Guide

Installing a Vulnerability Assessment Scanner (OpenVAS) on Kali Linux

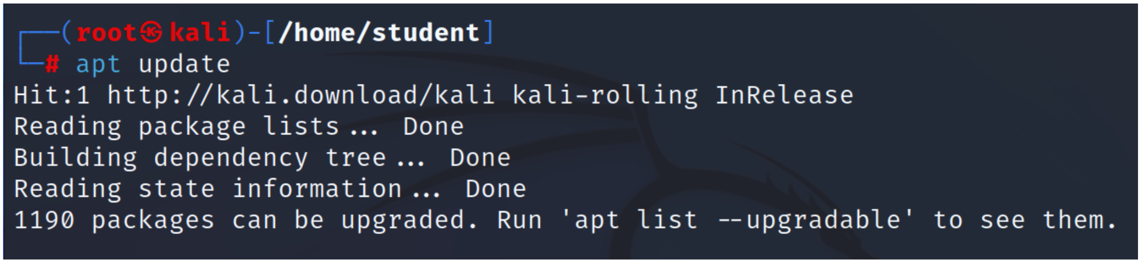
- Nuno Romão

Objective:

In this lab you'll be able to follow the step-by-step guide to install the Open Vulnerability Assessment Scanner, on a Kali Linux machine and use it as a Server to scan your organization for security vulnerabilities.

Star the process by updating and upgrading the system.

# apt update && apt upgrade

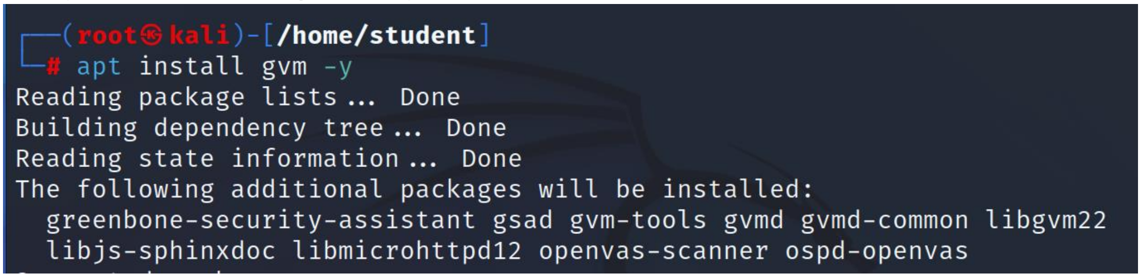


```
┌──(root㉿kali)-[/home/student]
└─# apt update
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1190 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Figure 1 - System updating

Install the OpenVAS application (Greenbone Vulnerability Management)

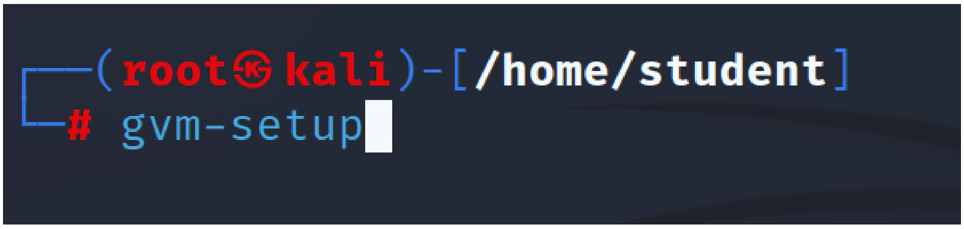
# apt install gvm -y



```
┌──(root㉿kali)-[/home/student]
└─# apt install gvm -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  greenbone-security-assistant gsad gvm-tools gvmd gvmd-common libgvm22
  libjs-sphinxdoc libmicrohttpd12 openvas-scanner ospd-openvas
```

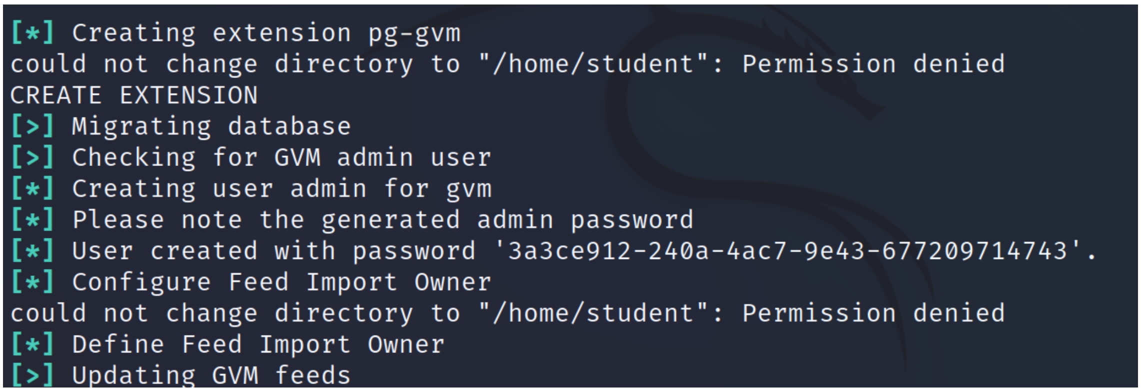
Figure 2 - Greenbone Vulnerability Management installation process

# gvm-setup



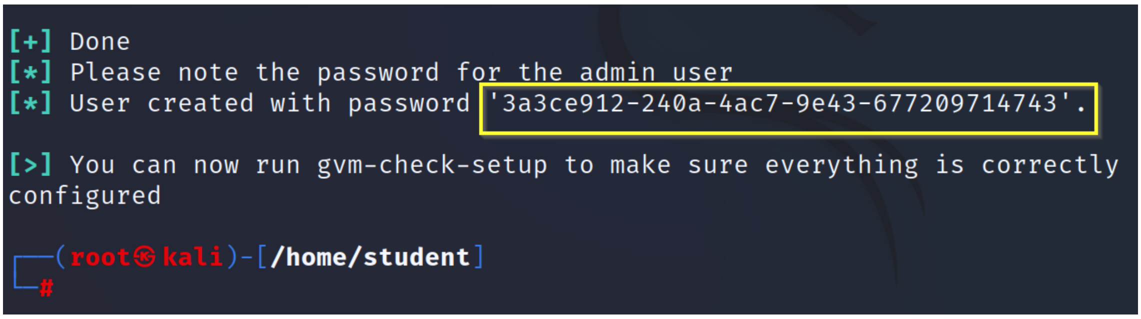
```
┌──(root㉿kali)-[/home/student]
└─# gvm-setup
```

Figure 3 - Run setup installation



```
[*] Creating extension pg-gvm
could not change directory to "/home/student": Permission denied
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '3a3ce912-240a-4ac7-9e43-677209714743'.
[*] Configure Feed Import Owner
could not change directory to "/home/student": Permission denied
[*] Define Feed Import Owner
[>] Updating GVM feeds
```

Figure 4 – Let the process run

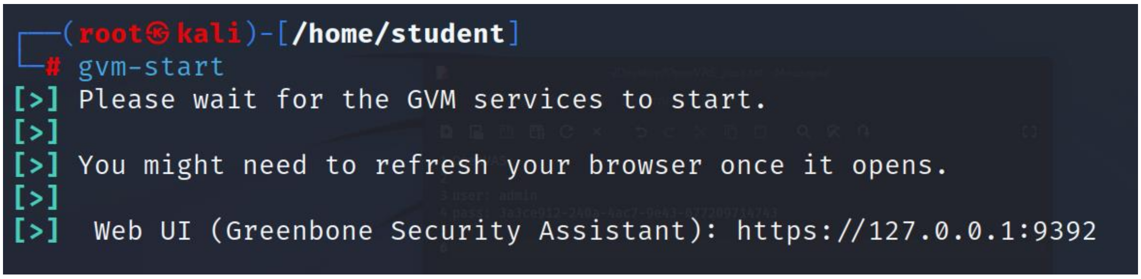


```
[+] Done
[*] Please note the password for the admin user
[*] User created with password '3a3ce912-240a-4ac7-9e43-677209714743'.

[>] You can now run gvm-check-setup to make sure everything is correctly
configured

┌──(root㉿kali)-[/home/student]
└─#
```

Figure 5 - Copy the generated admin password

Once the installation process finishes, start OpenVAS.

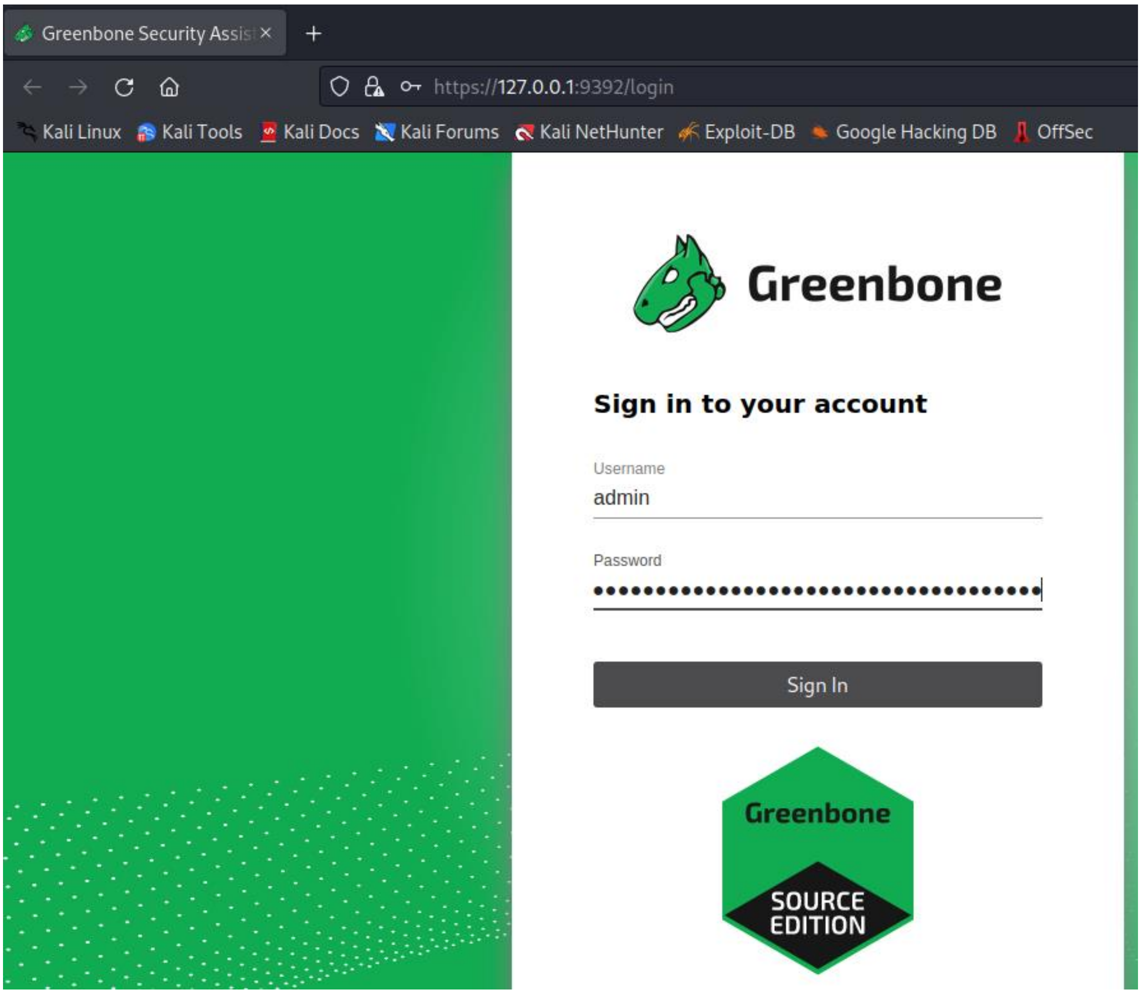
# gvm-start



```
┌──(root㉿kali)-[/home/student]
└─# gvm-start
[>] 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
```

Figure 6 - OpenVAS start installation process

Open the web browser and login with your credentials.



Greenbone Security Assis ×

https://127.0.0.1:9392/login

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Greenbone

Sign in to your account

Username
admin

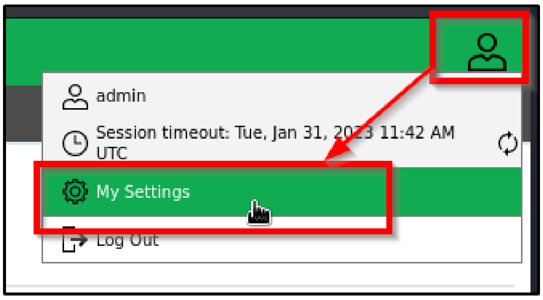
Password
•••••••••••••••••••••••••••••••••••

Sign In

Greenbone SOURCE EDITION

Figure 7 - OpenVAS login page

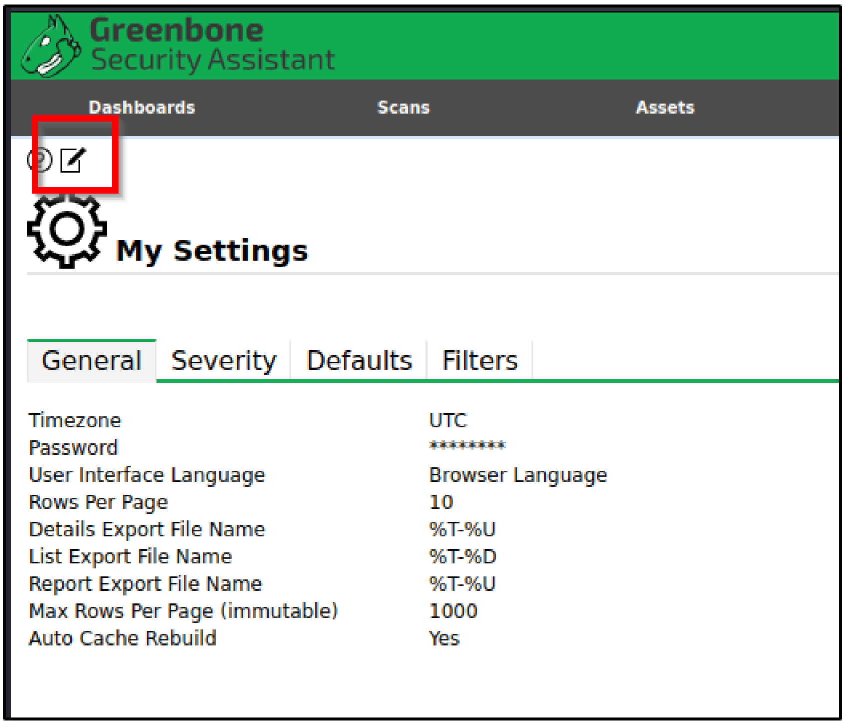
It is possible to change the default password to one of your liking.



admin

Session timeout: Tue, Jan 31, 2023 11:42 AM UTC

Figure 8 - OpenVAS settings

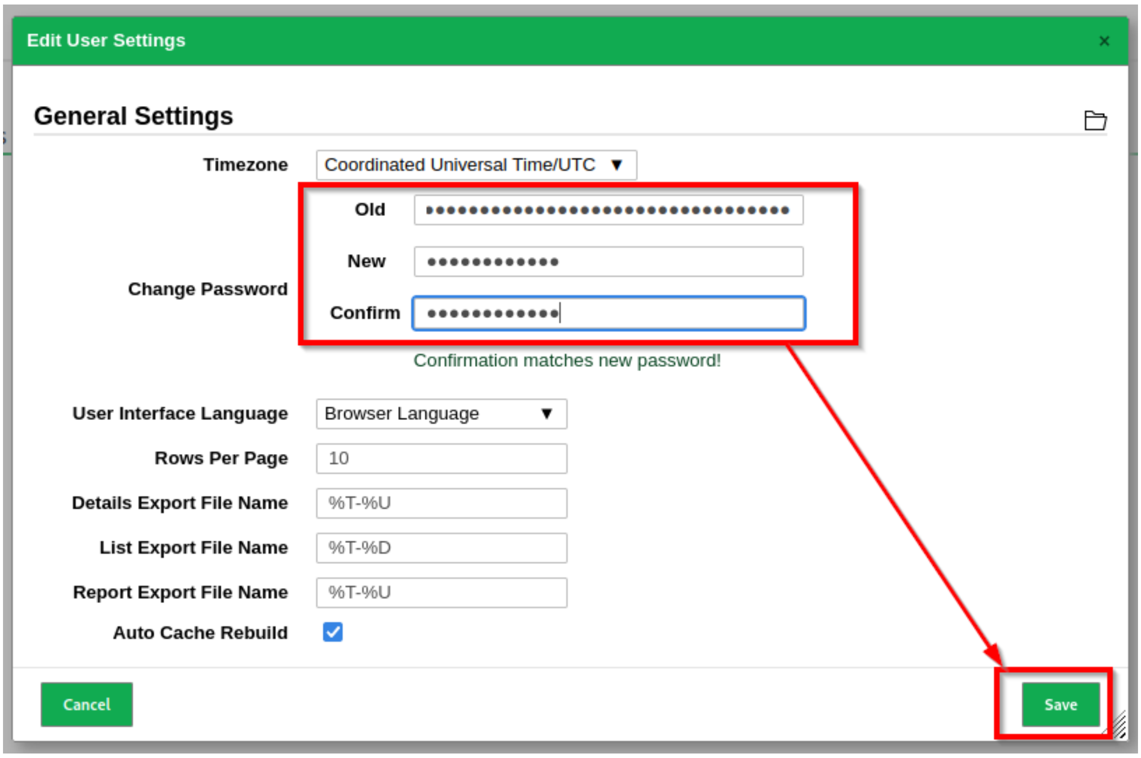


My Settings

General | Severity | Defaults | Filters

Timezone	UTC
Password	********
User Interface Language	Browser Language
Rows Per Page	10
Details Export File Name	%T-%U
List Export File Name	%T-%D
Report Export File Name	%T-%U
Max Rows Per Page (immutable)	1000
Auto Cache Rebuild	Yes

Figure 9 - Open settings to edit user password



General Settings

Timezone	Coordinated Universal Time/UTC ▼
Change Password	Old ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●● New ●●●●●●●●●●●●● Confirm ●●●●●●●●●●●●●
	Confirmation matches new password!
User Interface Language	Browser Language ▼
Rows Per Page	10
Details Export File Name	%T-%U
List Export File Name	%T-%D
Report Export File Name	%T-%U
Auto Cache Rebuild	☑

Figure 10 - Use the generated password and create a new one

You may need to wait a while, for the database to update. While the bottom right pie chart remains grayed out, it is not possible to use the scanner.
(it will take a long time for it to update, especially if you are using a virtual machine)

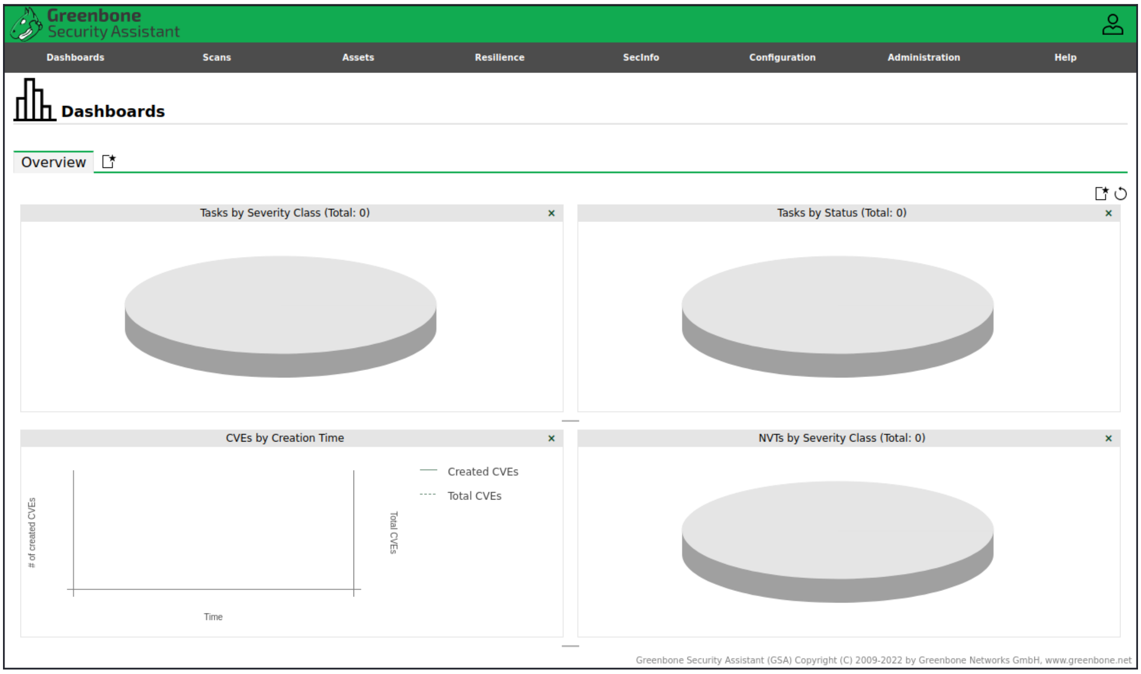

Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Dashboards
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
# of created CVEs
Total CVEs
Time
Created CVEs
Total CVEs
NVTs by Severity Class (Total: 0)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

Figure 11 - OpenVAS dashboard

You may check if the system is still updating its database, by going to administration and then feed status.

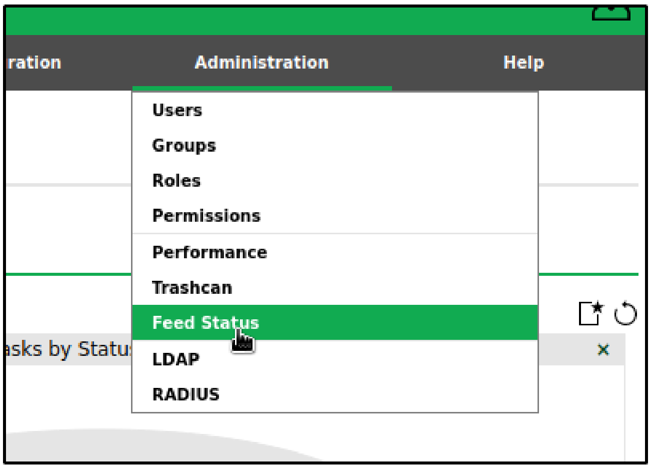
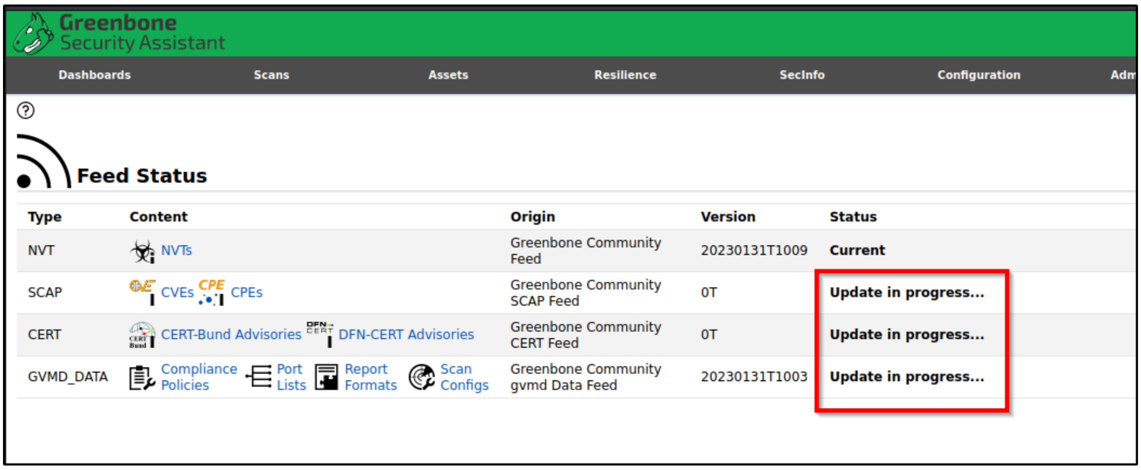


Figure 12 - OpenVAS feed status

[© Nuno Filipe Romão Pereira]



Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230131T1009	Current
SCAP	CVEs CPEs	Greenbone Community SCAP Feed	0T	Update in progress...
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	0T	Update in progress...
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20230131T1003	Update in progress...

Figure 13 - OpenVAS feed status

Wait until the update finishes.

When the update finishes, the dashboard will look like the following figure.

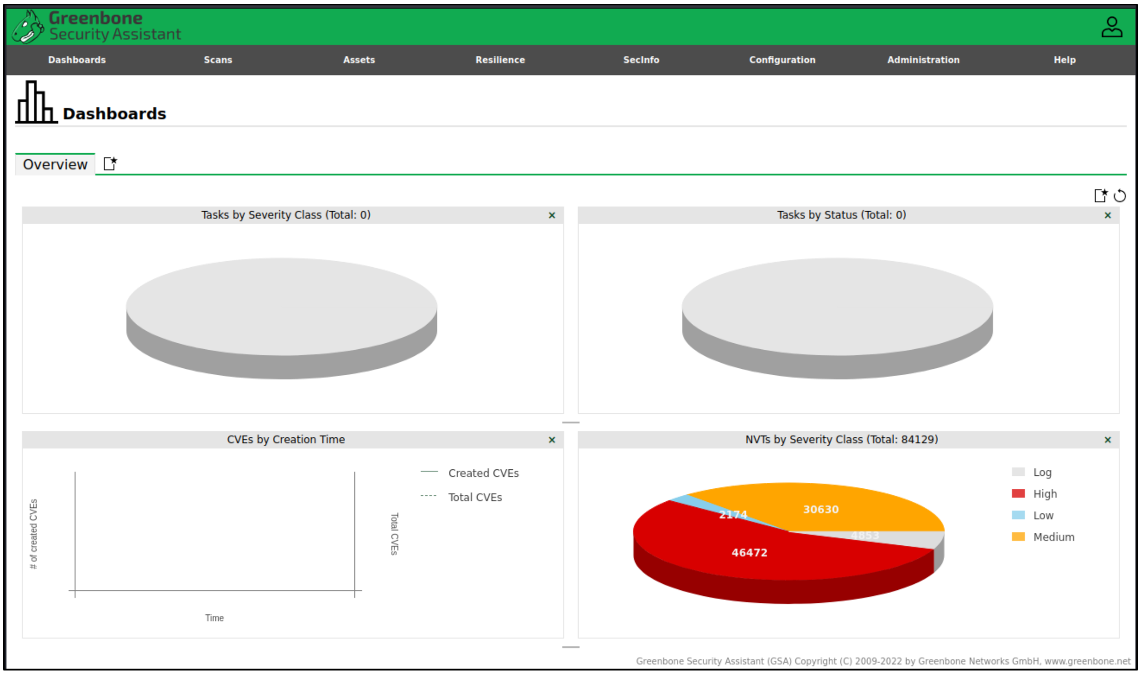


Figure 14 - Updated dashboard

You may add your targets to perform vulnerability scans later.

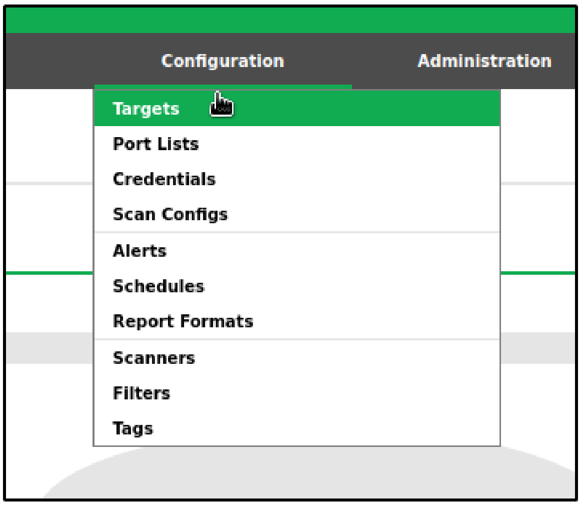
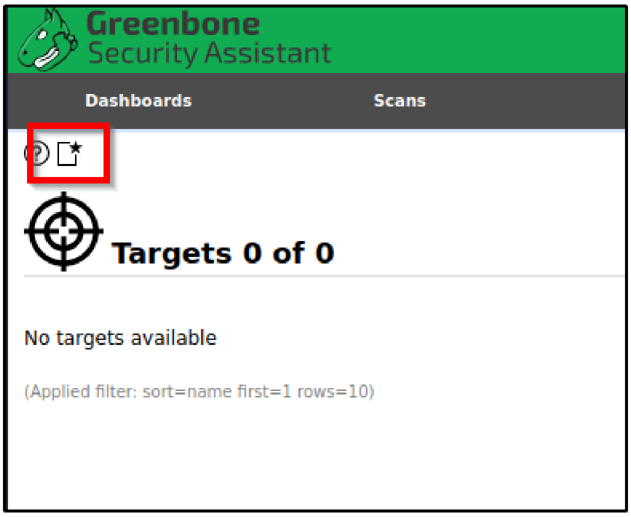


Figure 15 - Target menu

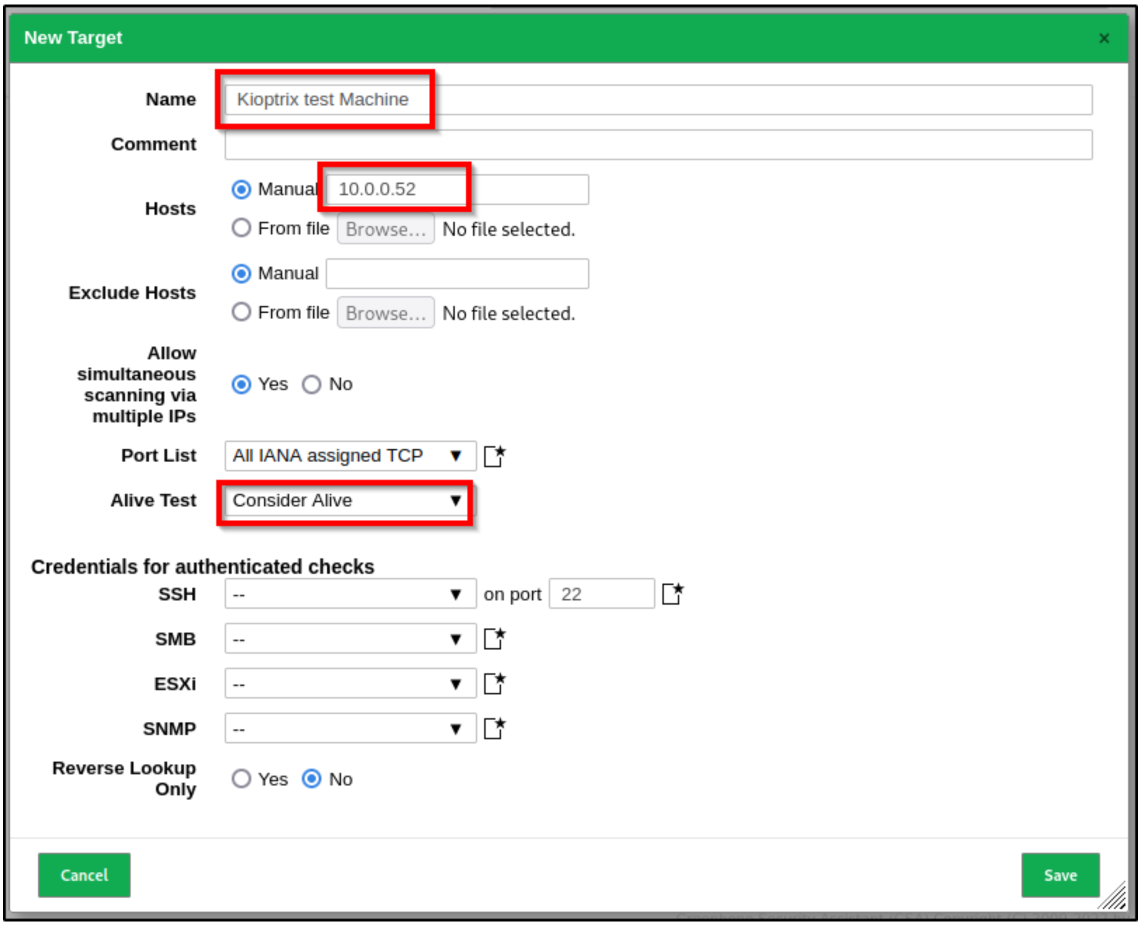


No targets available

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

Figure 16 - Add a new target

Add information regarding your targets.
Keep in mind that you can scan entire networks, but these can be very resource intensive, so it is recommended to scan one device at a time.



New Target

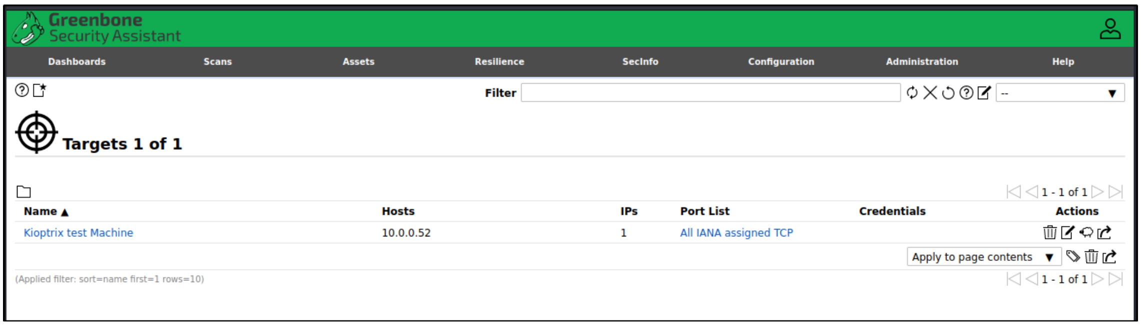
Name	Kioptrix test Machine
Comment	
Hosts	● Manual 10.0.0.52 ○ From file Browse… No file selected.
Exclude Hosts	● Manual ○ From file Browse… No file selected.
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All IANA assigned TCP
Alive Test	Consider Alive

Credentials for authenticated checks

SSH	-- on port 22
SMB	--
ESXi	--
SNMP	--
Reverse Lookup Only	○ Yes ● No

Figure 17 - Configure all settings regarding the machine you want to scan

After saving, you'll be able to setup a scan using your target.



Targets 1 of 1

1 - 1 of 1

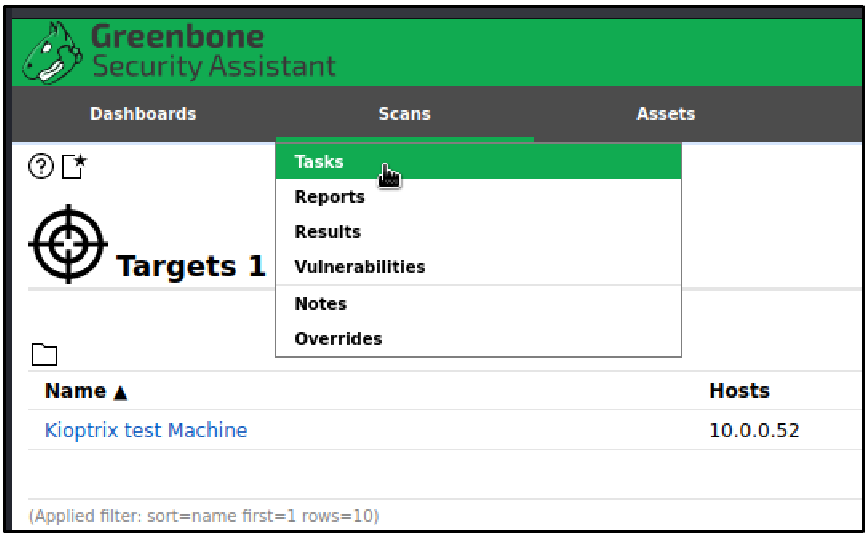
Name ▲	Hosts	IPs	Port List	Credentials	Actions
Kioptrix test Machine	10.0.0.52	1	All IANA assigned TCP		

Apply to page contents

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

1 - 1 of 1

Figure 18 - Target list



Targets 1

Name ▲	Hosts
Kioptrix test Machine	10.0.0.52

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

Figure 19 - Setup vulnerability scan

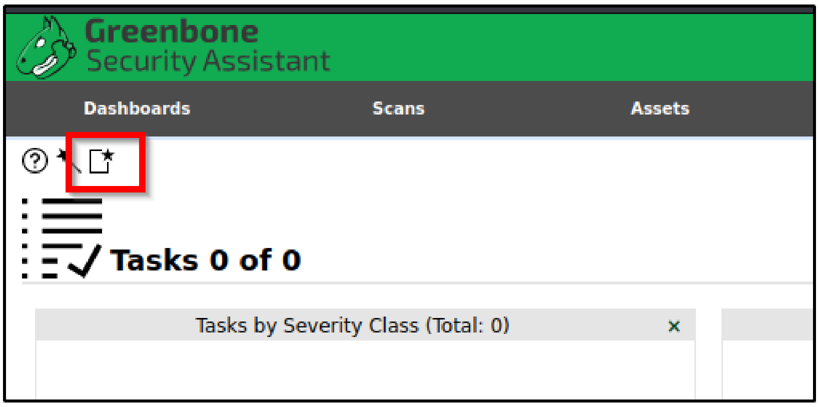


Figure 20 - Setup new vulnerability scan

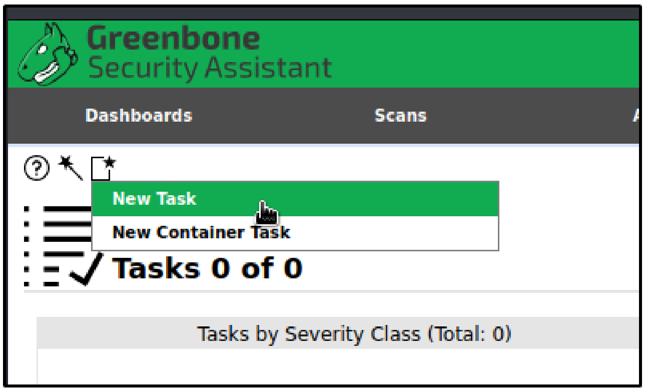
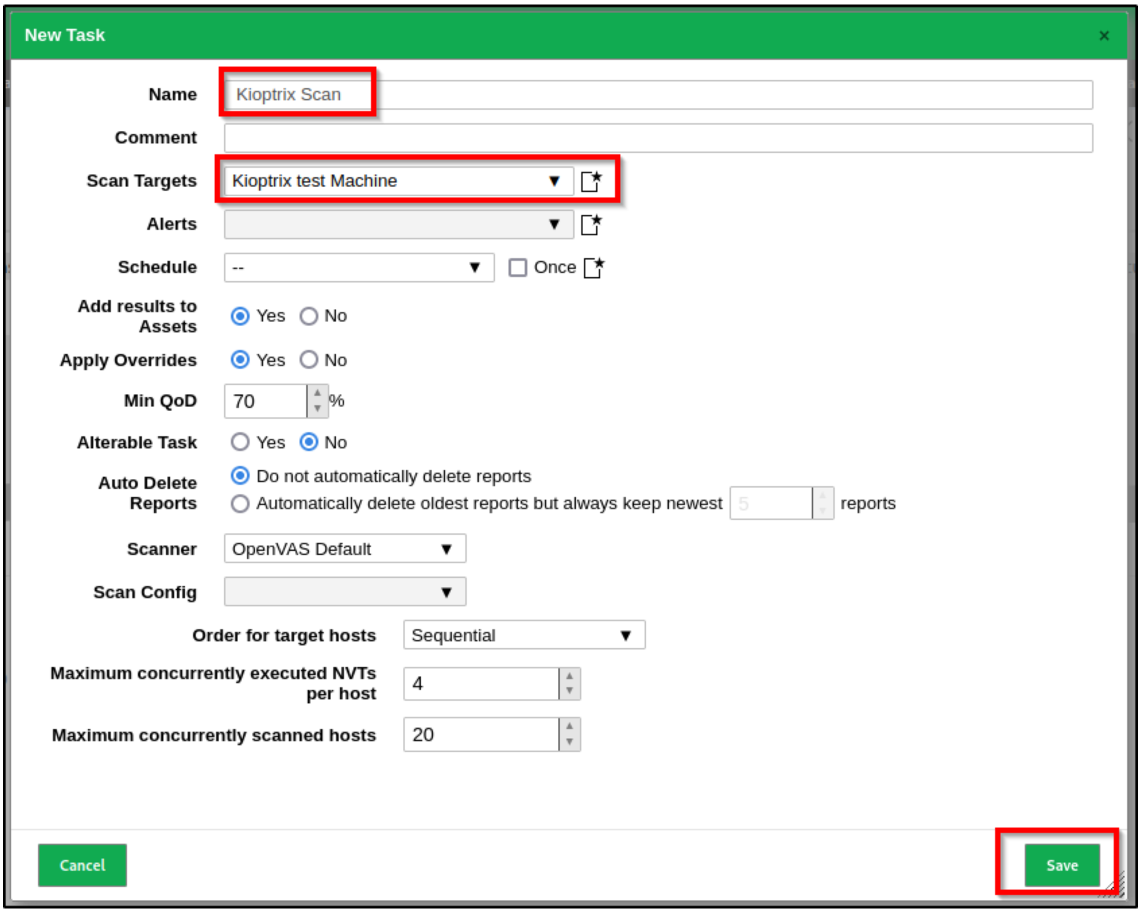


Figure 21 - Add a new task



New Task

Name: Kioptrix Scan

Comment:

Scan Targets: Kioptrix test Machine

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:

Order for target hosts: Sequential

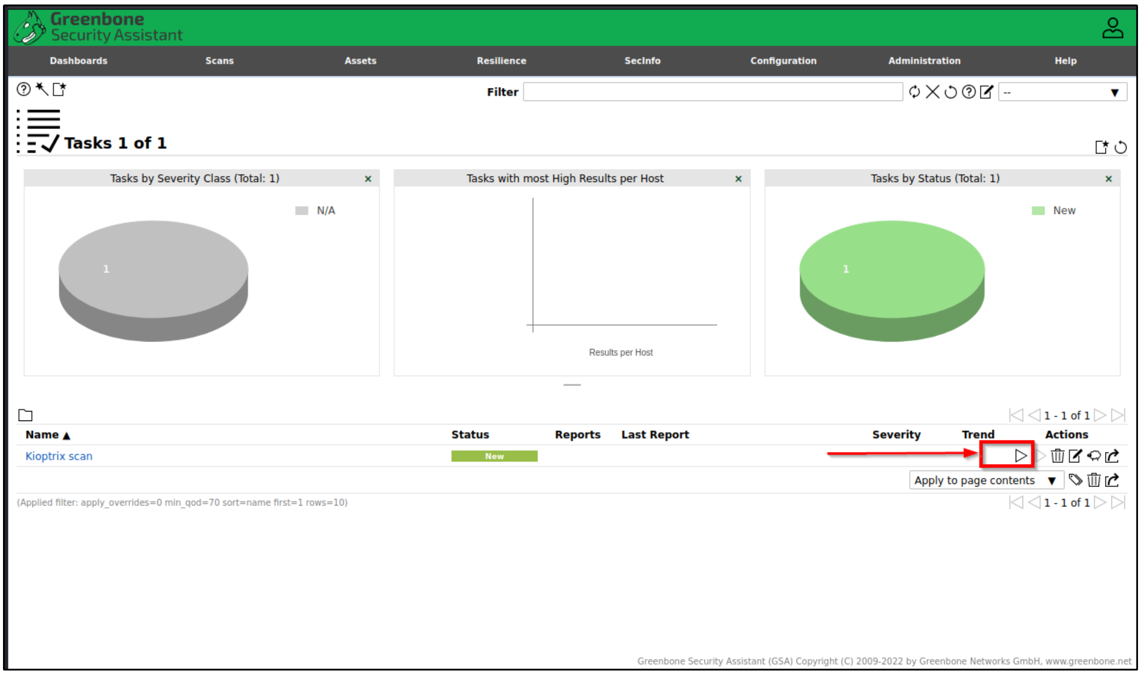
Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Figure 22 - Setup target scan configuration

Save the scan configuration.

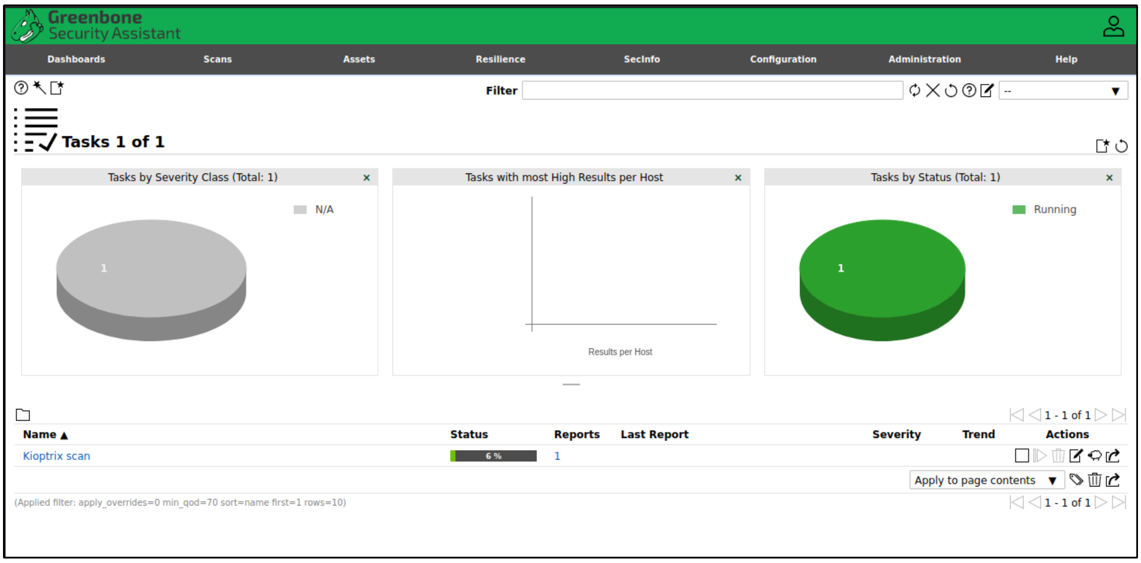
To start the scan process, please press "play" and wait for the scan to finish.


Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
--
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
New
1
1 - 1 of 1
Apply to page contents
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Kioptrix scan	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 23 - Start the scan process

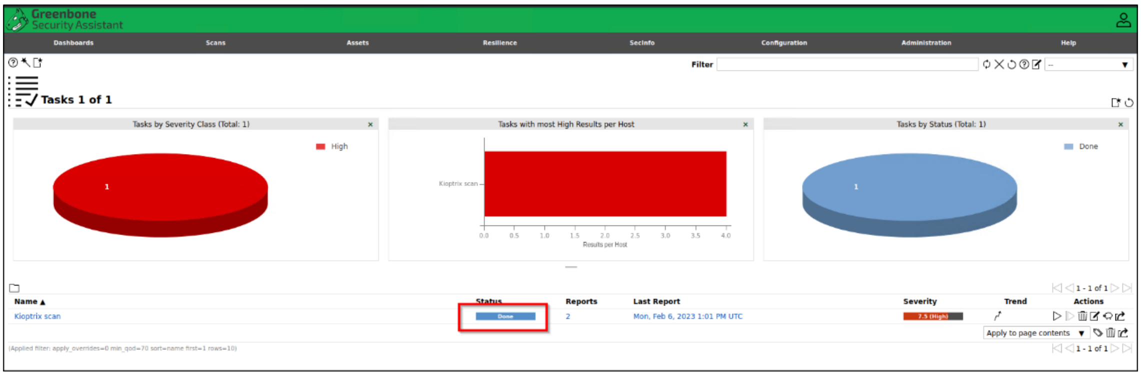


Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Kioptrix scan	6 %	1				

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 24 - Scan running

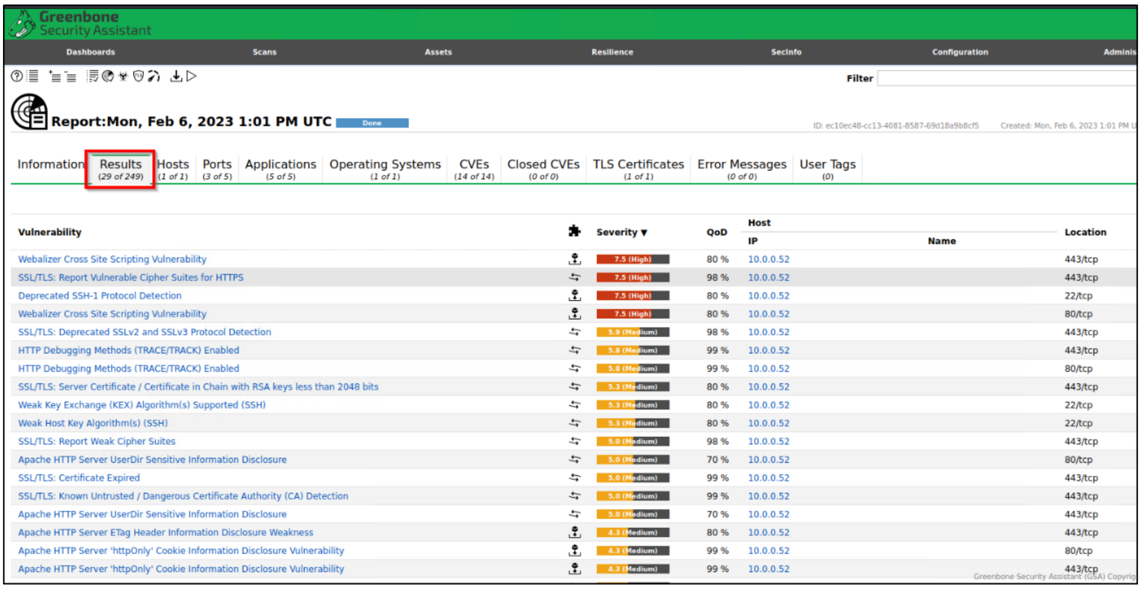
Once the scan finishes, you may check the vulnerabilities.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Kioptrix scan	Done	2	Mon, Feb 6, 2023 1:01 PM UTC	7.5 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 25 - Click on "Done"



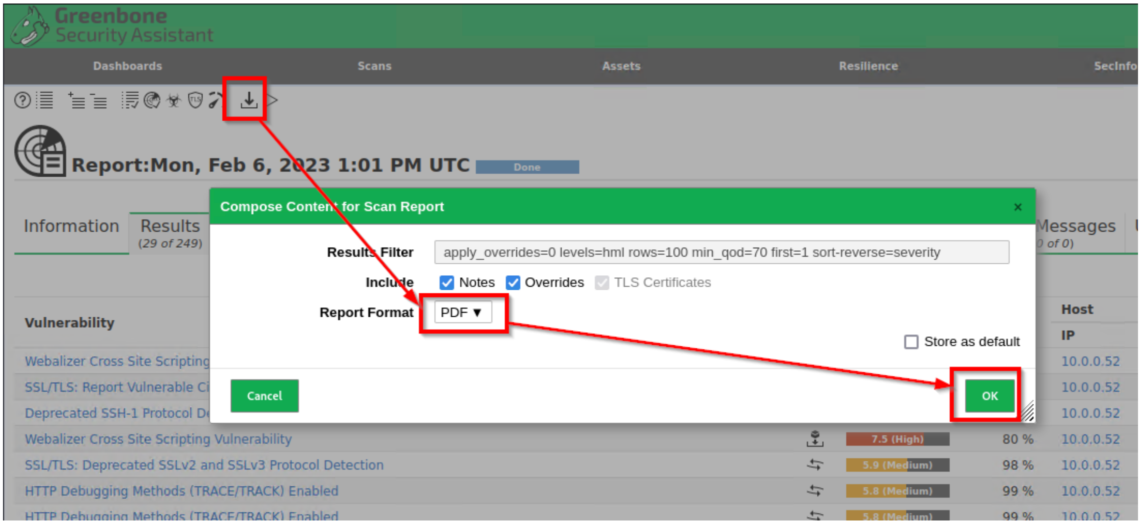
Report:Mon, Feb 6, 2023 1:01 PM UTC Done

ID: ec10ec48-cc13-4081-8587-69d18a9b8cf5 Created: Mon, Feb 6, 2023 1:01 PM U

Vulnerability		Severity ▼	QoD	Host		Location
				IP	Name	
Webalizer Cross Site Scripting Vulnerability		7.5 (High)	80 %	10.0.0.52		443/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		7.5 (High)	98 %	10.0.0.52		443/tcp
Deprecated SSH-1 Protocol Detection		7.5 (High)	80 %	10.0.0.52		22/tcp
Webalizer Cross Site Scripting Vulnerability		7.5 (High)	80 %	10.0.0.52		80/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		5.9 (Medium)	98 %	10.0.0.52		443/tcp
HTTP Debugging Methods (TRACE/TRACK) Enabled		5.8 (Medium)	99 %	10.0.0.52		443/tcp
HTTP Debugging Methods (TRACE/TRACK) Enabled		5.8 (Medium)	99 %	10.0.0.52		80/tcp
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits		5.3 (Medium)	80 %	10.0.0.52		443/tcp
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)		5.3 (Medium)	80 %	10.0.0.52		22/tcp
Weak Host Key Algorithm(s) (SSH)		5.3 (Medium)	80 %	10.0.0.52		22/tcp
SSL/TLS: Report Weak Cipher Suites		5.0 (Medium)	98 %	10.0.0.52		443/tcp
Apache HTTP Server UserDir Sensitive Information Disclosure		5.0 (Medium)	70 %	10.0.0.52		80/tcp
SSL/TLS: Certificate Expired		5.0 (Medium)	99 %	10.0.0.52		443/tcp
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection		5.0 (Medium)	99 %	10.0.0.52		443/tcp
Apache HTTP Server UserDir Sensitive Information Disclosure		5.0 (Medium)	70 %	10.0.0.52		443/tcp
Apache HTTP Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80 %	10.0.0.52		443/tcp
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99 %	10.0.0.52		80/tcp
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99 %	10.0.0.52		443/tcp

Figure 26 - It will be possible to validate your findings

It is possible to export a report:



Report:Mon, Feb 6, 2023 1:01 PM UTC Done

Compose Content for Scan Report

Results Filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity

Include: ☑ Notes ☑ Overrides ☑ TLS Certificates

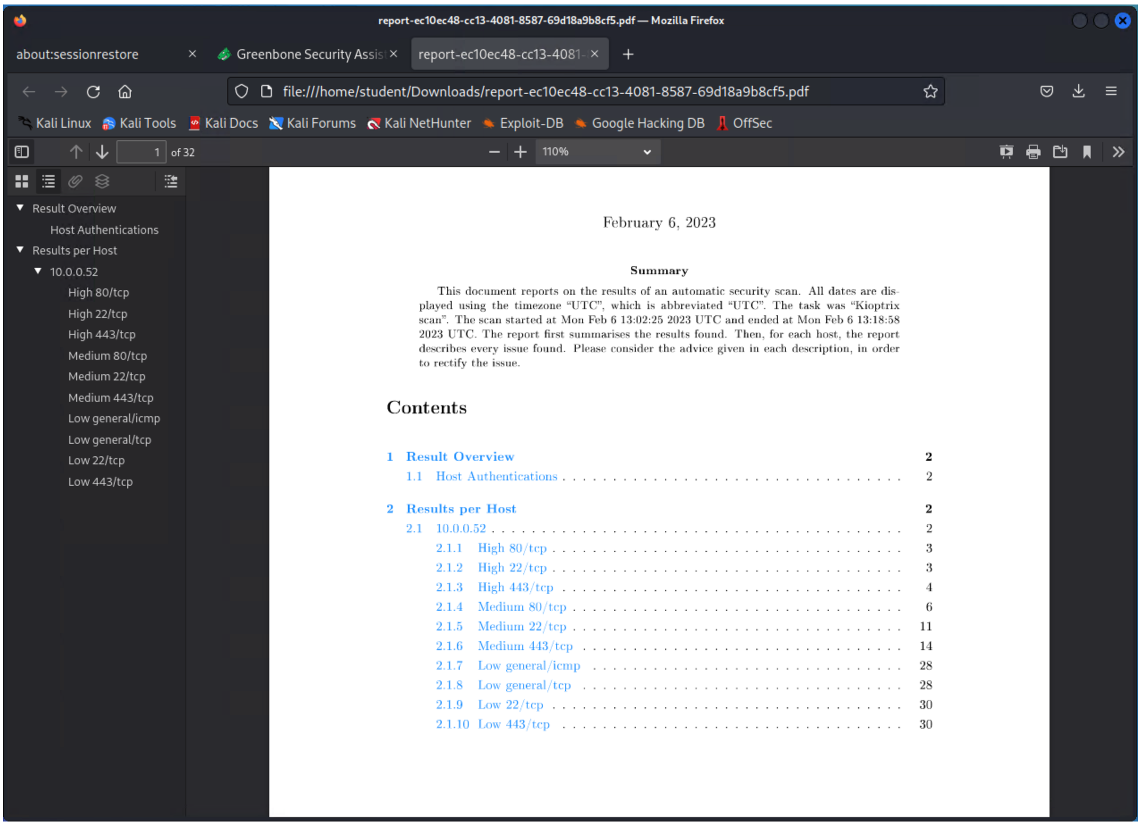
Report Format: PDF ▼

□ Store as default

Vulnerability	Severity	QoD	IP
Webalizer Cross Site Scripting Vulnerability	7.5 (High)	80 %	10.0.0.52
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	10.0.0.52
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	10.0.0.52
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	10.0.0.52

Figure 27 - Vulnerability Report export options

[© Nuno Filipe Romão Pereira]



February 6, 2023

Summary

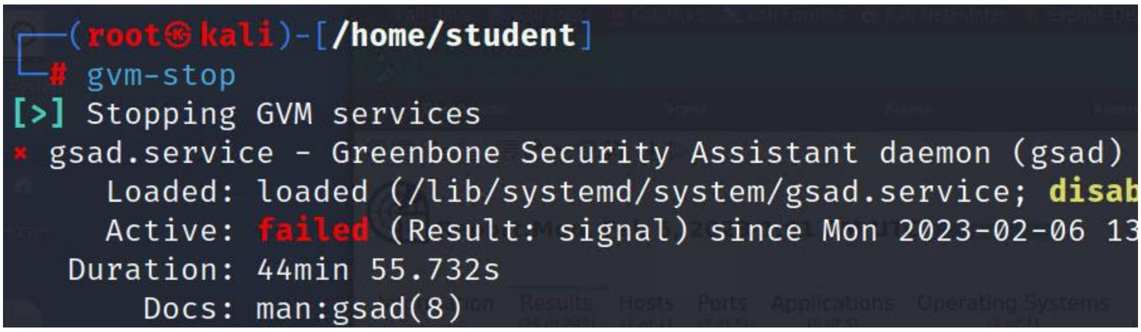
This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Kioptrix scan". The scan started at Mon Feb 6 13:02:25 2023 UTC and ended at Mon Feb 6 13:18:58 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Figure 28 - Vulnerability Report PDF file

If you want to allow access to OpenVAS's web application from any computer, you can change the service parameters.
With OpenVAS turned off, edit the greenbone-security-assistant.service.

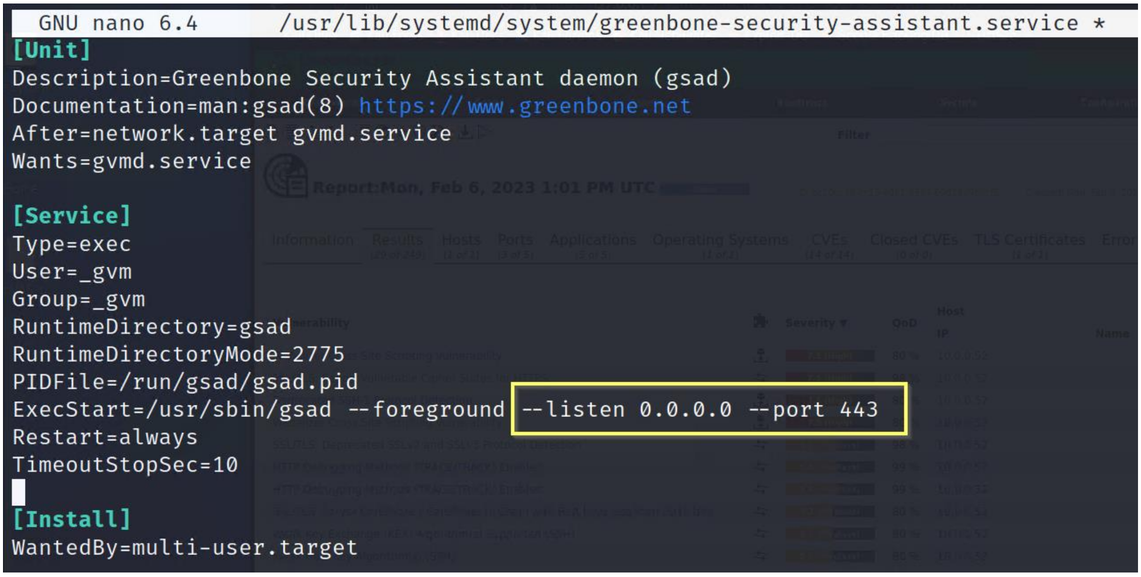
```
# gvm-stop
# nano   /usr/lib/systemd/system/greenbone-security-assistant.service
```



```
┌──(root㉿kali)-[/home/student]
└─# gvm-stop
[>] Stopping GVM services
× gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/lib/systemd/system/gsad.service; disab
     Active: failed (Result: signal) since Mon 2023-02-06 13
   Duration: 44min 55.732s
       Docs: man:gsad(8)
```

Figure 29 - Stop GVM service

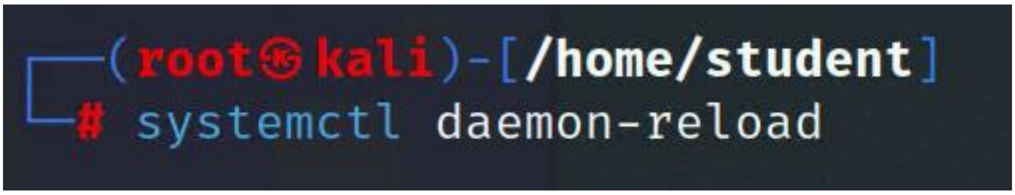
Edit the file and change the IP address to 0.0.0.0, and change the port to 443.



```
  GNU nano 6.4        /usr/lib/systemd/system/greenbone-security-assistant.service *
[Unit]
Description=Greenbone Security Assistant daemon (gsad)
Documentation=man:gsad(8) https://www.greenbone.net
After=network.target gvmd.service
Wants=gvmd.service

[Service]
Type=exec
User=_gvm
Group=_gvm
RuntimeDirectory=gsad
RuntimeDirectoryMode=2775
PIDFile=/run/gsad/gsad.pid
ExecStart=/usr/sbin/gsad --foreground --listen 0.0.0.0 --port 443
Restart=always
TimeoutStopSec=10

[Install]
WantedBy=multi-user.target
```

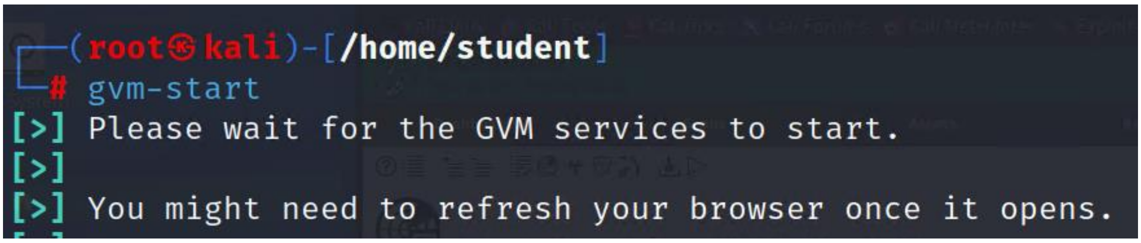
Figure 30 - GVM service configuration

Save the file, quit, reload the daemon services and start OpenVAS again.
When connecting to Kali Linux using port 443, you'll have access to OpenVAS web application.



```
┌──(root㉿kali)-[/home/student]
└─# systemctl daemon-reload
```

Figure 31 - Reload services



```
┌──(root㉿kali)-[/home/student]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
```

Figure 32 - Start GVM again

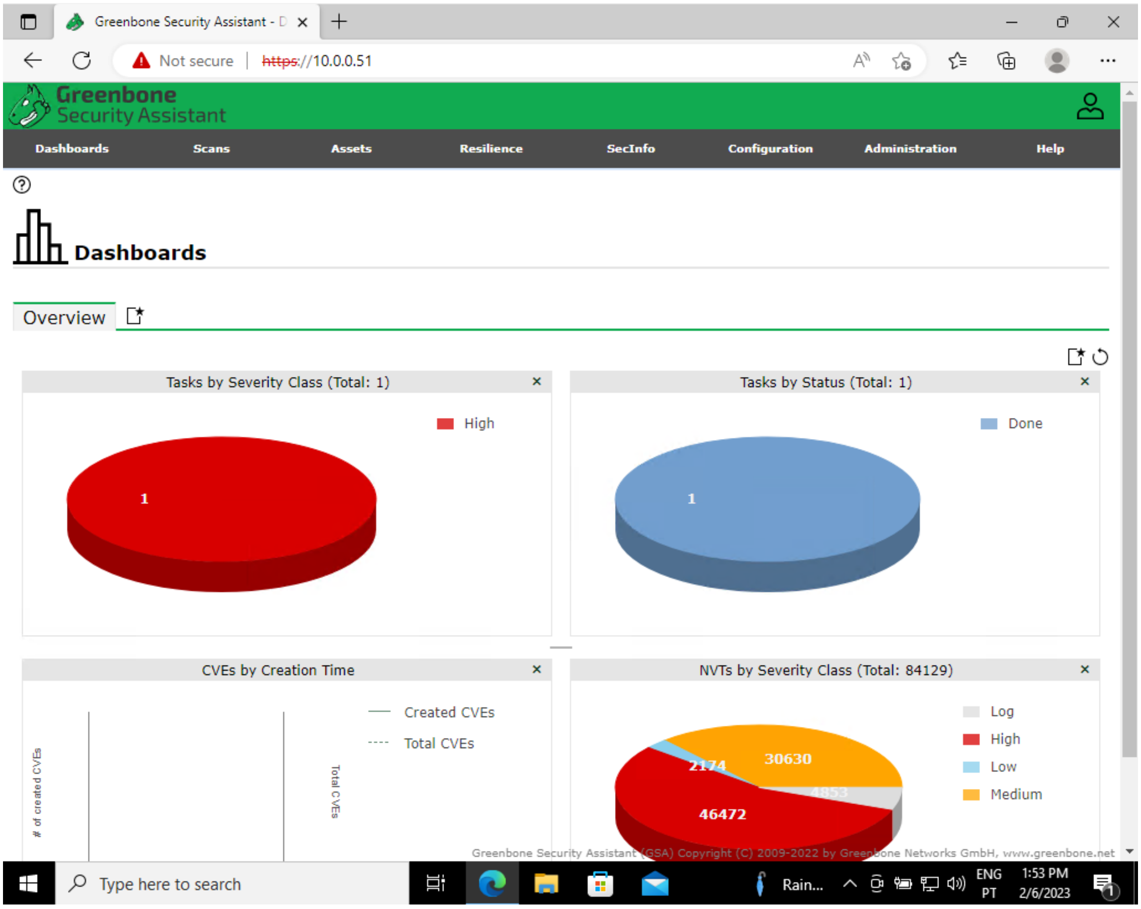


Figure 33 - Connect to OpenVAS using another machine on the network