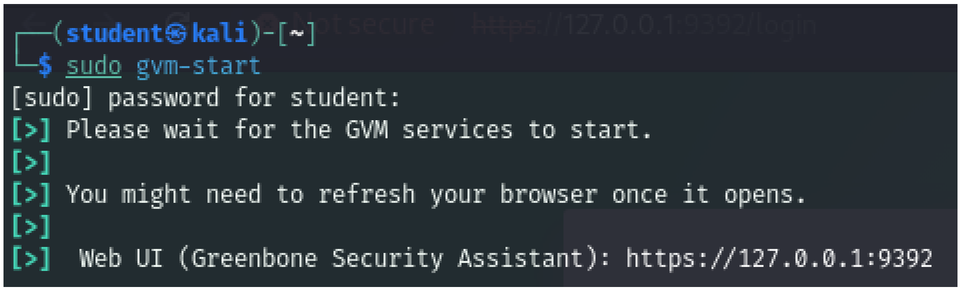
Part 1 : Execute openvas scans

1. Start OpenVAS on Kali Linux

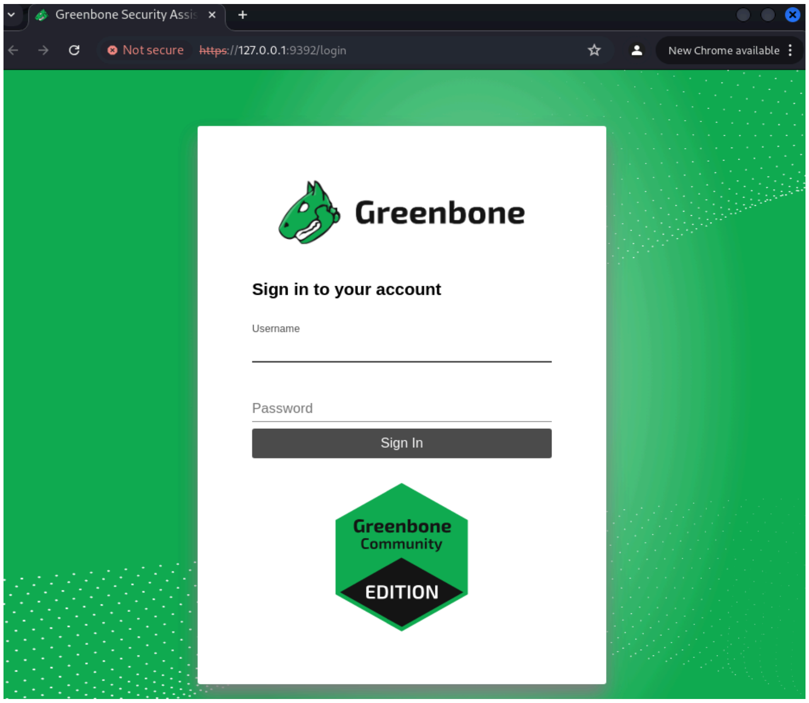
Open kali linux
Open terminal

Type in the terminal the command: sudo gvm-start



```
┌──(student㉿kali)-[~]
└─$ sudo gvm-start
[sudo] password for student:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

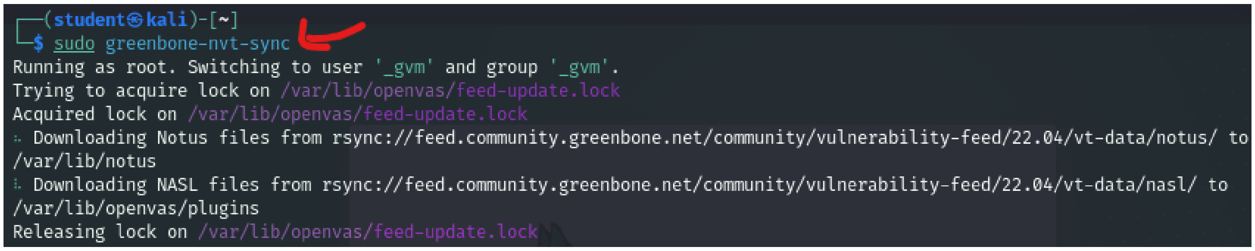
A browser page with openvas login should appear



2. Update openvas feeds

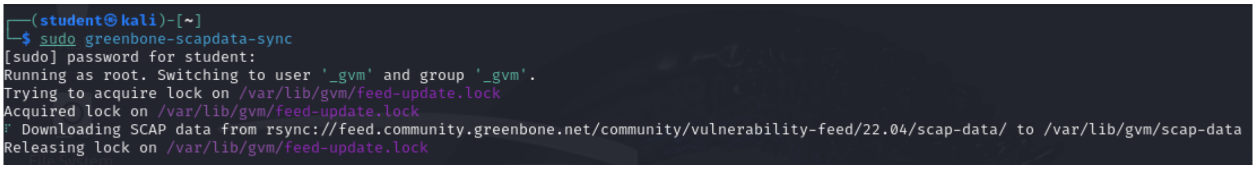
Login to the openvas site.
Go to the Administration tab and check Feed Status
If the status of the content is not current, update feeds using the following commands:

In the terminal type : sudo greenbone-nvt-sync
This will update the NVT's feed



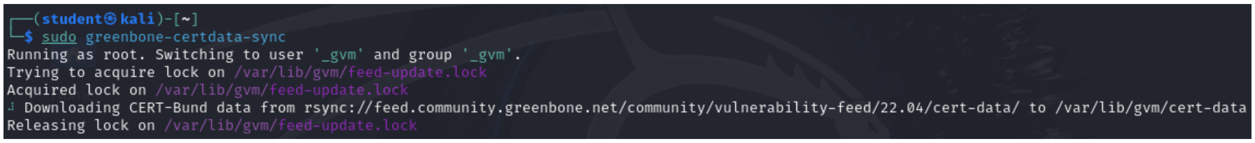
```
┌──(student㉿kali)-[~]
└─$ sudo greenbone-nvt-sync
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
⠦ Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to
/var/lib/notus
⠇ Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to
/var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
```

In the terminal type : sudo greenbone-scapdata-sync
This will update the scapdata feed



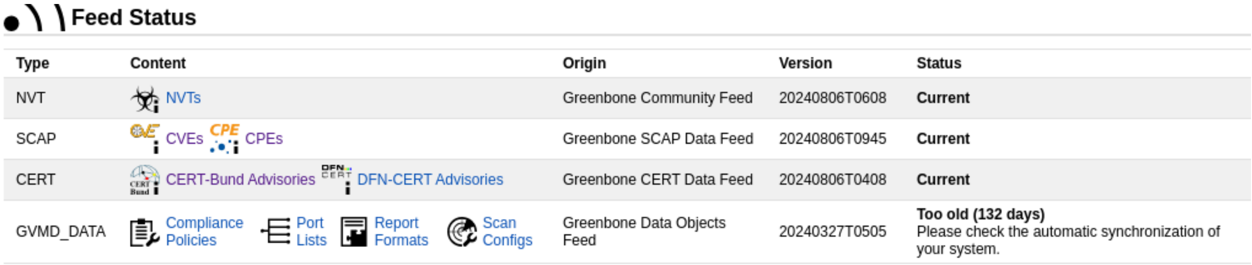
```
┌──(student㉿kali)-[~]
└─$ sudo greenbone-scapdata-sync
[sudo] password for student:
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
⠏ Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to /var/lib/gvm/scap-data
Releasing lock on /var/lib/gvm/feed-update.lock
```

In the terminal type : sudo greenbone-certdata-sync
This will update the certdata feed



```
┌──(student㉿kali)-[~]
└─$ sudo greenbone-certdata-sync
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
⠼ Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
Releasing lock on /var/lib/gvm/feed-update.lock
```

Then, if the feed status is updated, you should see this in the administrations page:



Feed Status

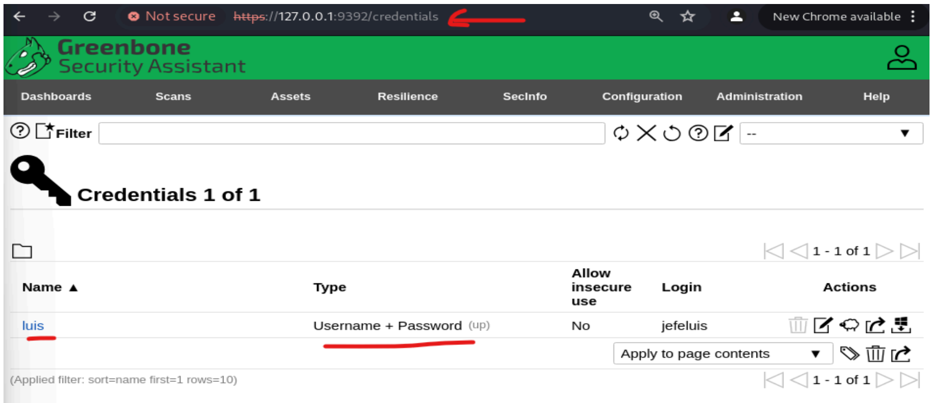
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20240806T0608	**Current**
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20240806T0945	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20240806T0408	**Current**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20240327T0505	**Too old (132 days)** Please check the automatic synchronization of your system.

3. Add Credential

Navigate to the Configuration tab
Select Credentials
Click the Add New Credential icon.
Insert the following info:

- Name: luis
- Username: jefeluis
- Password: jefeluis
- press save

In the credentials page you should see :



Credentials 1 of 1

1 - 1 of 1

Name ▲	Type	Allow insecure use	Login	Actions
luis	Username + Password (up)	No	jefeluis	

(Applied filter: sort=name first=1 rows=10)

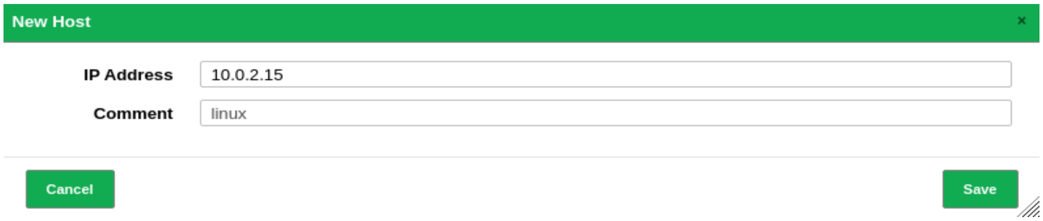
1 - 1 of 1

4. Add Hosts

Go to the Assets tab
Select Hosts

<u>Add linux computer as host</u>
Click the Add New Host icon
Insert the following info:

- Name: linux
- IP Address: 10.0.2.15
- Press save



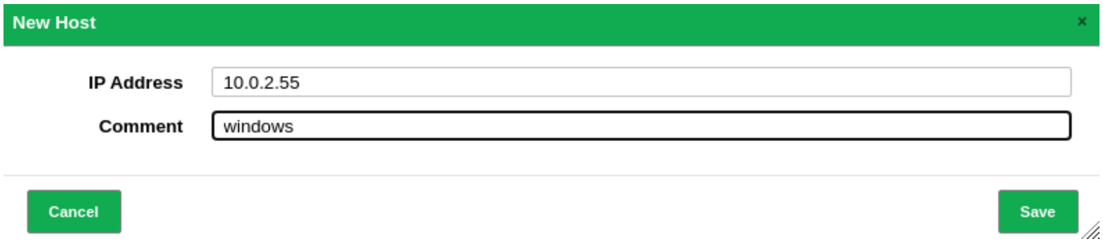
IP Address	10.0.2.15
Comment	linux

Add windows computer as host

Click the Add New Host icon.

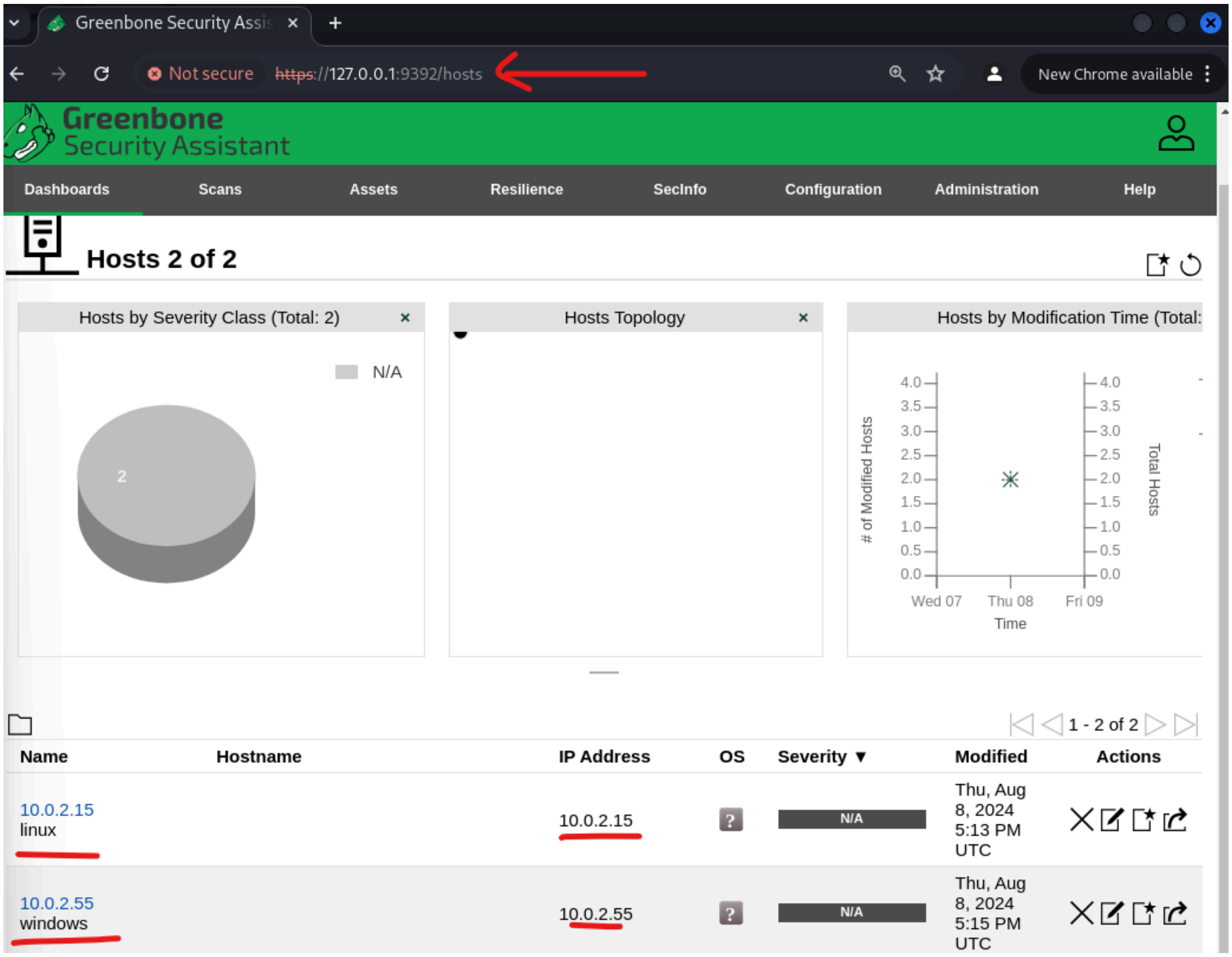
Insert the following info:

- Name: windows
- IP Address: 10.0.2.55
- Press save


New Host ×

IP Address	10.0.2.55
Comment	windows

In the hosts page you should see both hosts listed :



Hosts 2 of 2

Name	Hostname	IP Address	OS	Severity ▼	Modified	Actions
10.0.2.15 linux		10.0.2.15	?	N/A	Thu, Aug 8, 2024 5:13 PM UTC	
10.0.2.55 windows		10.0.2.55	?	N/A	Thu, Aug 8, 2024 5:15 PM UTC	

5. Add Targets

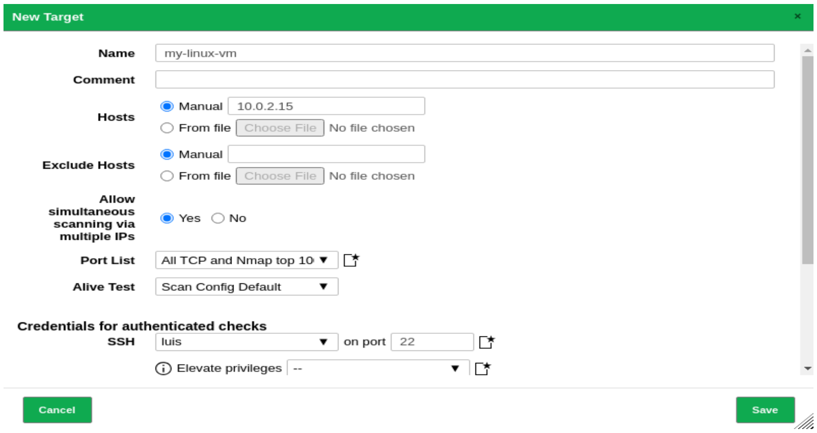
Navigate to the Configuration tab, Select Targets

<u>Add linux computer as target</u>

Click the Add New Target icon

Insert the following info:

- Name: my-linux-vm
- IP Address: 10.0.2.15
- Credentials for Authenticated Checks: SSH [luis]
- Port Lists: Nmap scan.
- Press save



Name: my-linux-vm

Comment:

Hosts: ● Manual 10.0.2.15 ○ From file Choose File No file chosen

Exclude Hosts: ● Manual ○ From file Choose File No file chosen

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All TCP and Nmap top 10 ▼

Alive Test: Scan Config Default ▼

Credentials for authenticated checks

SSH: luis ▼ on port 22

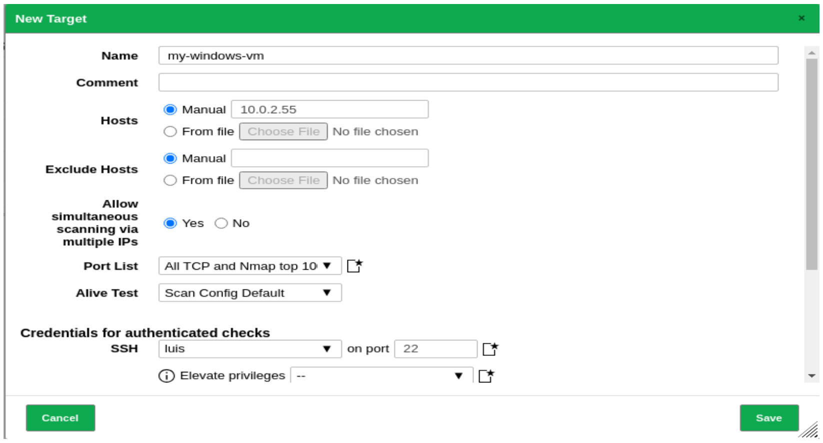
ⓘ Elevate privileges -- ▼

<u>Add windows computer as target.</u>

Click the Add New Target icon.

Insert the following info:

- Name: my-windows-vm
- IP Address: 10.0.2.55
- Credentials for Authenticated Checks: Select SSH [luis]
- Port Lists: Nmap scan
- Press save



Name: my-windows-vm

Comment:

Hosts: ● Manual 10.0.2.55 ○ From file Choose File No file chosen

Exclude Hosts: ● Manual ○ From file Choose File No file chosen

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All TCP and Nmap top 10 ▼

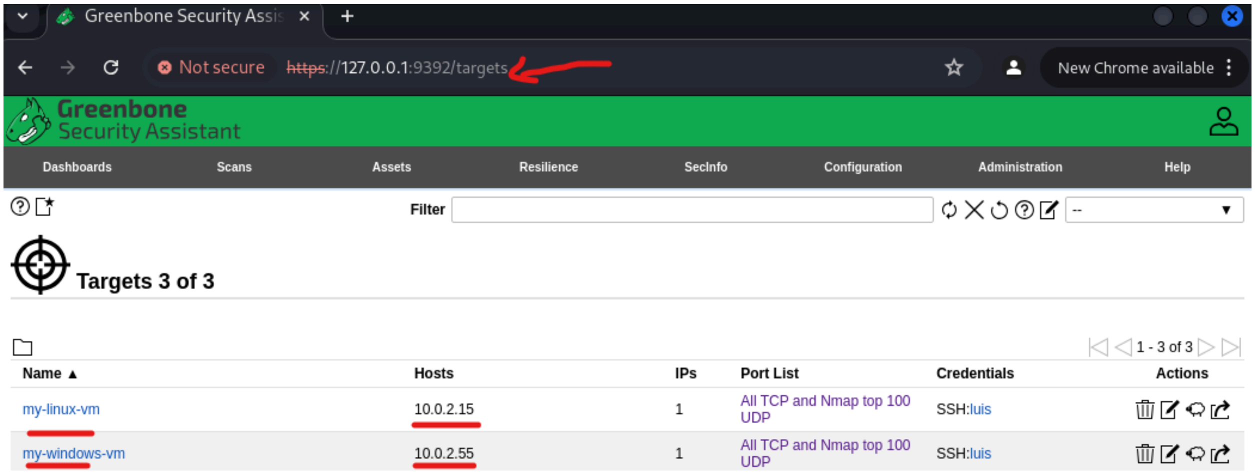
Alive Test: Scan Config Default ▼

Credentials for authenticated checks

SSH: luis ▼ on port 22

ⓘ Elevate privileges -- ▼

In the targets page you should see both targets listed:



https://127.0.0.1:9392/targets

Targets 3 of 3

Name ▲	Hosts	IPs	Port List	Credentials	Actions
my-linux-vm	10.0.2.15	1	All TCP and Nmap top 100 UDP	SSH:luis	
my-windows-vm	10.0.2.55	1	All TCP and Nmap top 100 UDP	SSH:luis	

6. Create Scanning tasks

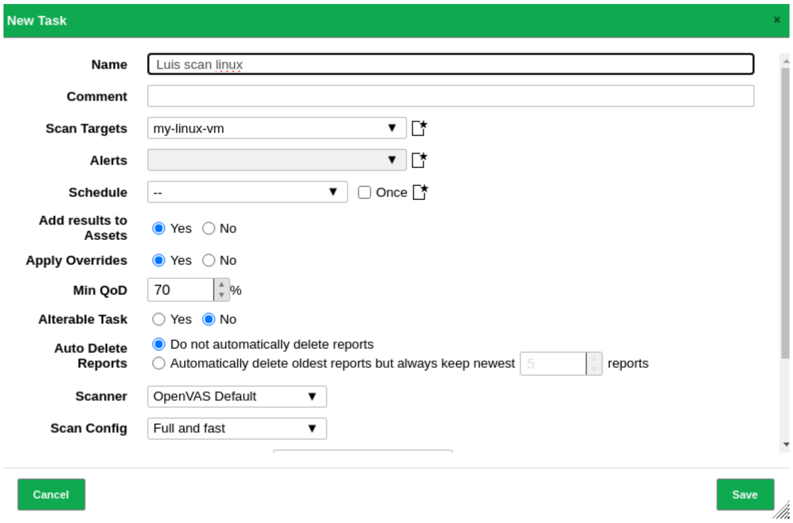
Go to the Scans tab

Create linux scan task

Select New Task

Insert the following info:

- Name: Luis scan linux
- Scan target: my-linux-vm
- Quality of Detection (QoD) : 70%
- Scan Config: Full and Fast



New Task

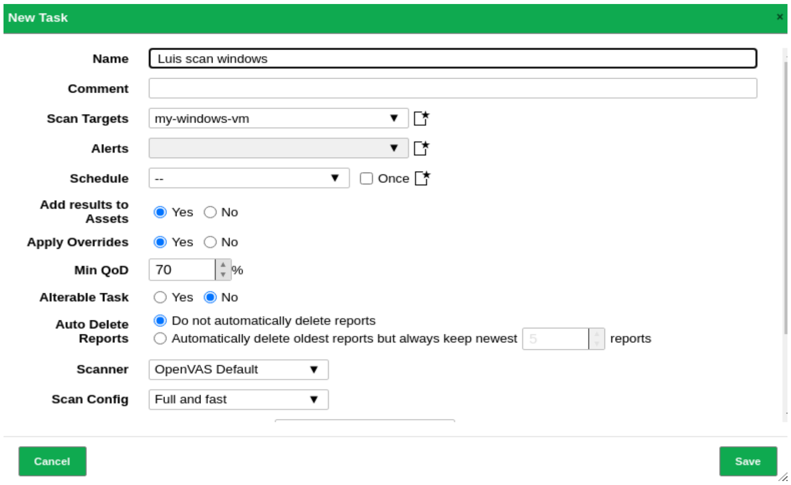
Name	Luis scan linux
Comment	
Scan Targets	my-linux-vm ▼
Alerts	▼
Schedule	-- ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼

Scan windows computer

Select New Task

Insert the following info:

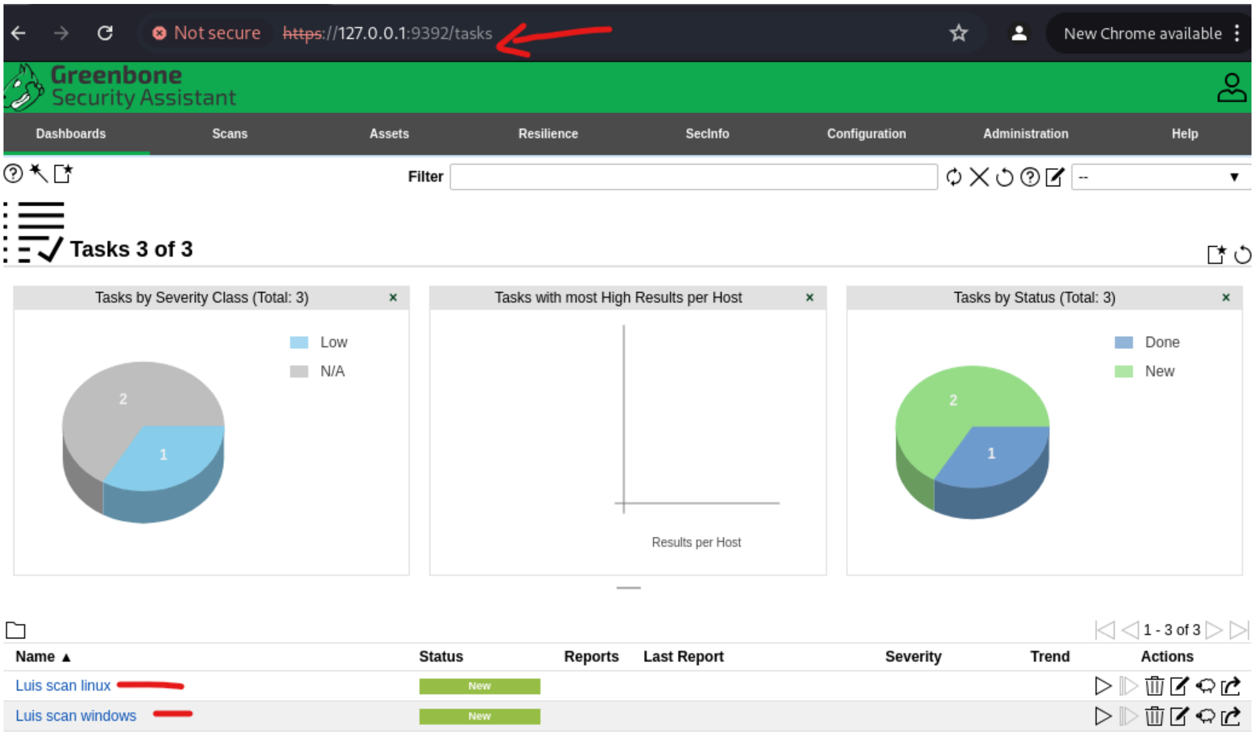
- Name: Luis scan windows
- Scan target: target my-windows-vm
- Quality of Detection (QoD) : 70%
- Scan Config: Full and Fast



New Task

Name	Luis scan windows
Comment	
Scan Targets	my-windows-vm
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

In the tasks page you should see :

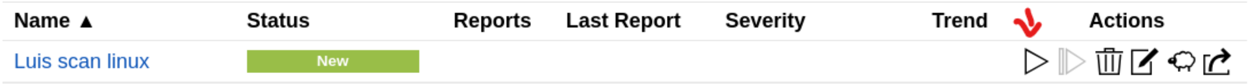


Tasks 3 of 3

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Luis scan linux	New					
Luis scan windows	New					

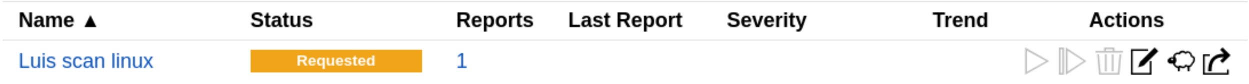
7. Execute scans

Turn on the linux machine
Press scan icon in open vas



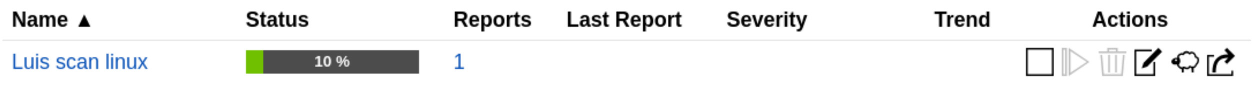
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Luis scan linux	New					▷

Scan will be requested



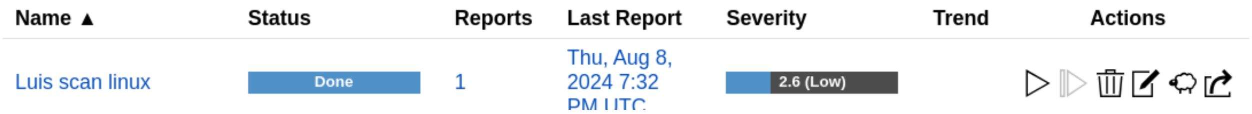
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Luis scan linux	Requested	1				

Scan will start



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Luis scan linux	10 %	1				□

Scan complete



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Luis scan linux	Done	1	Thu, Aug 8, 2024 7:32 PM UTC	2.6 (Low)		▷