Dr. Ritika Ladha

Lecture 8: Cyber Security

- Introduction to OpenVAS
- Installation Guide
- Basic Scan Tasks on OpenVAS

OpenVAS (Open Vulnerability Assessment System) is an open-source framework used for vulnerability scanning and management. It is designed to detect security issues within networks, systems, and applications. Here's an introduction to OpenVAS and how to use it:

Key Features of OpenVAS

1. Comprehensive Scanning: OpenVAS can perform deep and comprehensive scans to identify vulnerabilities in network services, operating systems, web applications, databases, and more.

2. Regular Updates: The vulnerability database is regularly updated to include the latest known vulnerabilities and security checks.

3. Extensibility: Users can create custom checks and extend the capabilities of OpenVAS using its scripting language.

4. Reporting: OpenVAS generates detailed reports of vulnerabilities found, which include severity ratings and potential impacts.

5. Compliance Checking: It can check for compliance with various security standards, such as PCI-DSS, HIPAA, and others.

Components of OpenVAS

1. OpenVAS Scanner: The actual scanning engine that performs the network vulnerability tests.

2. OpenVAS Manager: Manages scan configurations, schedules, and stores scan results.

3. Greenbone Security Assistant (GSA): A web-based interface to manage scans, view results, and generate reports.

4. Greenbone Vulnerability Manager (GVM): Integrates with OpenVAS Manager to provide the core management functionality.

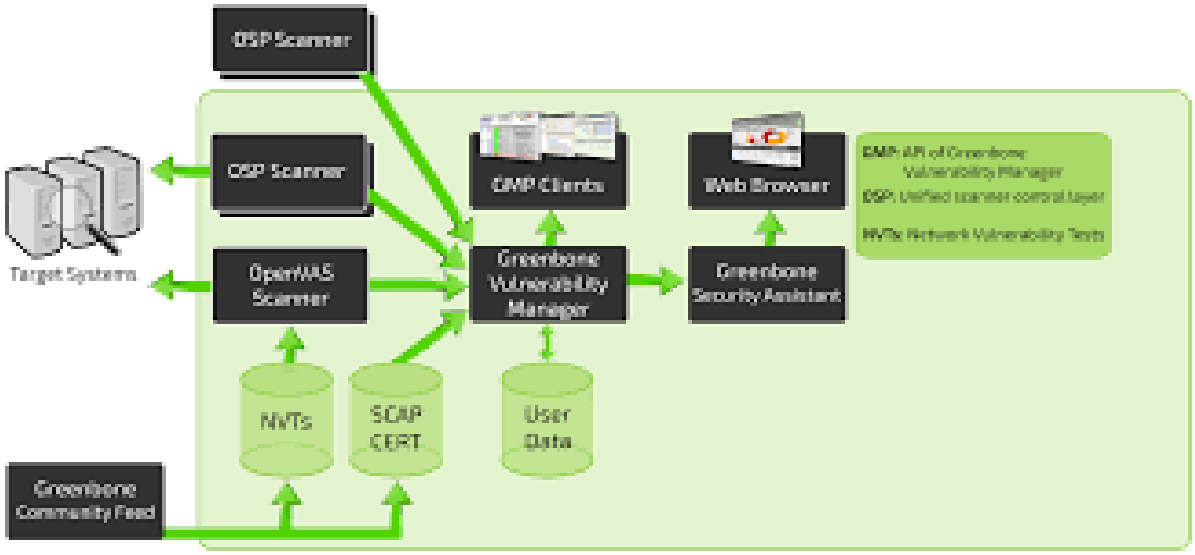
5. Greenbone Security Feed (GSF): Provides the updated list of vulnerability tests.

Dr. Ritika Ladha

GVM Framework Architecture

As previously mentioned OpenVAS is built off the GreenBone Vulnerability Management (GVM) solution and is only one of the appliances that is released from GreenBone.

There are many components that are apart of the architecture for the GVM framework, but we can break it down into three distinct sections: Front-End, Back-End, and Vulnerability/Information feed.



Vulnerability/Information Feed (NVT, SCAP CERT, User Data, Community Feed)

This section will contain all information and vulnerability tests that come from the Greenbone Community Feed that will be the main baseline for testing against systems. This can also include User Data provided by the user in place of Greenbone NVTs and SCAP CERTs.

Back-End (OSP, OpenVAS, Targets)

The back-end infrastructure is what will be actually conducting all of the vulnerability scanning and processing data and NVTS through OpenVAS and GVM. Greenbone Vulnerability Manager will be the middle man between the scanners and the front-end user interfaces.

Front-End (GSA, Web Interfaces)

This is what you interact with when you navigate to OpenVAS in your browser. The web interfaces are built off of the Greenbone Security Assistant and make life easier for an analyst or operator when working with OpenVAS or other forms of scanners through the GVM.

Dr. Ritika Ladha

Installation and Setup

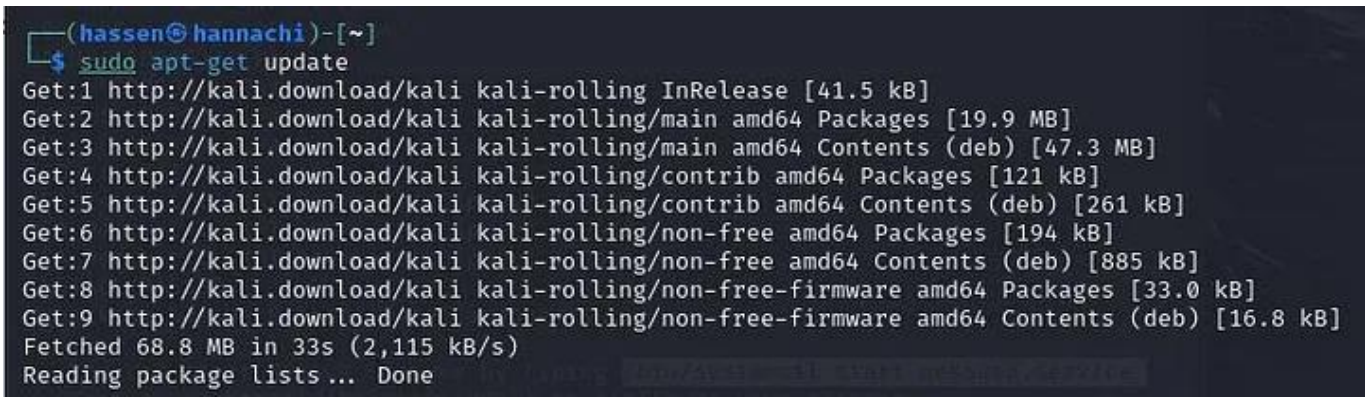
OpenVAS, an endpoint scanning application and web application used to identify and detect vulnerabilities. It is widely used by companies as part of their risk mitigation solutions to quickly identify gaps in their production and even development servers or applications. This is not a complete solution, 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

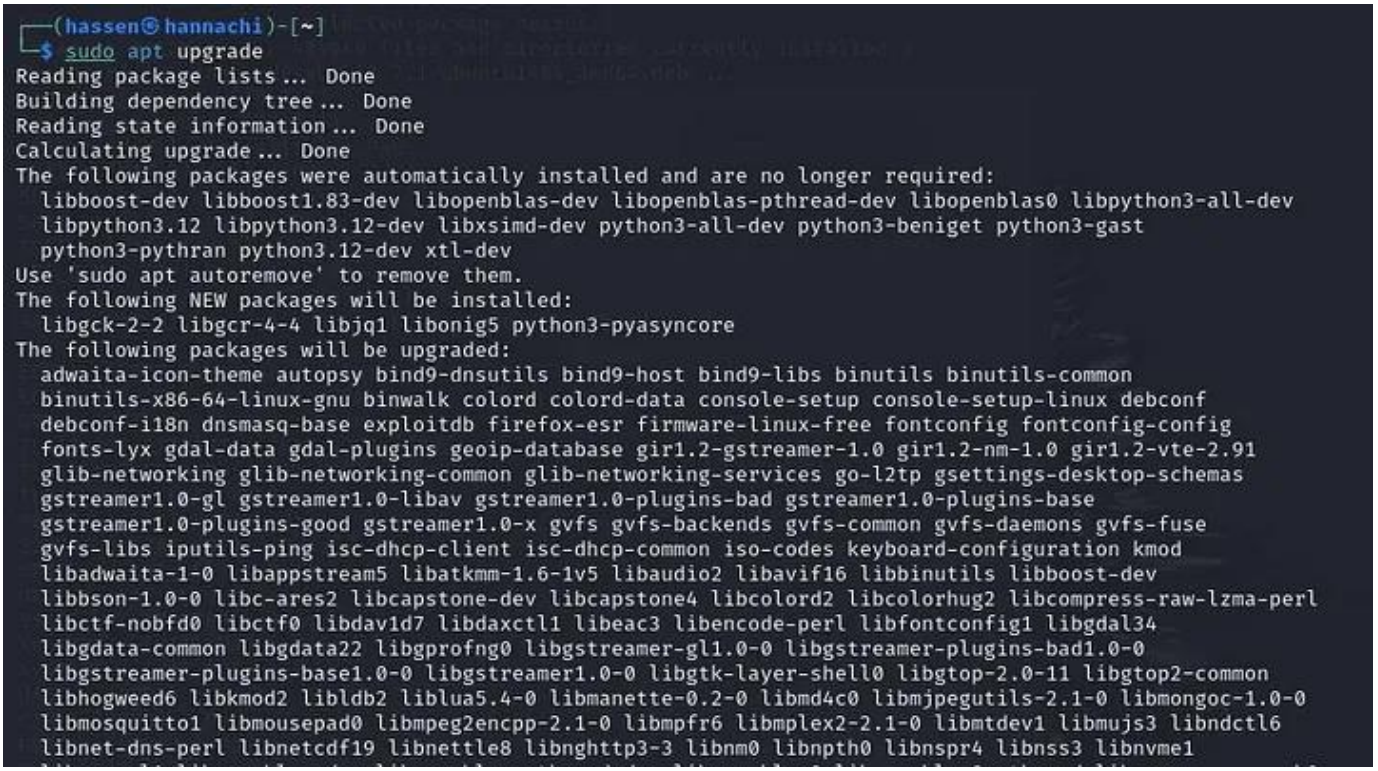
Unless you have already done so, make sure that the Kali Linux is up to date and install the latest Kali Linux. You automatically download the latest rules, create admin users, and start the various services. Depending on bandwidth and computer resources, this may take a while.

sudo apt update — or use sudo apt-get update



Dr. Ritika Ladha

sudo apt upgrade -y



sudo apt dist-upgrade -y

Installing OpenVAS on Kali Linux

Dr. Ritika Ladha

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

sudo apt install openvas

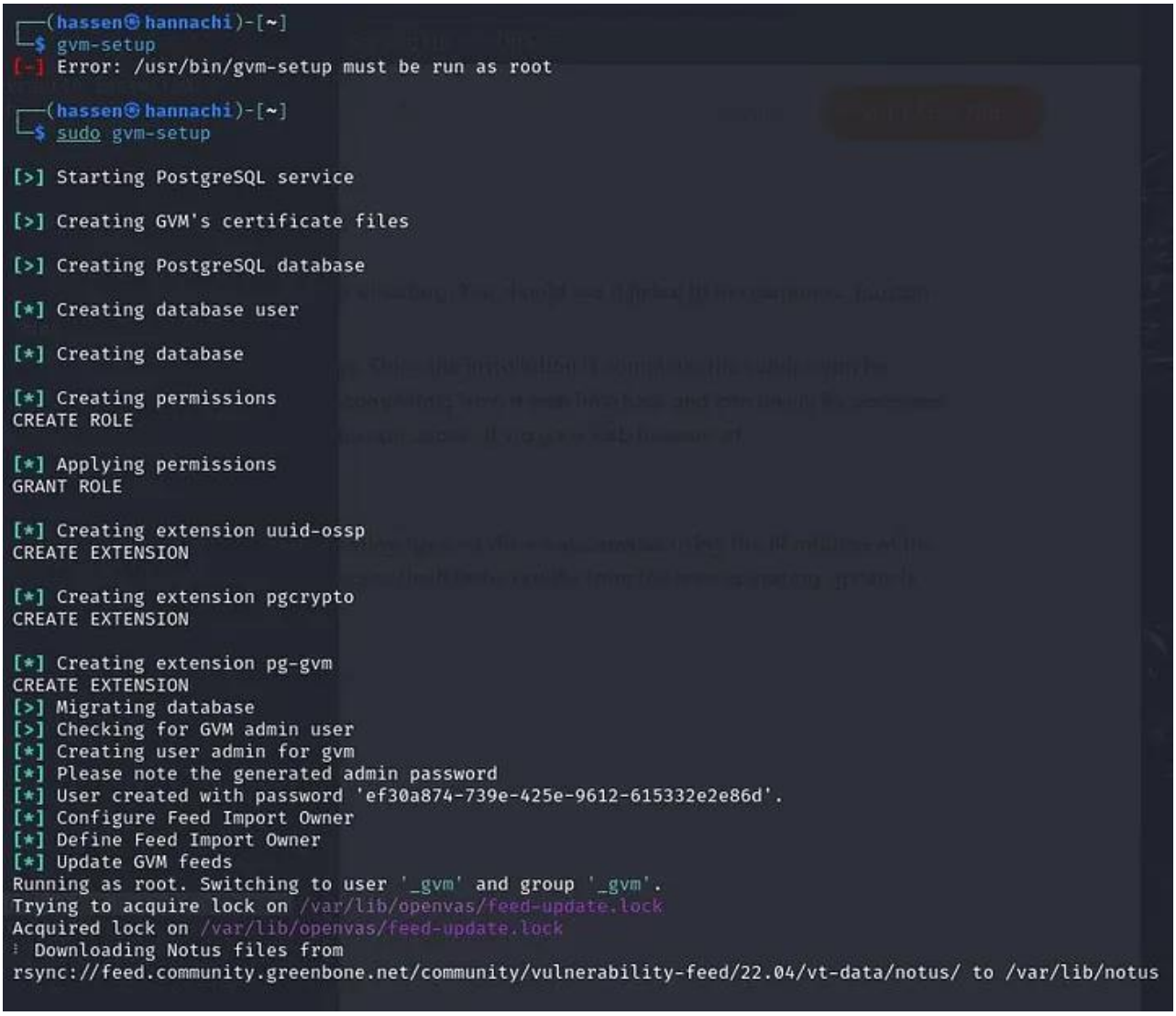
or use

sudo apt install gvm

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



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

Note: 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.

Dr. Ritika Ladha

update admin user password

Note: To create a new user

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

```
┌──(hassen㉿hannachi)-[~]
└─$ sudo gvm-check-setup
gvm-check-setup 23.11.0
  Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 22.7.9.
        OK: Notus Scanner is present in version 22.6.2.
        OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
        OK: _gvm owns all files in /var/lib/openvas/gnupg
        OK: redis-server is present.
        OK: scanner (db_address setting) is configured properly using the redis-
server socket: /var/run/redis-openvas/redis-server.sock
        OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
        OK: _gvm owns all files in /var/lib/openvas/plugins
        OK: NVT collection in /var/lib/openvas/plugins contains 88489 NVTs.
        OK: The notus directory /var/lib/notus/products contains 456 NVTs.
Checking that the obsolete redis database has been removed
        OK: No old Redis DB
        Starting ospd-openvas service
        Waiting for ospd-openvas service
        OK: ospd-openvas service is active.
        OK: ospd-OpenVAS is present in version 22.6.2.
Step 2: Checking GVMD Manager ...
        OK: GVM Manager (gvmd) is present in version 23.1.0.
Step 3: Checking Certificates ...
        OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clien
tcert.pem.
        OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
        OK: SCAP data found in /var/lib/gvm/scap-data.
        OK: CERT data found in /var/lib/gvm/cert-data.
```

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

Dr. Ritika Ladha

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.

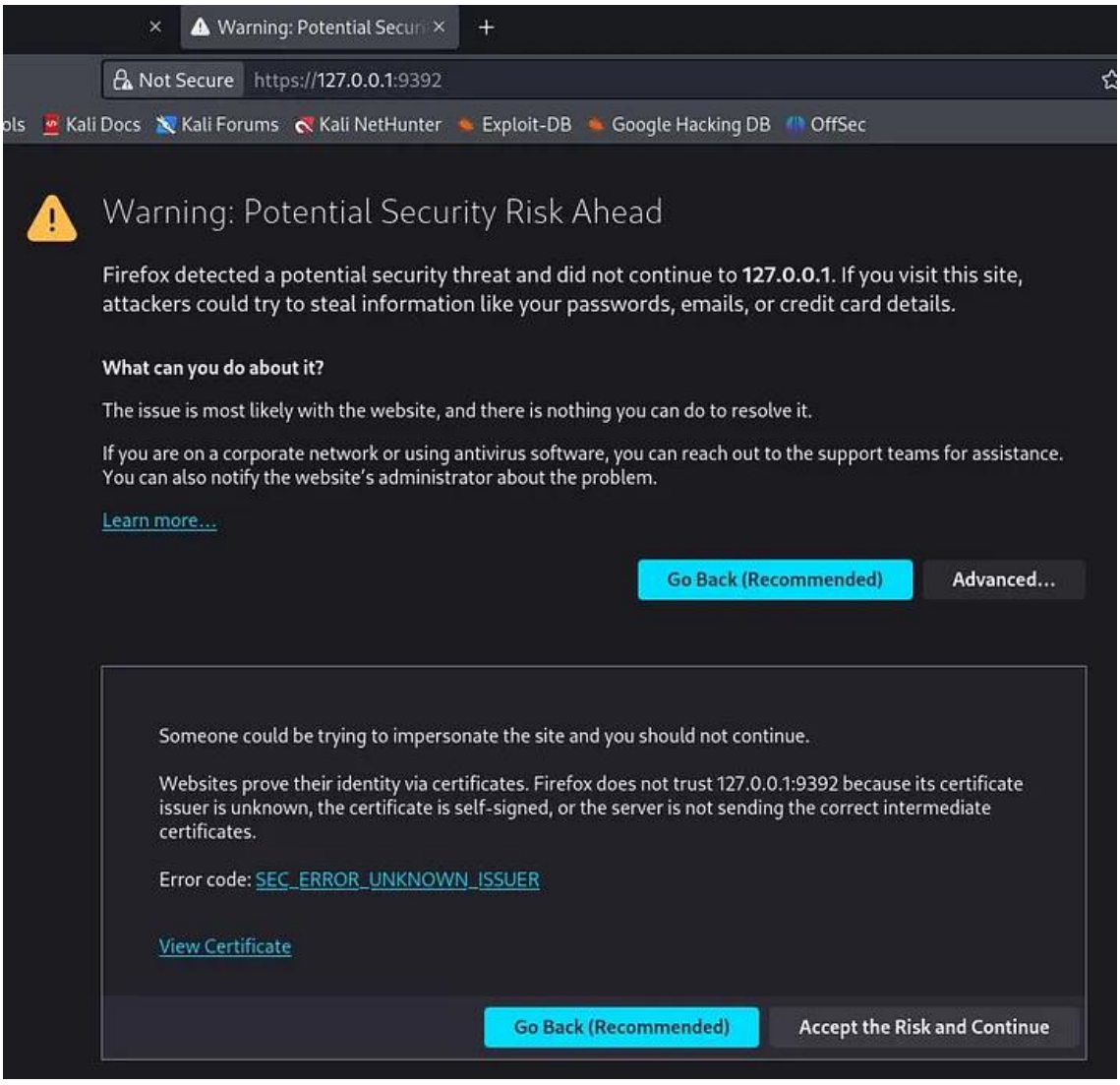
Run the following command to start the services:

sudo gvm-start

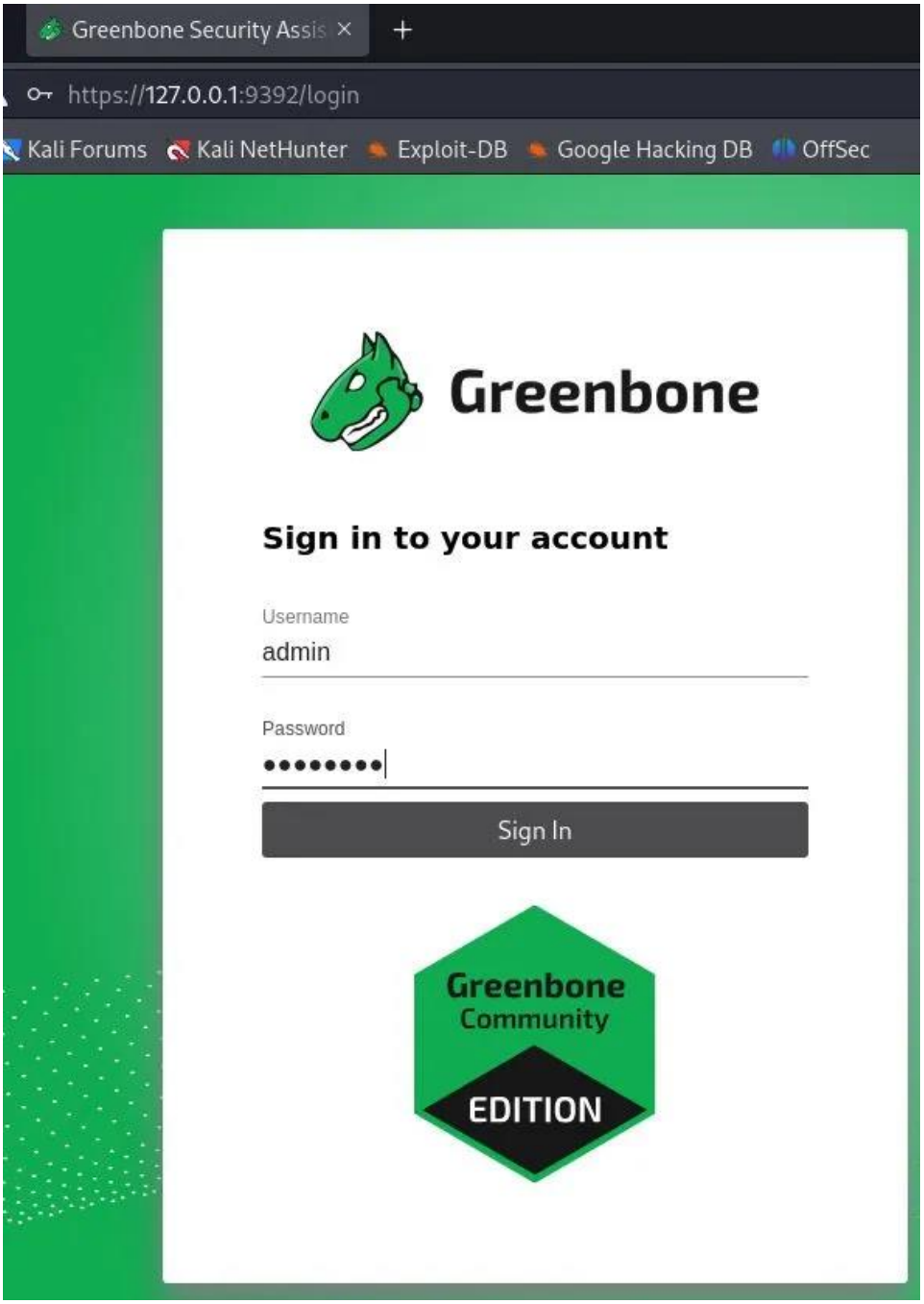
Hint: To stop the OpenVAS services again, run: sudo gvm-stop

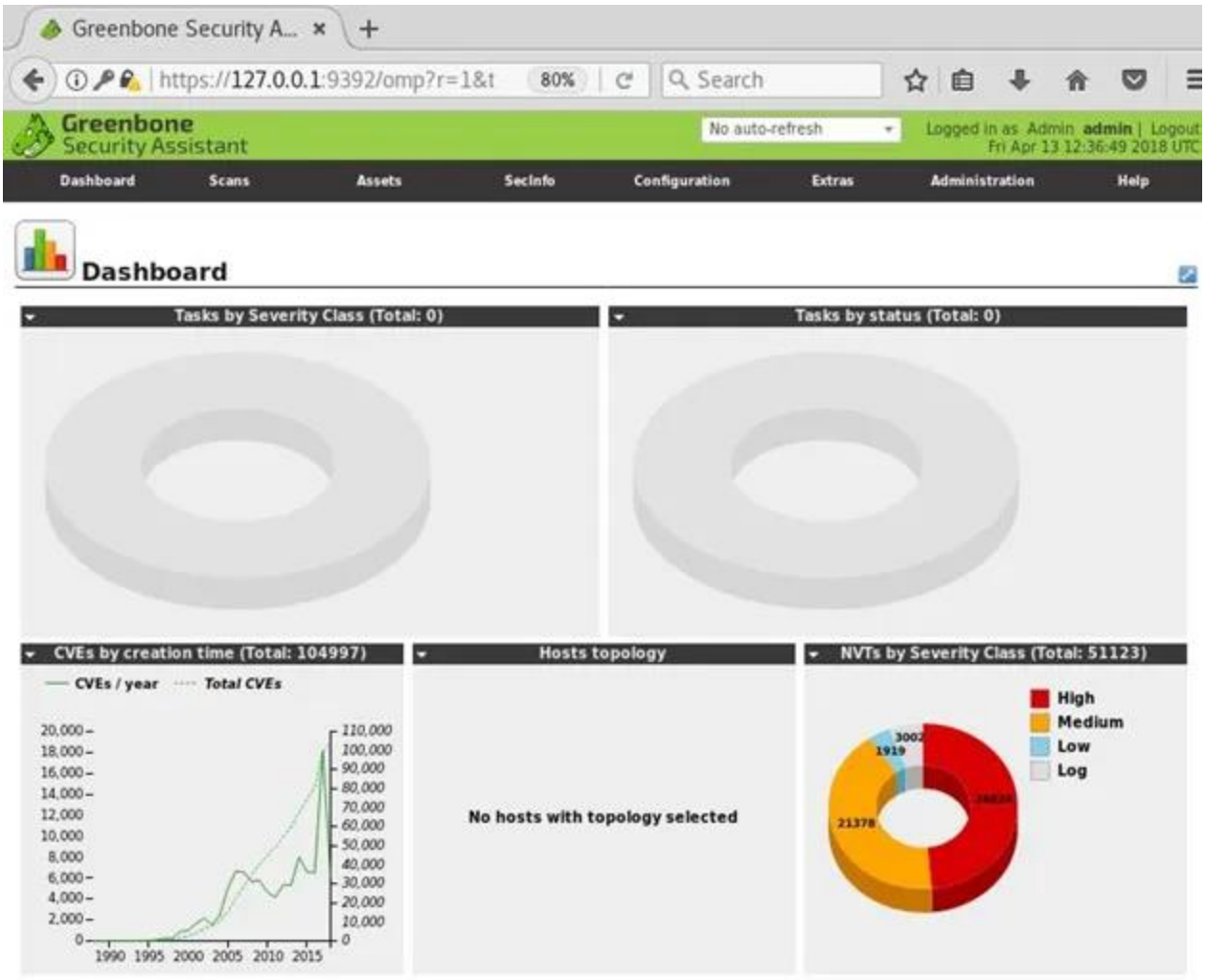
After the configuration process is complete, all the necessary OpenVAS processes will start and the web interface will open automatically (In my case I had to open the browser manually). The web interface is running locally on port 9392 and can be accessed through https://localhost:9392

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:

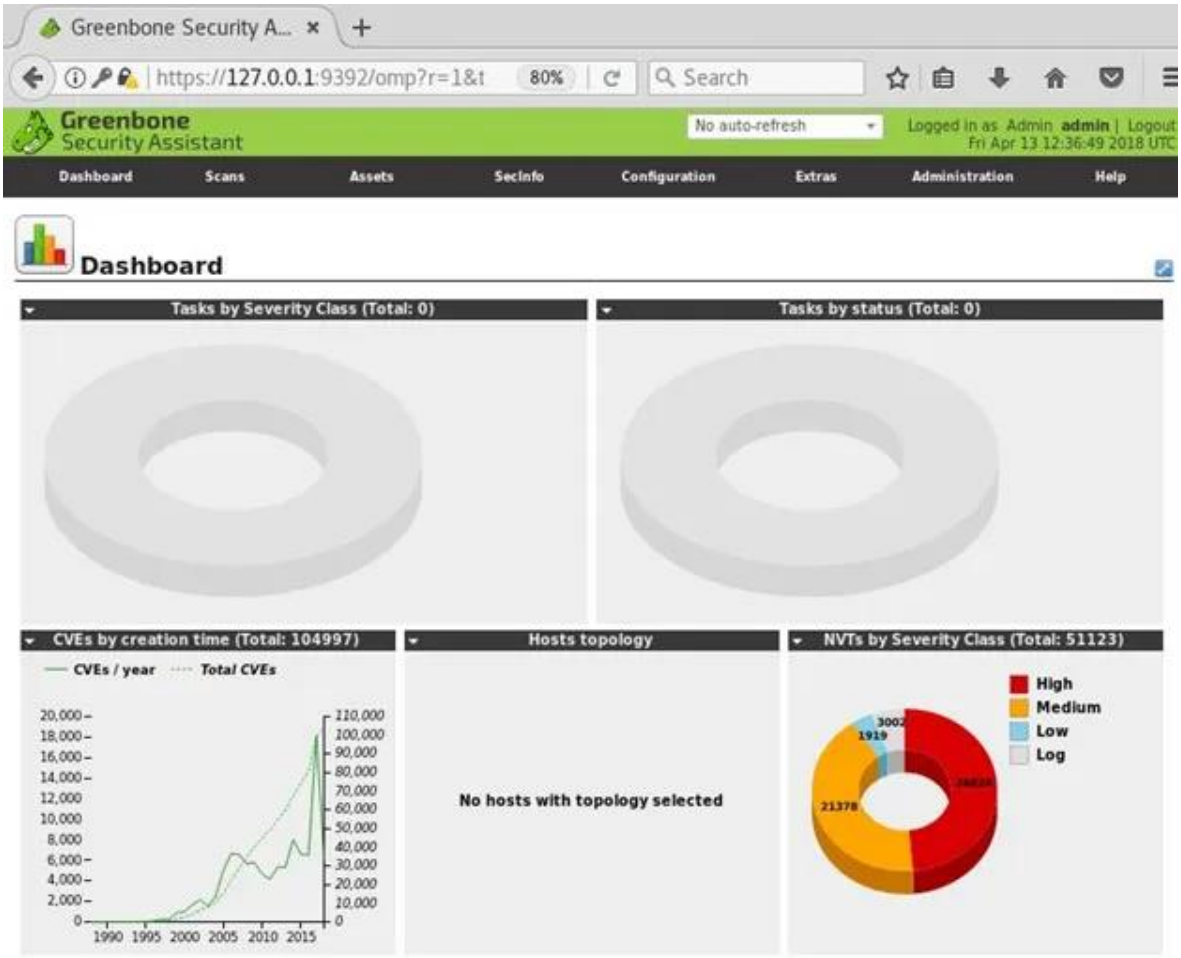




Configuration for a new target

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.

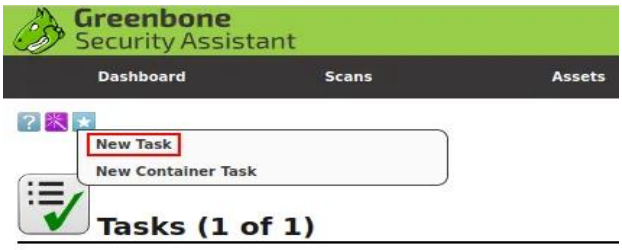


Schedule the scanning process

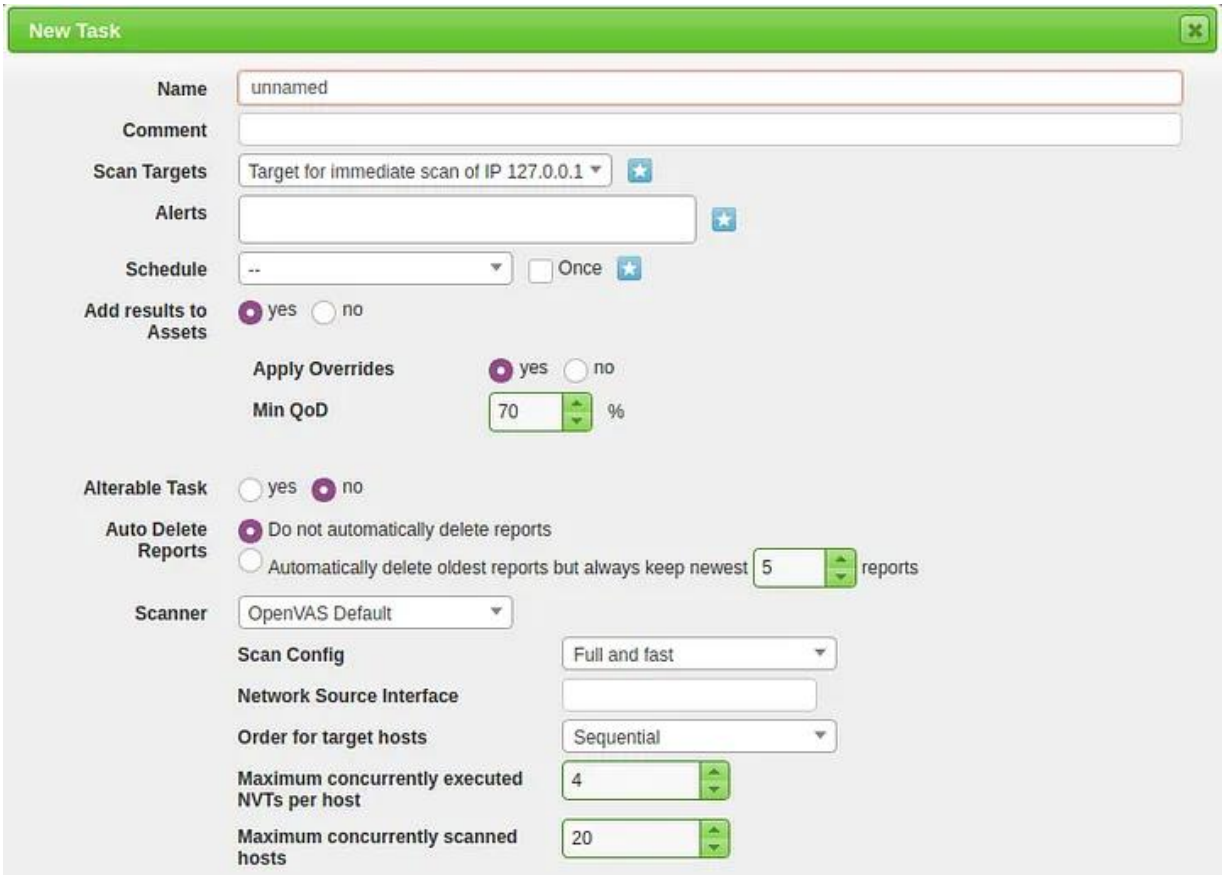
Now that we know everything is normal, we can take a closer look at OpenVAS and how it works. Expand the car to scan and> start the task of creating a scan task for the managed computer.

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.

Name: permits North American country to line the name the scan are going to be referred to as inside OpenVAS

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.

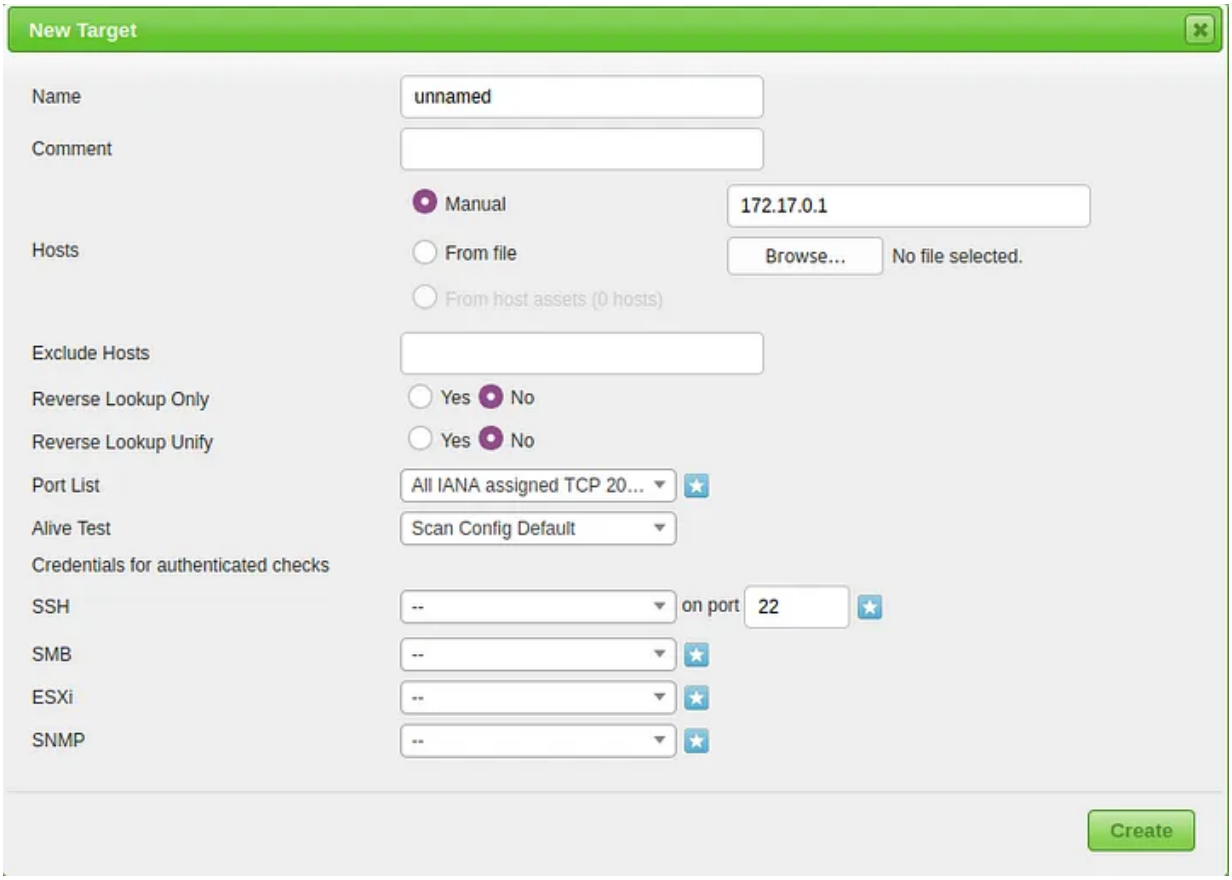
Scanner: The scanner to use by default will use the OpenVAS design but you’ll be able to set this to any scanner of your selecting within the settings menu.

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.

Dr. Ritika Ladha

Scoping a New Target

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

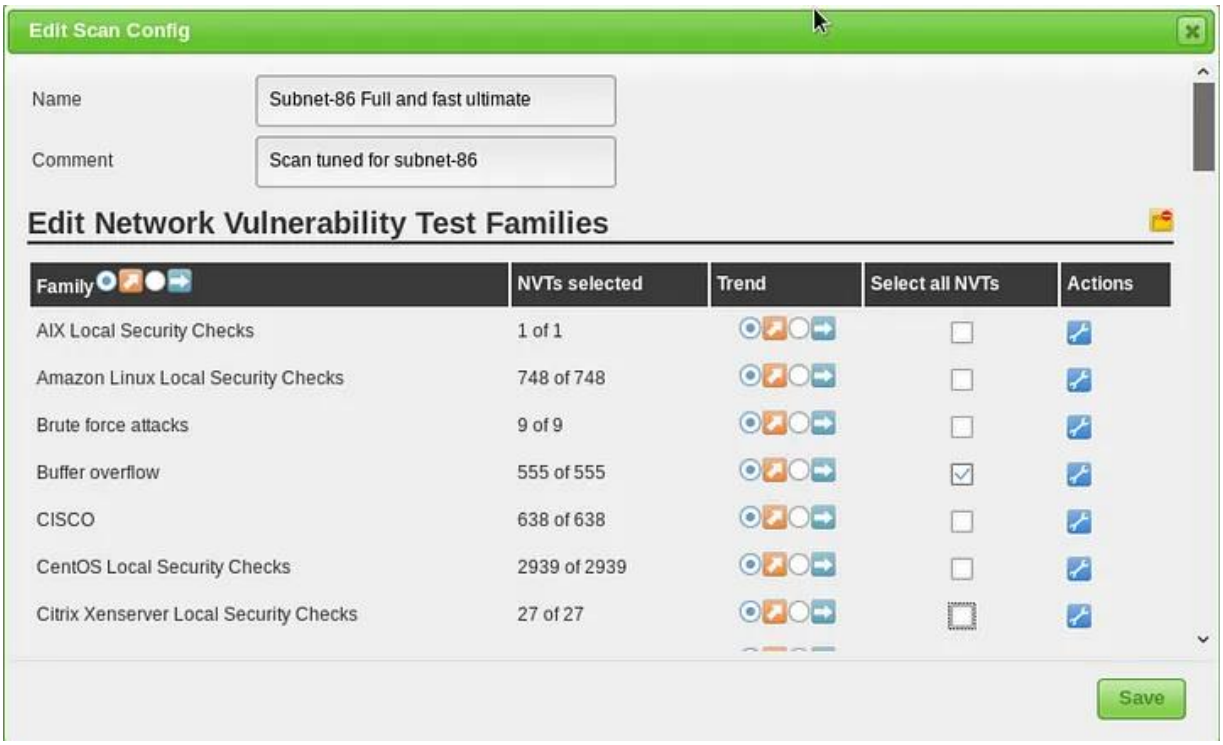


Above is that the menu for configuring a replacement target. the 2 main choices you may have to be compelled to assemble are the Name and therefore the Hosts. This procedure is fairly uncomplicated and different options will solely be employed in advanced vulnerability management solutions. These are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

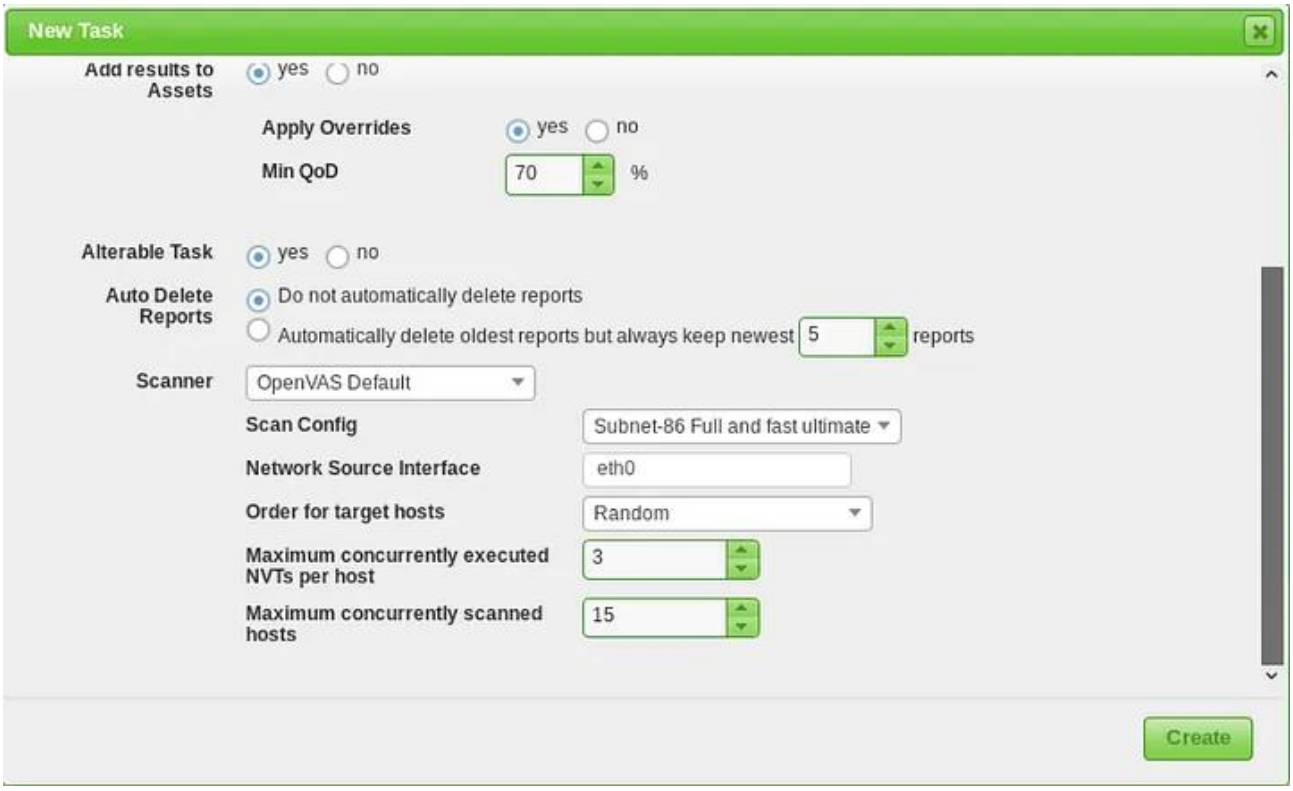
Scan Configuration

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.

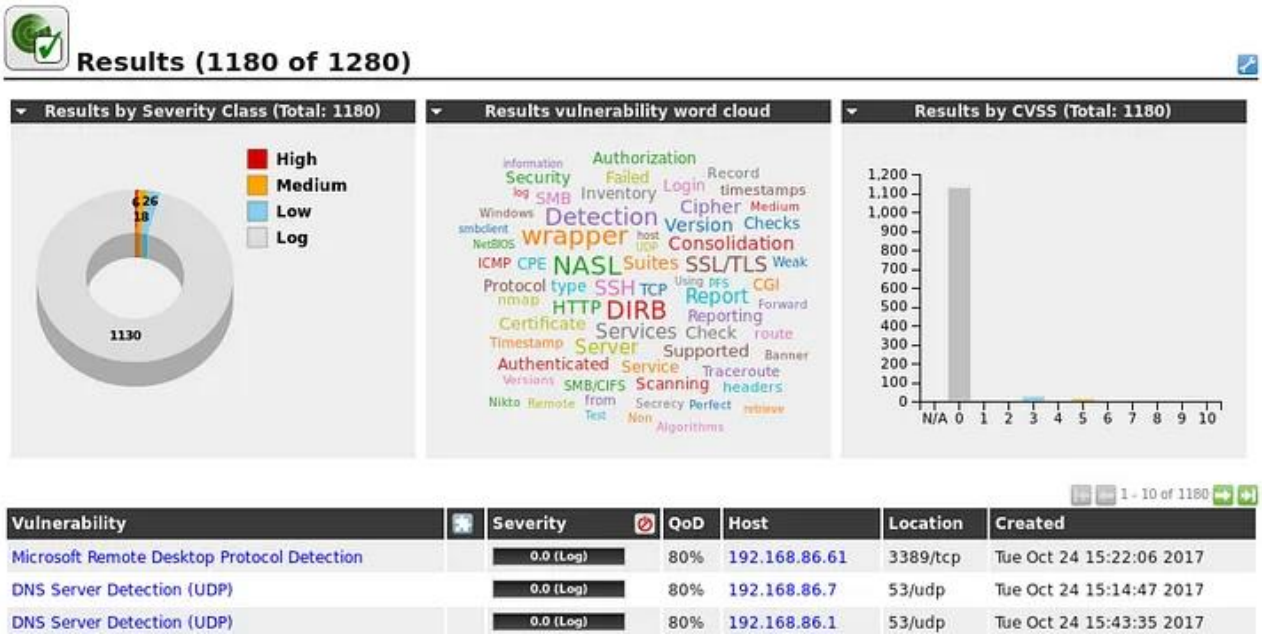


Task Configuration

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.



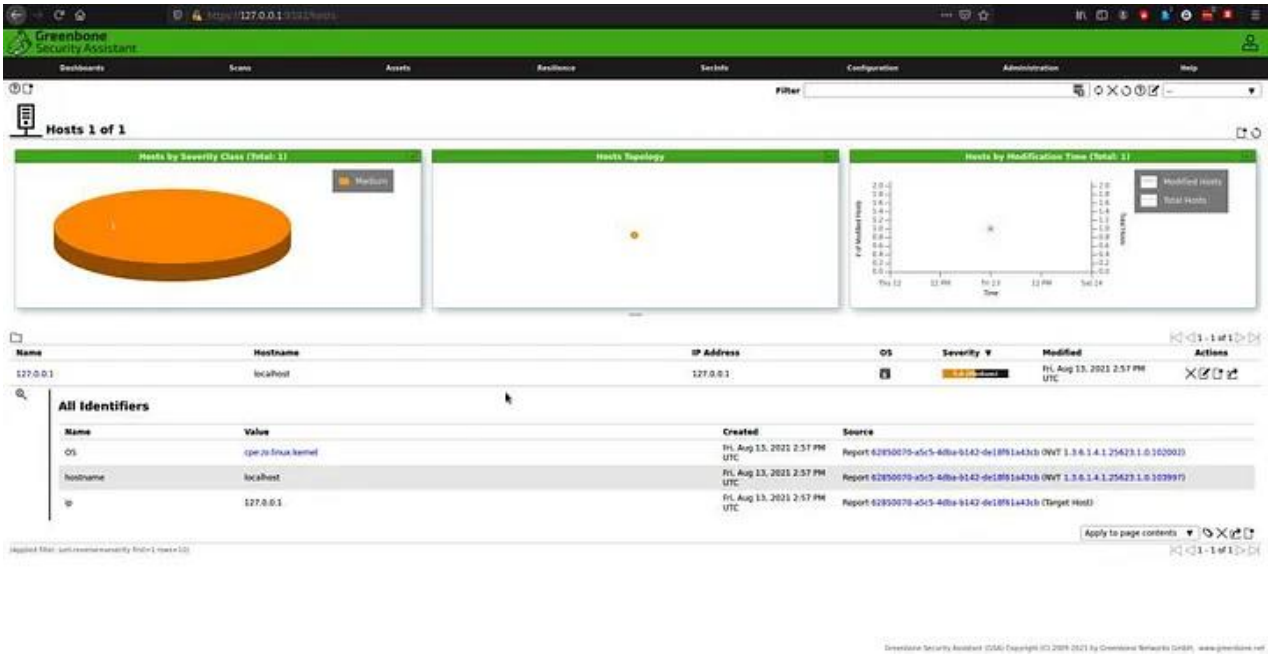
With our more finely-tuned scan settings and target selection, the results of our scan are much more useful.



Dr. Ritika Ladha

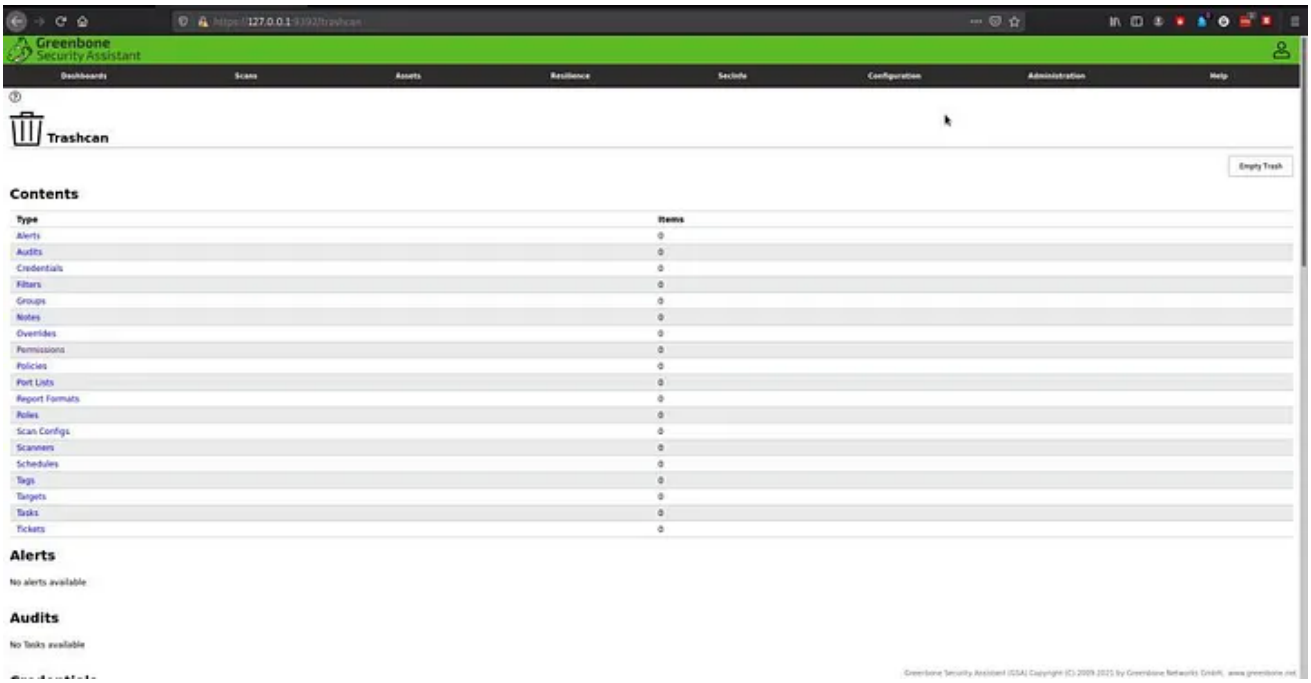
Assets

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



Additional features

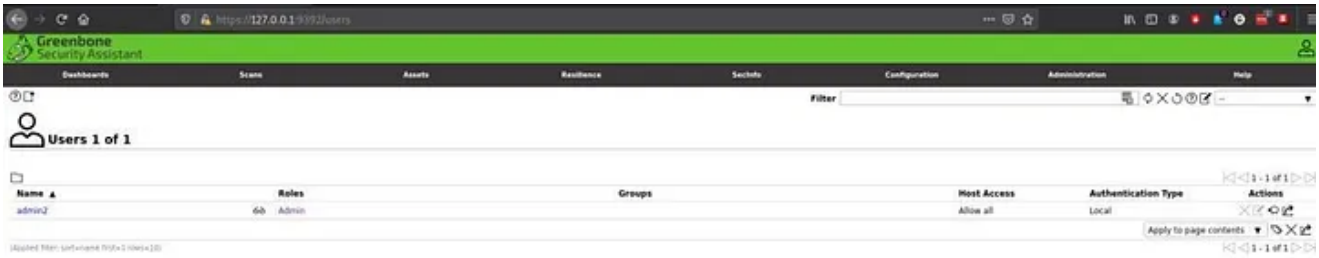
Allow adding common parameters to OpenVAS:



Dr. Ritika Ladha

Administration

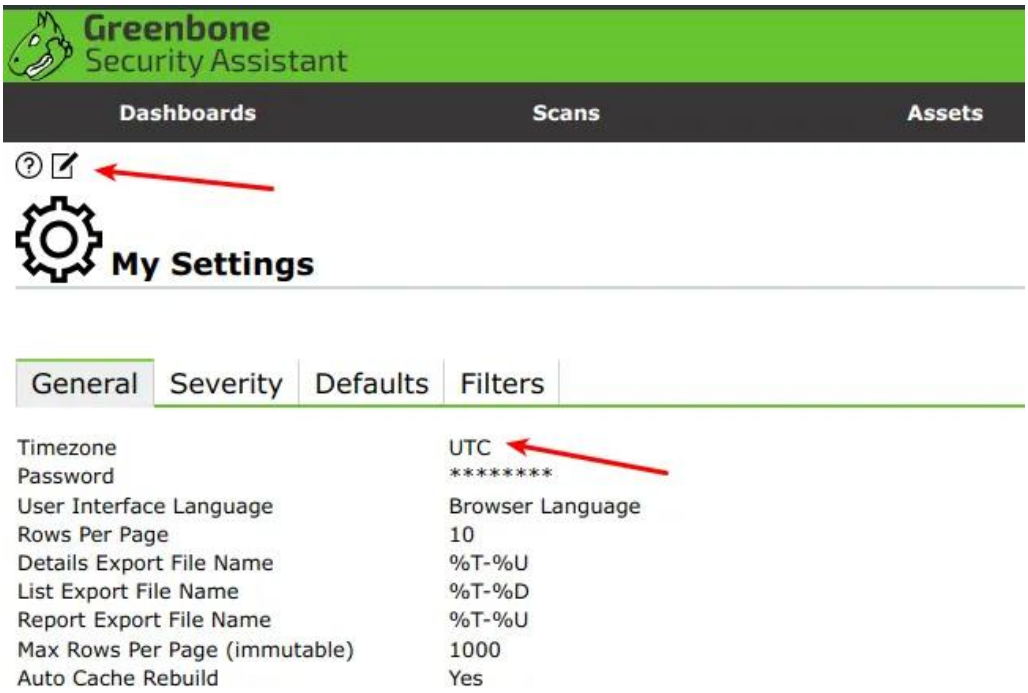
As the name suggests, you can manage passwords, users, etc.:



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



Dr. Ritika Ladha

Advanced Configuration

1. Custom Scan Configurations: Users can create custom scan configurations to tailor the vulnerability checks according to specific requirements.

2. User Management: Administrators can create multiple user accounts with different permission levels.

3. Automating Scans: OpenVAS supports scheduling scans to run at specified intervals, ensuring continuous monitoring.

4. Integrations: OpenVAS can be integrated with other security tools and SIEM systems for a comprehensive security management approach.

Best Practices

1. Regular Updates: Ensure that OpenVAS and its vulnerability database are regularly updated to detect the latest vulnerabilities.

2. Custom Policies: Customize scan policies to fit the specific security needs of your environment.

3. Frequent Scanning: Perform regular scans to identify and remediate vulnerabilities promptly.

4. Review and Act: Regularly review scan results and take appropriate actions to mitigate identified vulnerabilities.

5. Secure OpenVAS: Ensure that the OpenVAS server and web interface are secured and accessible only to authorized personnel.

OpenVAS is a powerful tool for maintaining the security posture of an organization by identifying and managing vulnerabilities effectively. By leveraging its capabilities, organizations can proactively protect their assets from potential security threats.