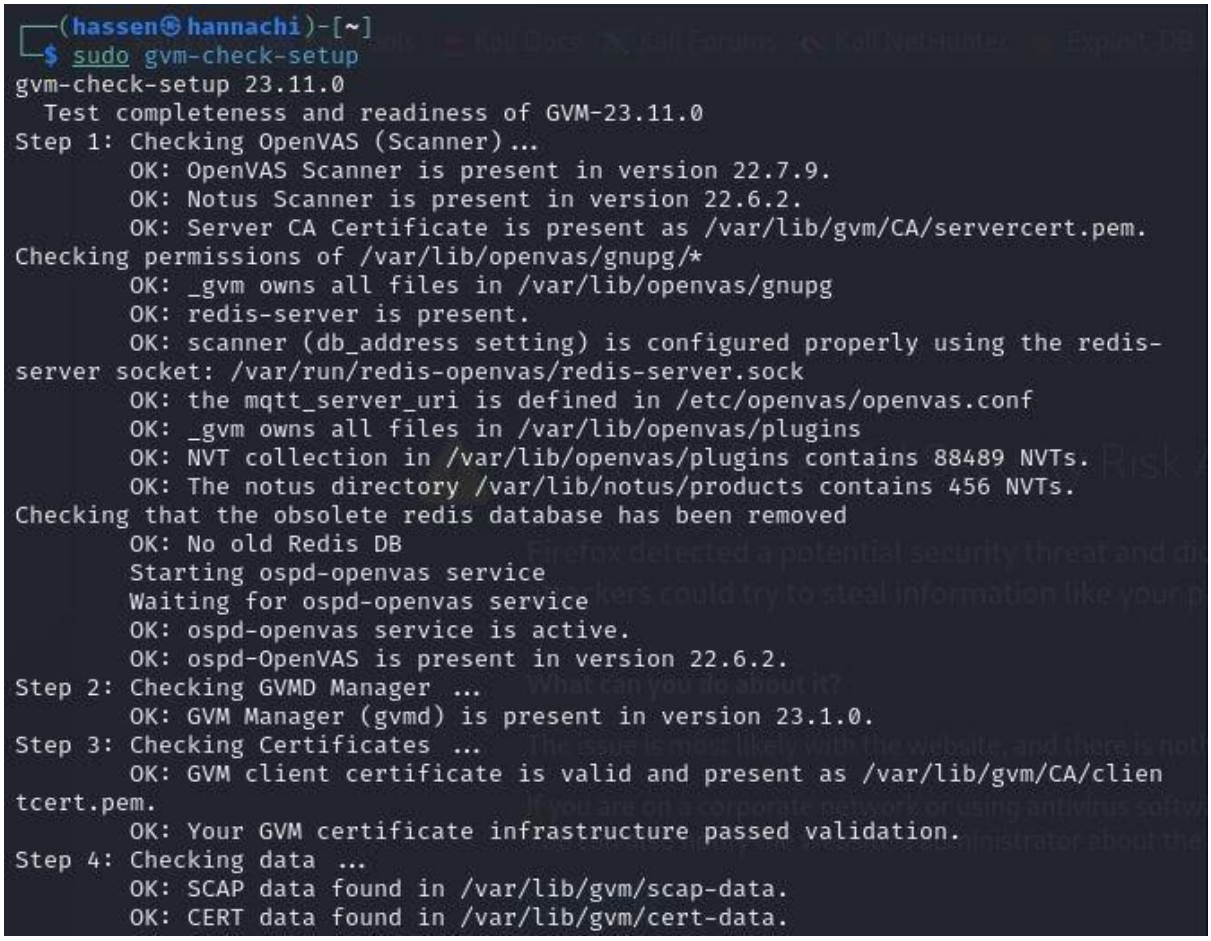
To change the password of the existing user

***sudo runuser -u _gvm — gvmd — user=admin — new-password=new_password***

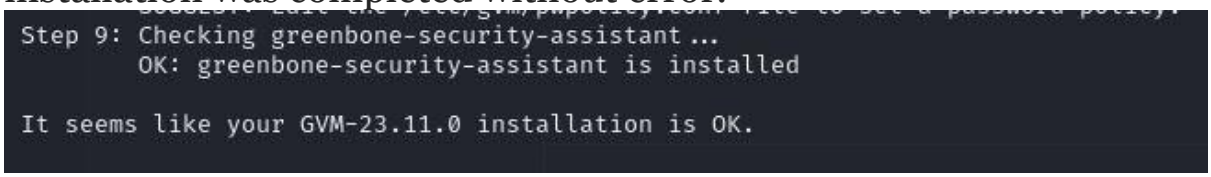
### Verify the Installation

You can verify your installation with.

- ***sudo gvm-check-setup***

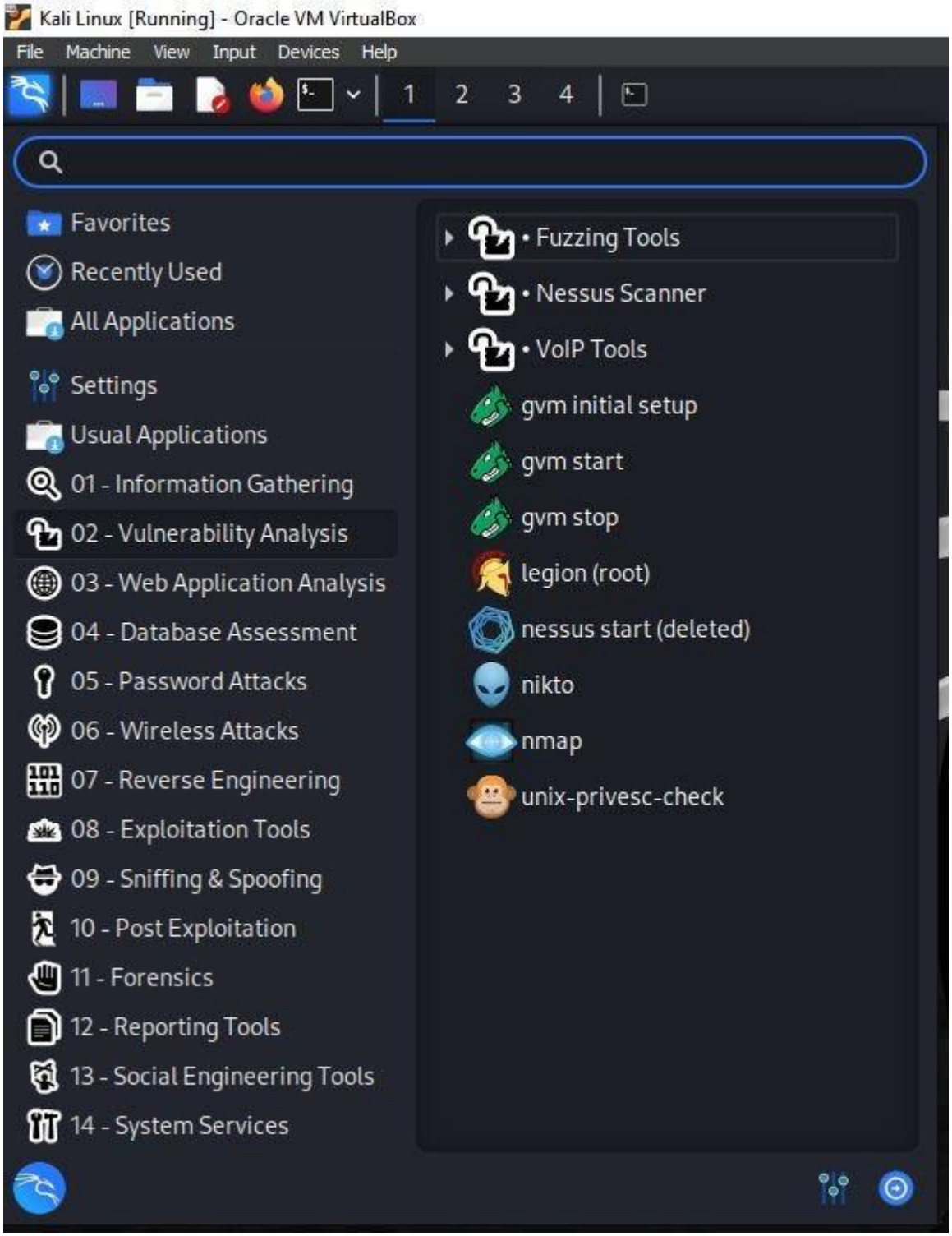



after the process is complete, we should get a confirmation that the installation was completed without error.



### Starting and stopping OpenVAS

Before starting to install the virtual appliance, the last step I have to consider is to start and stop the OpenVAS service. OpenVAS services consume a lot of unnecessary resources, so it is recommended that you disable these services when you are not using OpenVAS.



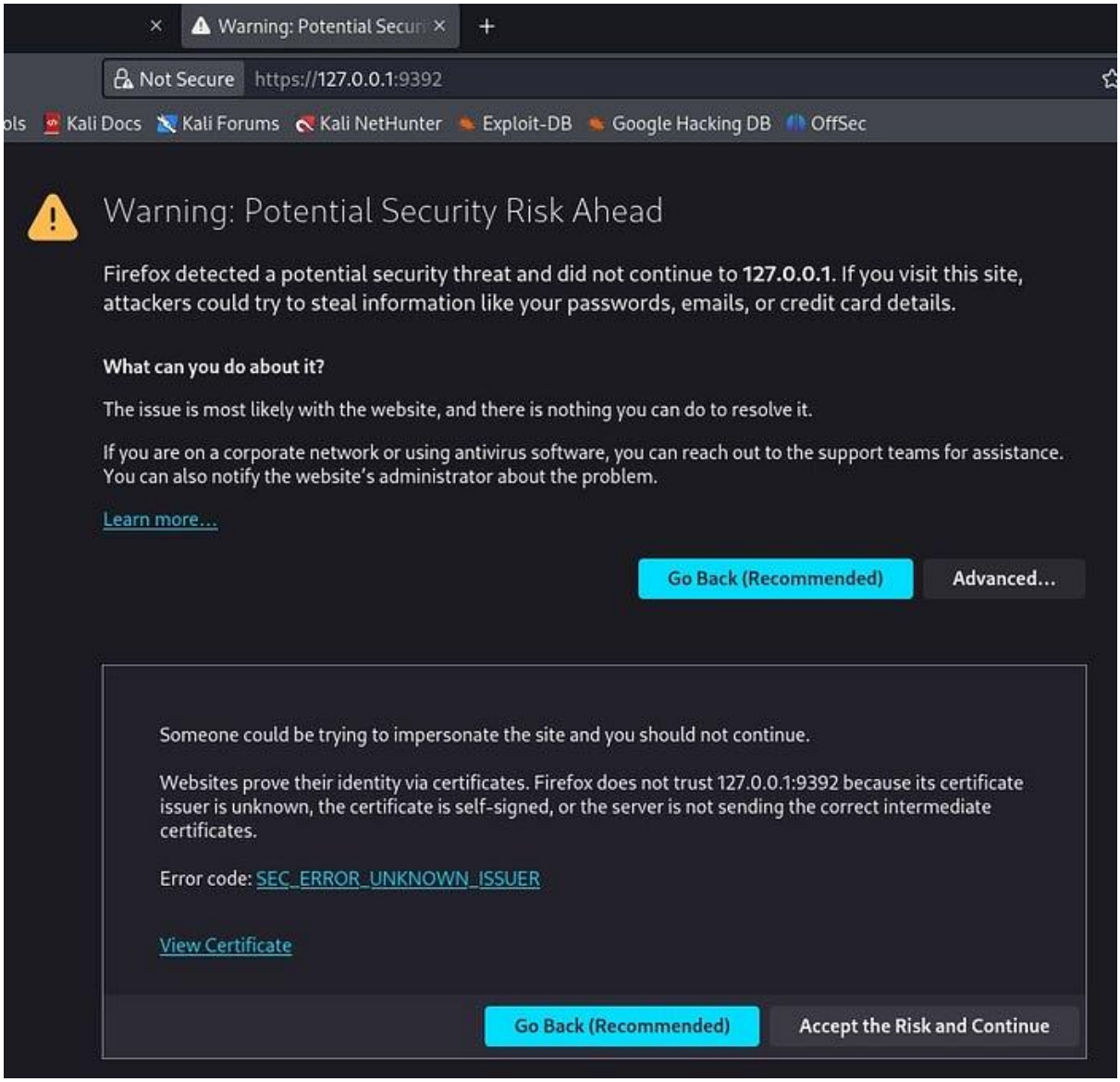
Run the following command to start the services:

- ***sudo gvm-start***

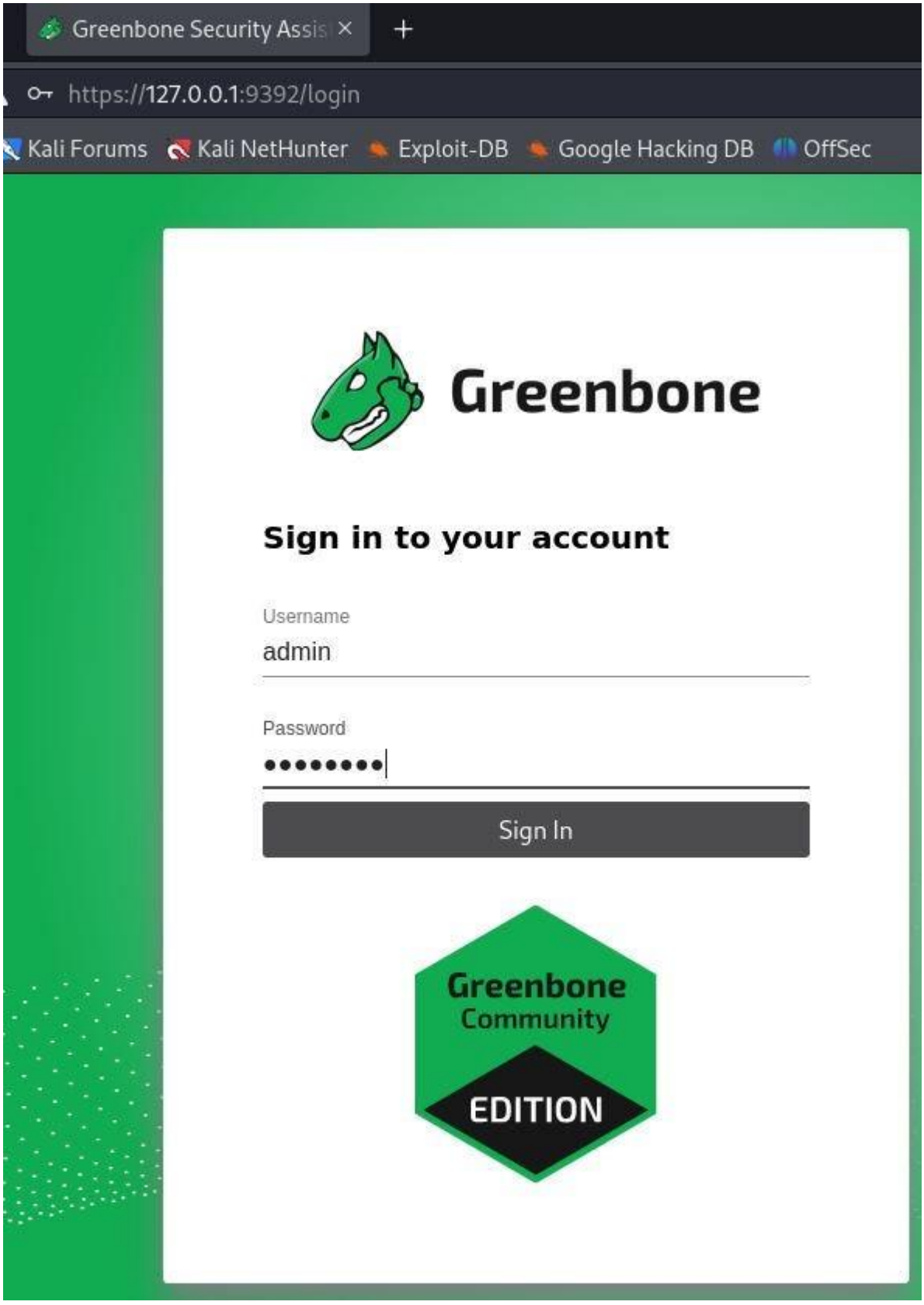

***Hint***: *To stop the OpenVAS services again, run:* ***sudo gvm-stop***

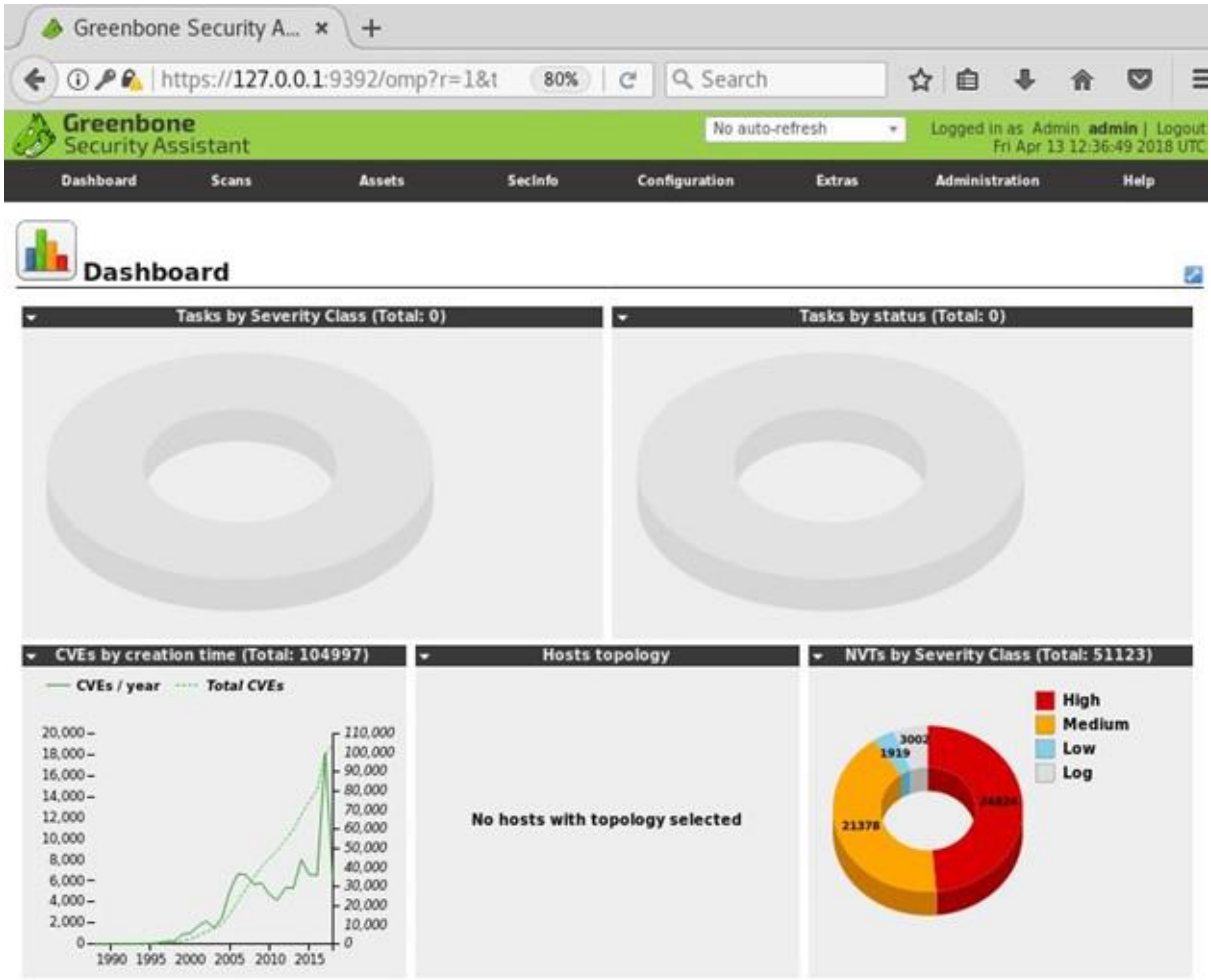
After the configuration process is complete, all the necessary OpenVAS processes will start and the web interface will open automatically (In my case I had to open the browser manually). The web interface is *running locally* on *port 9392* and can be accessed through **https://localhost:9392**

First time you want to open this URL you will get a security warning. Click on **Advanced** and **Accept the Risk and Continue**.




The next step is to accept the self-signed certificate warning and use the automatically generated admin credentials (in my case I rest the admin password) to login on to the web interface:

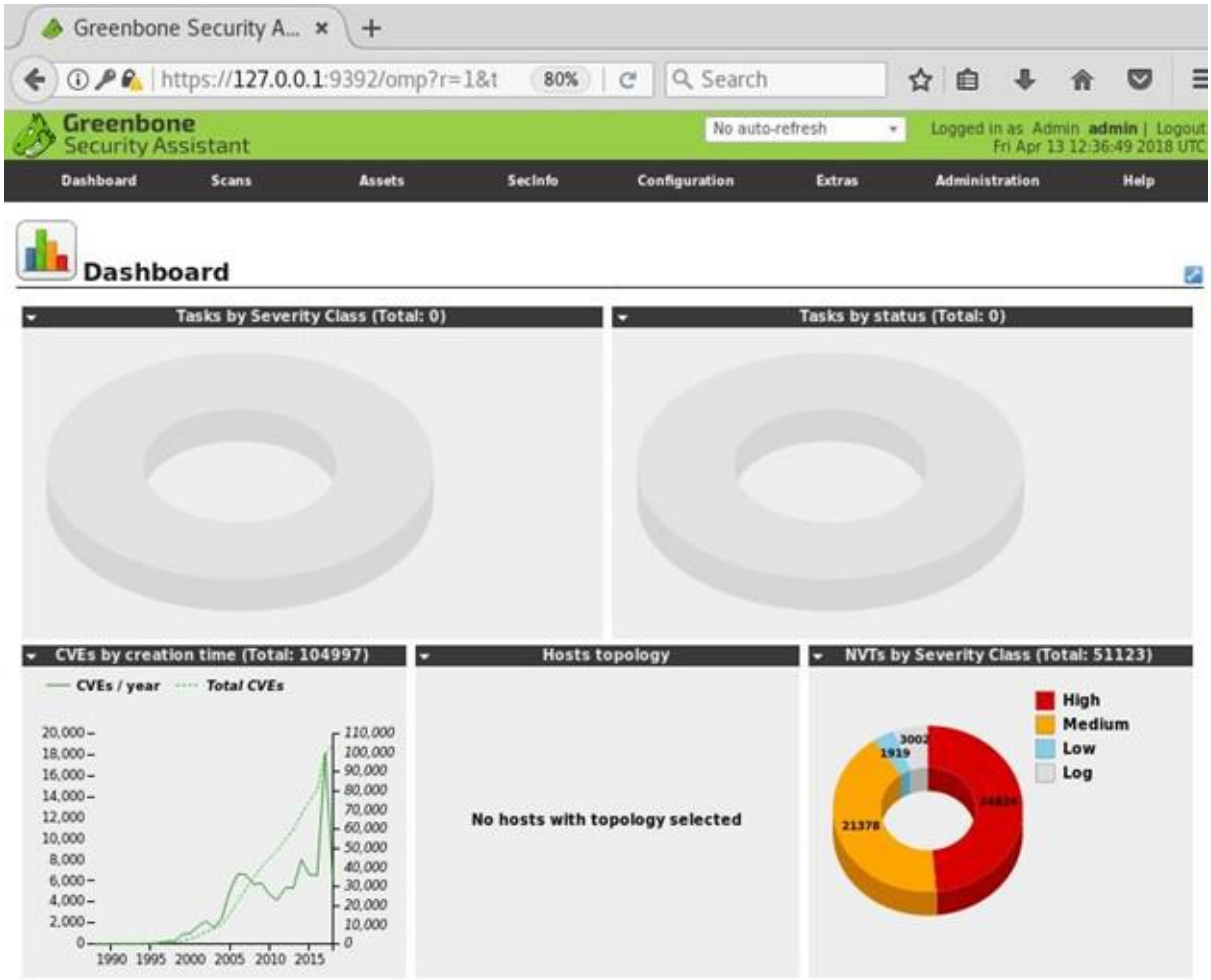

Greenbone Security Assis
https://127.0.0.1:9392/login
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Sign in to your account
Username
admin
Password
Sign In
Greenbone
Community
EDITION




## Configuration for a new target

Begin by navigating to ***Scans > Tasks*** and clicking on the ***purple magic wand icon*** to begin the basic configuration wizard. After successfully navigating to the wizard, you should see a pop-up window similar to the one shown above. You can set up the initial scan of the local host here to make sure everything is set up correctly.

Scanning may take a while. Please allow OpenVAS enough time to complete the scan. You will then see a new dashboard for monitoring and analyzing your completed and ongoing scans, as shown below.

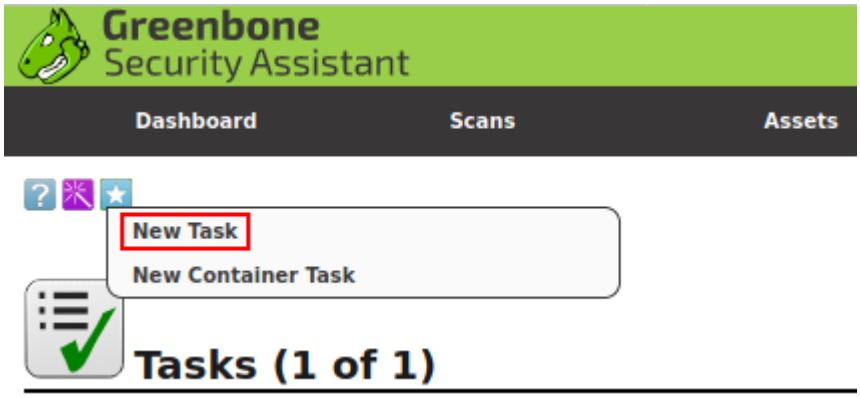



## Schedule the scanning process

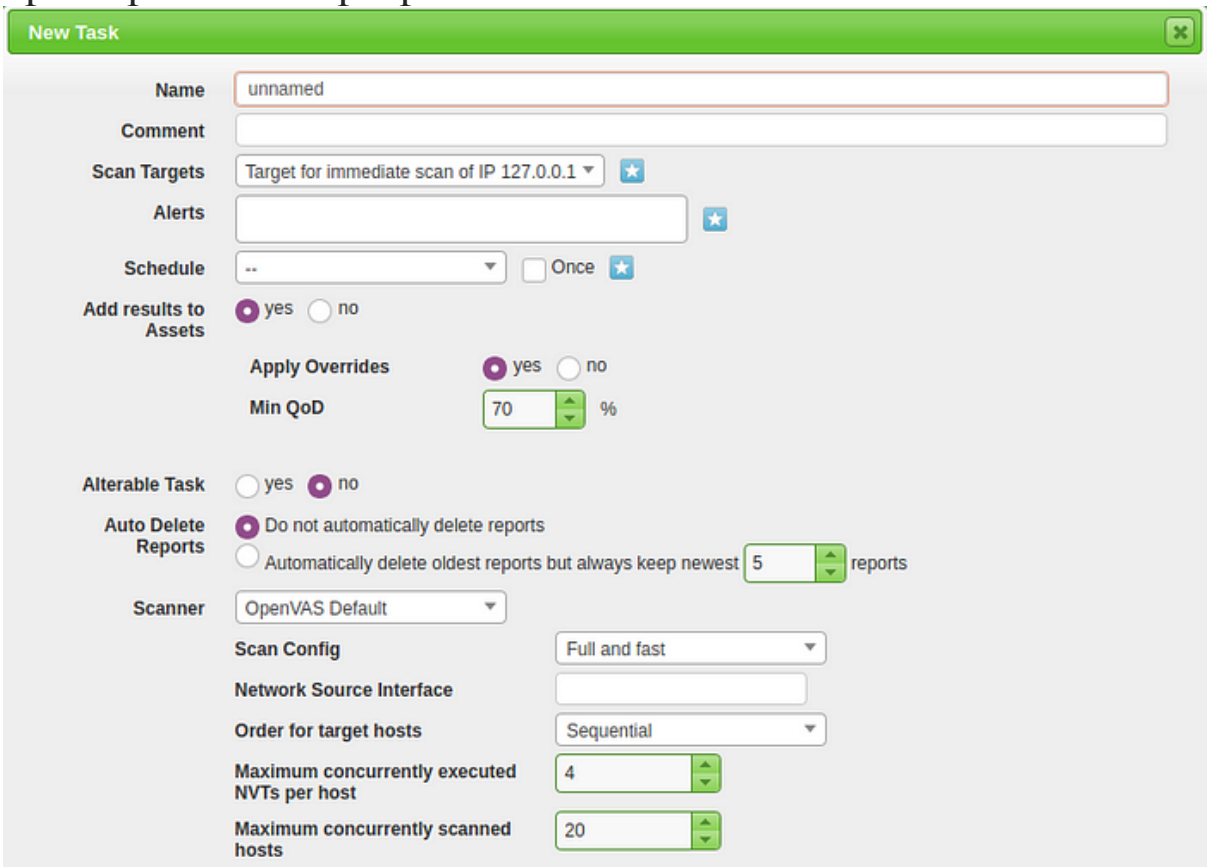
Now that we know everything is normal, we can take a closer look at OpenVAS and how it works. Expand the car to **scan and> start the task** of creating a scan task for the managed computer.

## Creating a Task

To create a custom task, navigate to the star icon in the upper right corner of the taskbar and select New task.




After selecting ” New Task” from the drop-down menu, you will see a large pop-up window with many options. We will introduce each option part and its purpose.

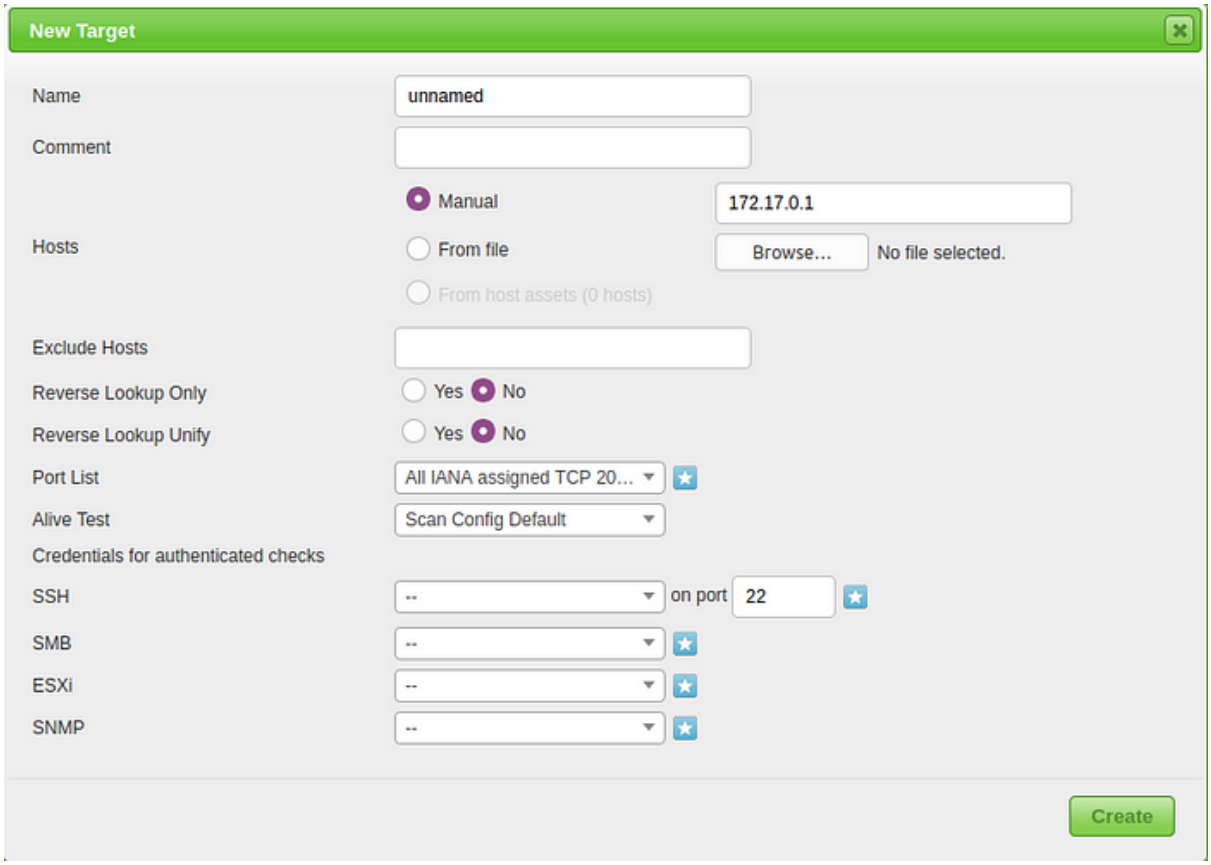



For this task, we’ll be specializing only in the Name, Scan Targets, and Scanner Type, and Scan Config. In later tasks, we will be focusing on the opposite choices for additional advanced configuration and implementation/automation.

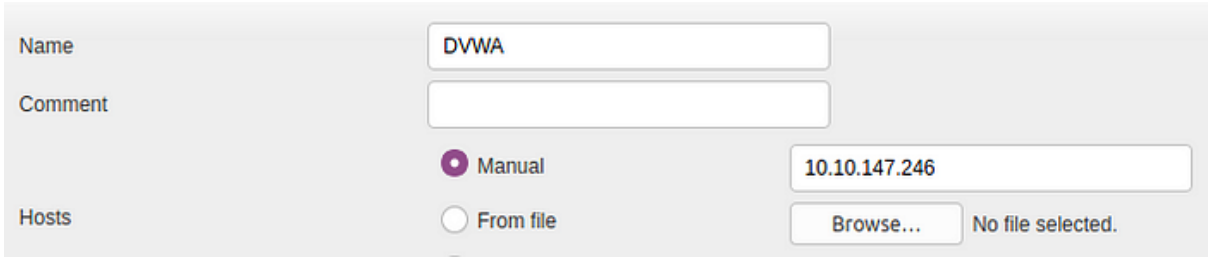
1. **Name**: permits North American country to line the name the scan are going to be referred to as inside OpenVAS
2. **Scan Targets:** The targets to scan, can embrace Hosts, Ports, and Credentials. to make a brand new target you may follow another pop-up, this can be lined later during this task.
3. **Scanner:** The scanner to use by default will use the OpenVAS design but you'll be able to set this to any scanner of your selecting within the settings menu.
4. **Scan Config**: OpenVAS has seven totally different scan sorts you can choose from and can be used supported however you're aggressive or what info you wish to gather from your scan.

### Scoping a New Target

To scope a new target, navigate to the star icon next to Scan Targets.




Above is that the menu for configuring a replacement target. the 2 main choices you may have to be compelled to assemble are the Name and therefore the Hosts. This procedure is fairly uncomplicated and different options will solely be employed in advanced vulnerability management solutions. These are going to be lined in later tasks.

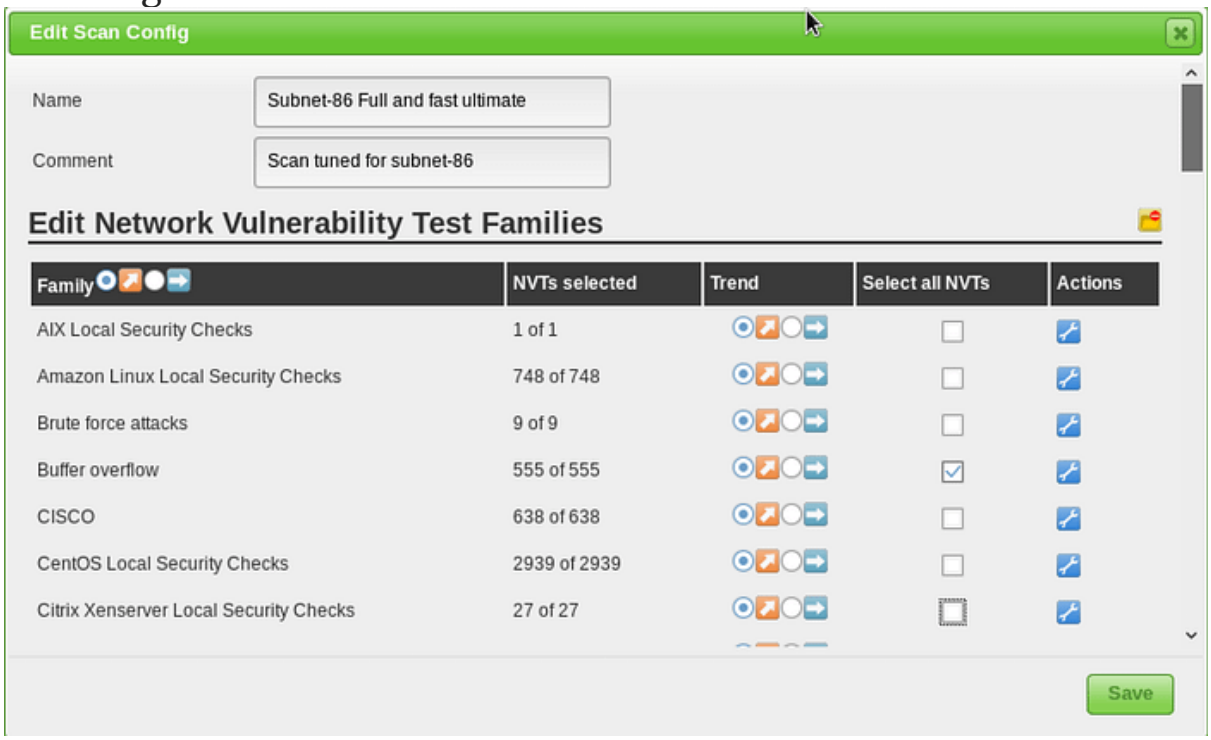



Now that we've got our target scoped we are able to still produce our task and start the scan. When the task is created, you'll come to the

scanning management panel, wherever you'll track and execute the task. To run the task, navigate to the run icon within the operation.

## Scan Configuration

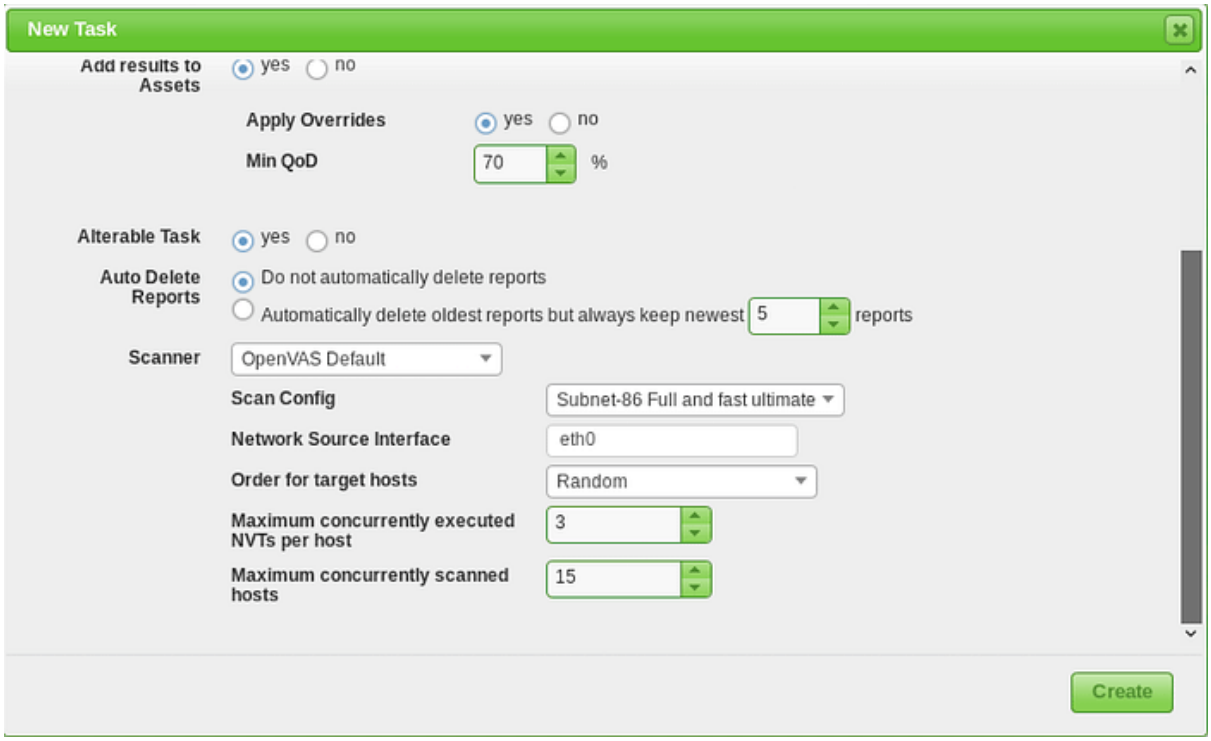
Prior to launching a vulnerability scan, you should fine-tune the Scan Config that will be used, which can be done under the "Scan Configs" section of the "Configuration" menu. You can clone any of the default Scan Configs and edit its options, disabling any services or checks that you don't require. If you use Nmap to conduct some prior analysis of your target(s), you can save hours of vulnerability scanning time.



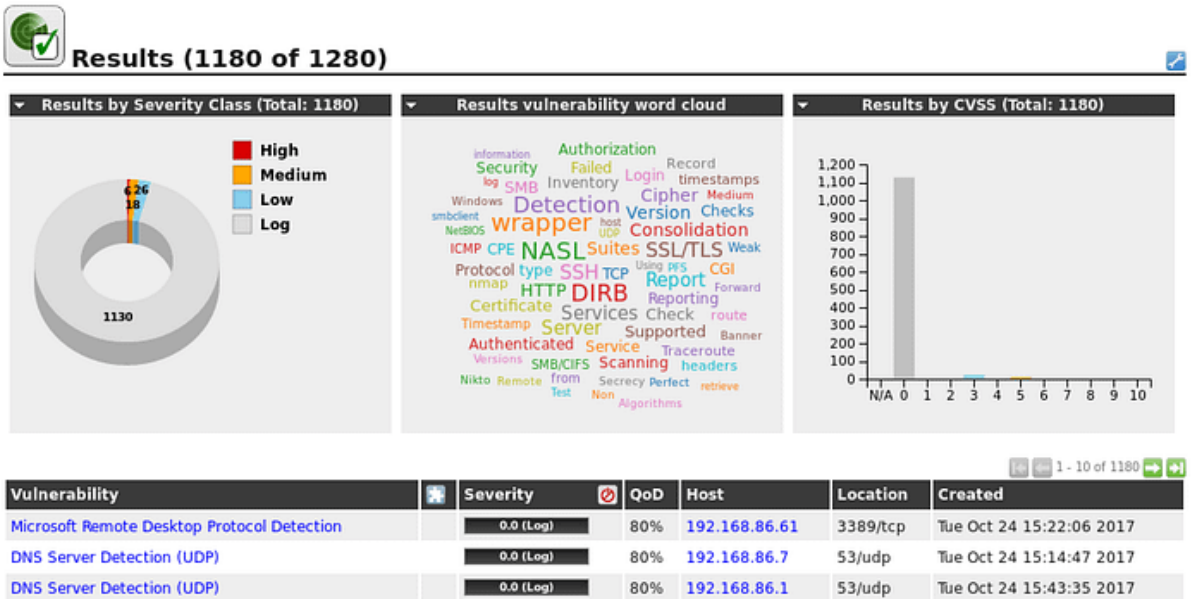

## Task Configuration

Your credentials, targets, and scan configurations are setup so now you're ready to put everything together and run a vulnerability scan. In OpenVAS, vulnerability scans are conducted as "Tasks". When you set up a new task, you can further optimize the scan by either

increasing or decreasing the concurrent activities that take place. With our system with 3GB of RAM, we adjusted our task settings as shown below.

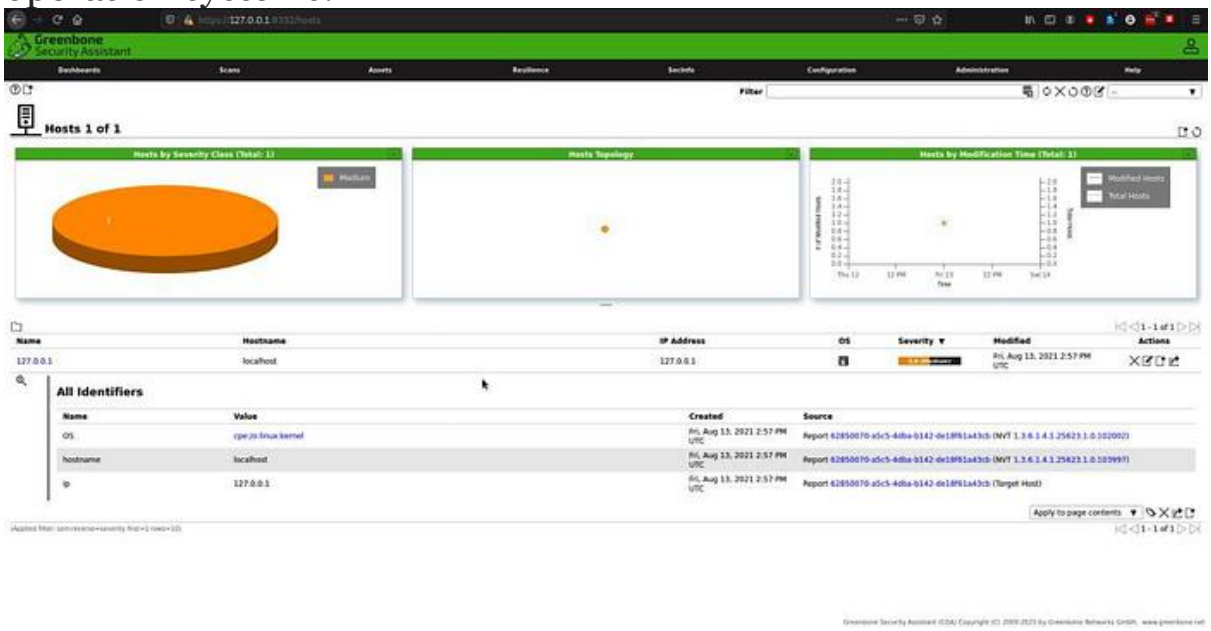



With our more finely-tuned scan settings and target selection, the results of our scan are much more useful.



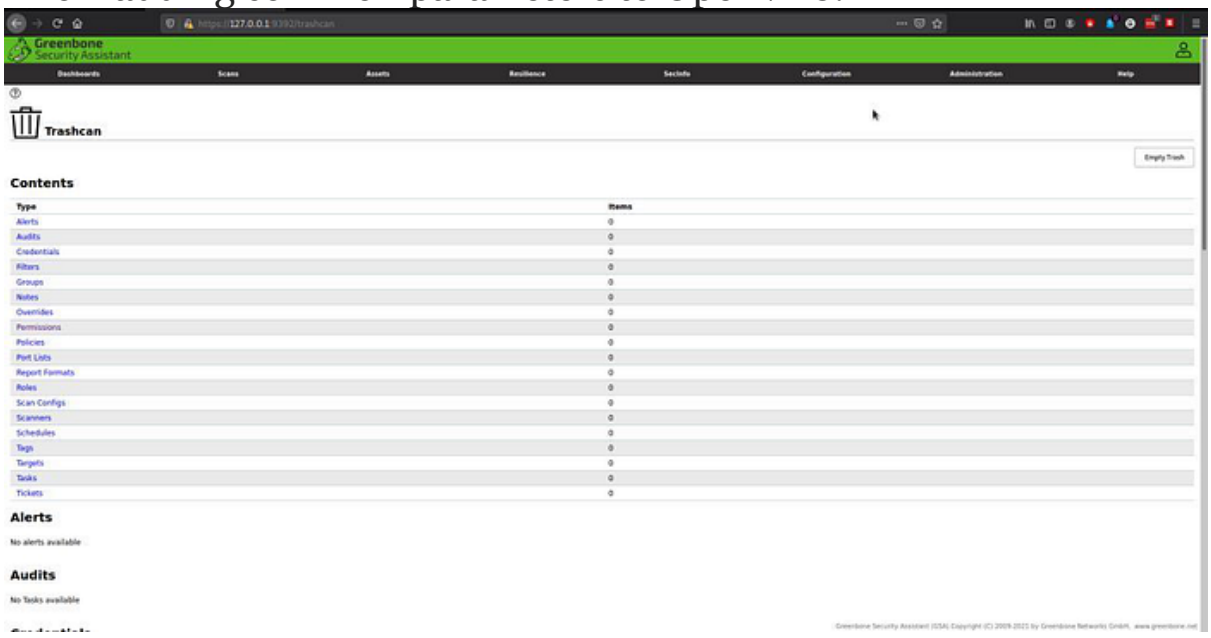

## Assets

It permits visualizing the vulnerability of the parts akin to hosts or in operation systems:



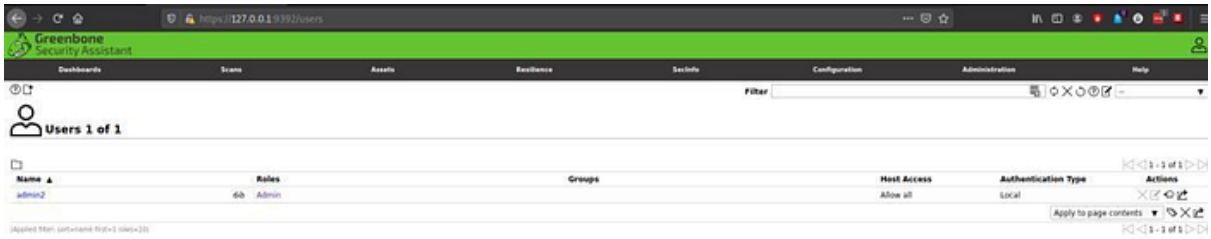

## Additional features

Allow adding common parameters to OpenVAS:




## Administration

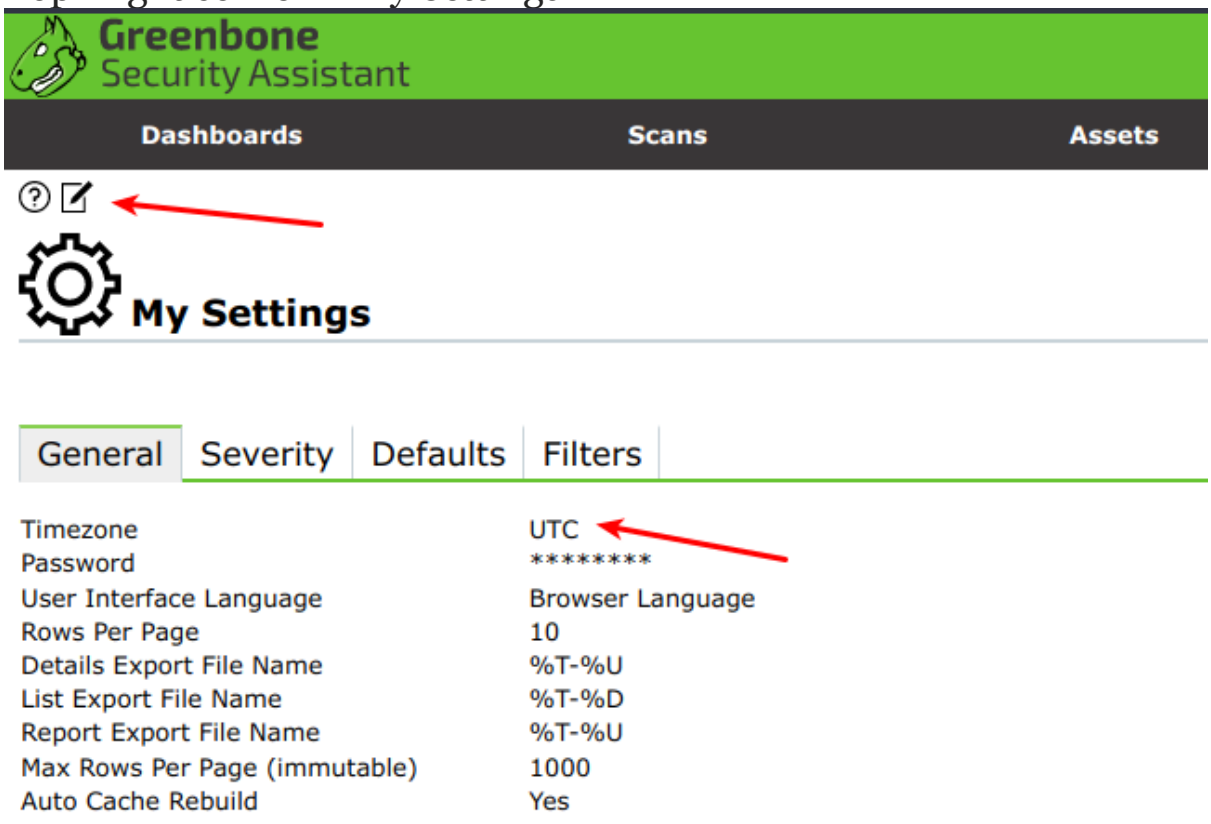
As the name suggests, you can manage passwords, users, etc.:




## Change timezone

***Note***: Recommend setting the timezone as UTC, the report displays UTC time only no matter what timezone you set

Top-Right corner > My Settings




With the wide range of options available in OpenVAS, we were only really able to just scratch the surface in this post but if you take your time and effectively tune your vulnerability scans, you will find that

the bad reputation of OpenVAS and other vulnerability scanners is undeserved. The number of connected devices in our homes and workplaces is increasing all the time and managing them becomes more of a challenge. Making effective use of a vulnerability scanner can make that management at least a little bit easier.