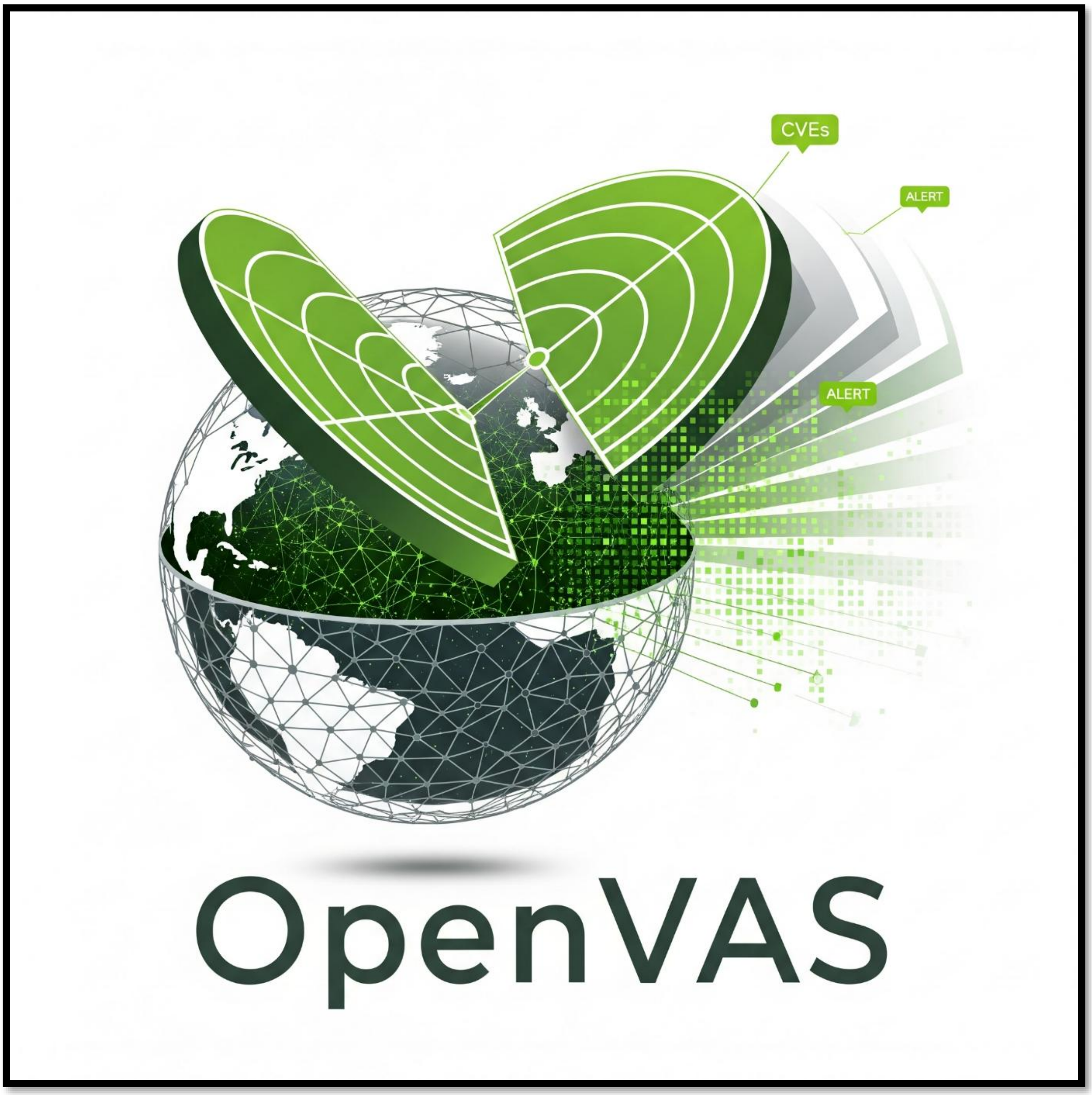
Day 11 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: OpenVAS



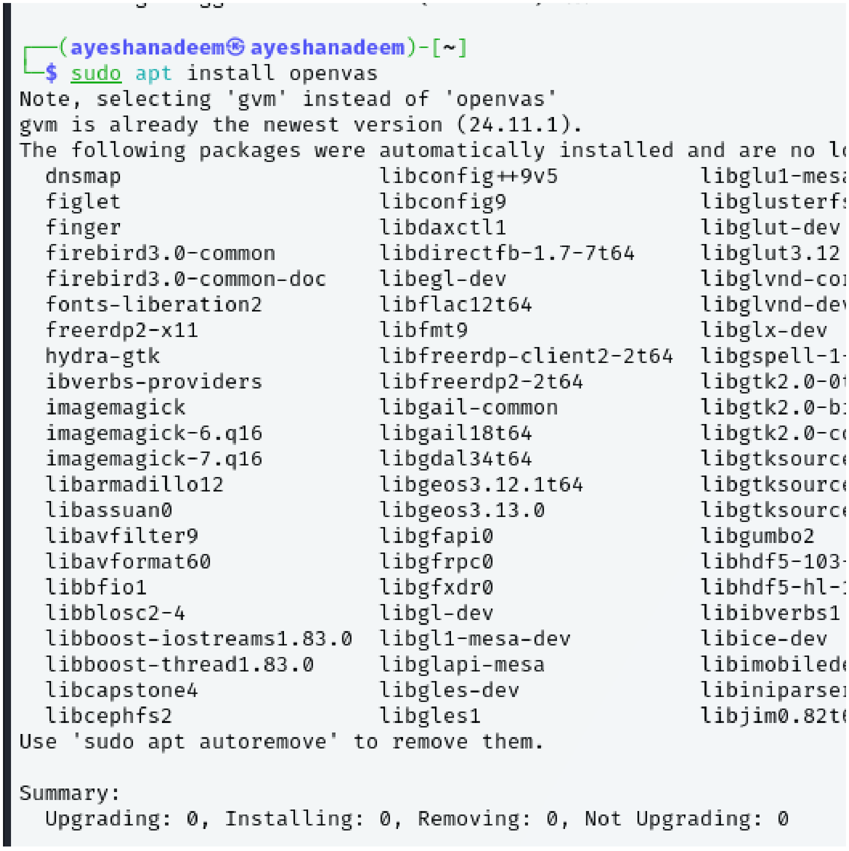
Contact Me: ayeshanm8@gmail.com

Date: 11th July, 2025

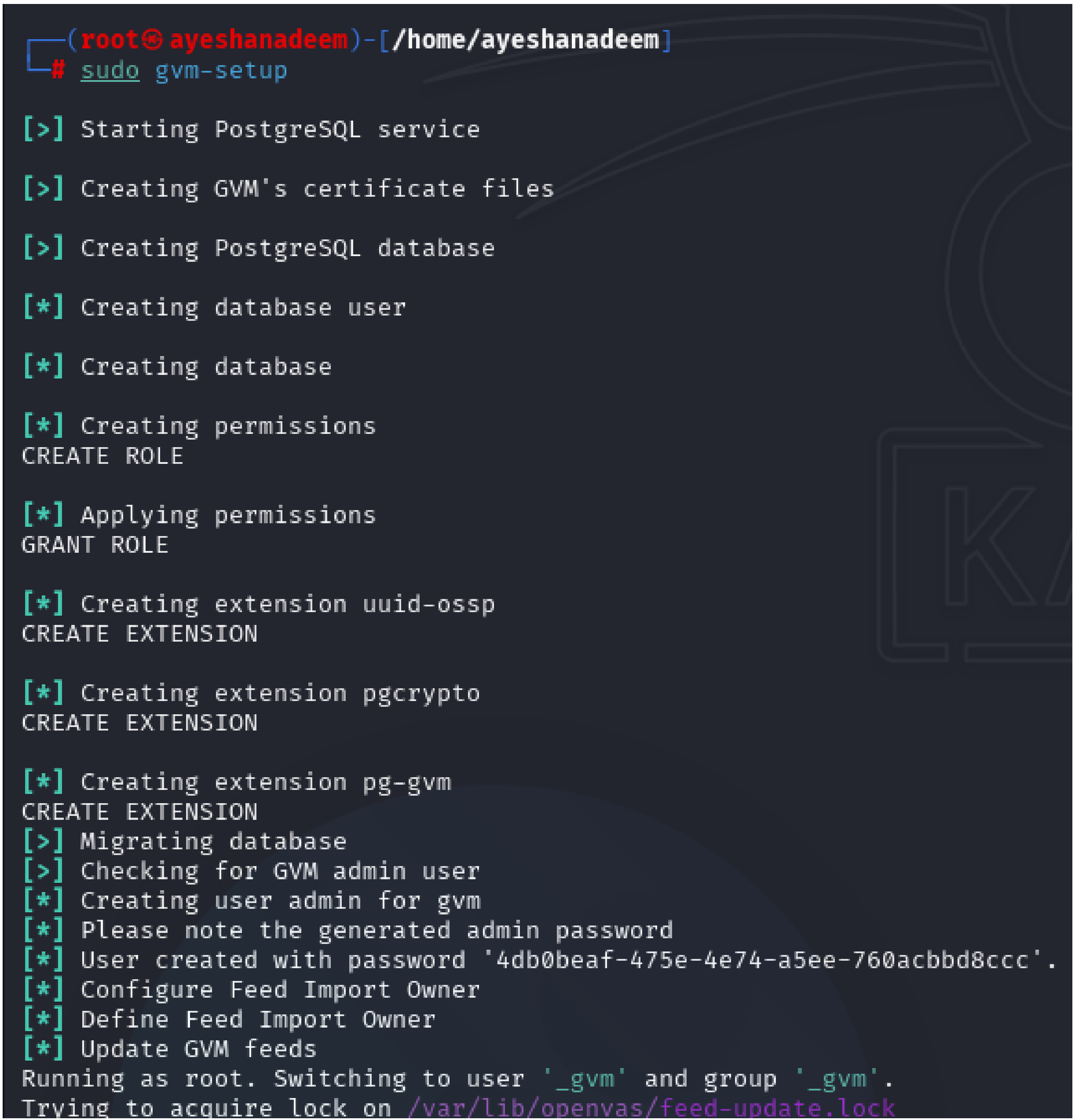
OpenVAS: Open Source Vulnerability Scanner

Task 1:

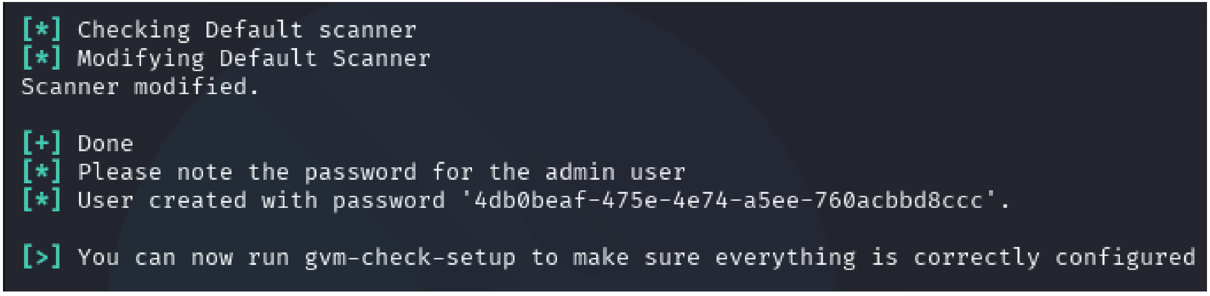
Install & Setup OpenVAS:



```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ sudo apt install openvas
Note, selecting 'gvm' instead of 'openvas'
gvm is already the newest version (24.11.1).
The following packages were automatically installed and are no l
  dnsmap                      libconfig++9v5            libglu1-mes
  figlet                      libconfig9                libglusterf
  finger                      libdaxctl1                libglut-dev
  firebird3.0-common          libdirectfb-1.7-7t64      libglut3.12
  firebird3.0-common-doc      libegl-dev                libglvnd-co
  fonts-liberation2           libflac12t64              libglvnd-de
  freerdp2-x11                libfmt9                   libglx-dev
  hydra-gtk                   libfreerdp-client2-2t64   libgspell-1-
  ibverbs-providers           libfreerdp2-2t64          libgtk2.0-0
  imagemagick                 libgail-common            libgtk2.0-b
  imagemagick-6.q16           libgail18t64              libgtk2.0-c
  imagemagick-7.q16           libgdal34t64              libgtksourc
  libarmadillo12              libgeos3.12.1t64          libgtksourc
  libassuan0                  libgeos3.13.0             libgtksourc
  libavfilter9                libgfapi0                 libgumbo2
  libavformat60               libgfrpc0                 libhdf5-103-
  libbfio1                    libgfxdr0                 libhdf5-hl-
  libblosc2-4                 libgl-dev                 libibverbs1
  libboost-iostreams1.83.0    libgl1-mesa-dev           libice-dev
  libboost-thread1.83.0       libglapi-mesa             libimobiled
  libcapstone4                libgles-dev               libiniparse
  libcephfs2                  libgles1                  libjim0.82t
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```



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

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database

[*] Creating database user

[*] Creating database

[*] Creating permissions
CREATE ROLE

[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION

[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '4db0beaf-475e-4e74-a5ee-760acbbd8ccc'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
```

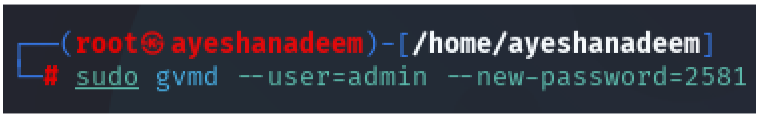


```
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '4db0beaf-475e-4e74-a5ee-760acbbd8ccc'.

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

Task 2

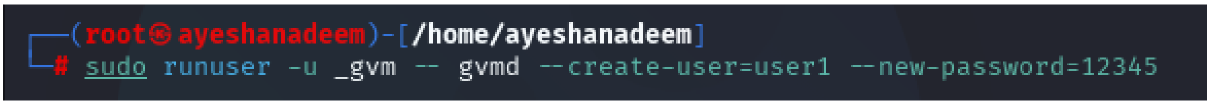
Configure & Start GVM

Creating Admin & setting Password:



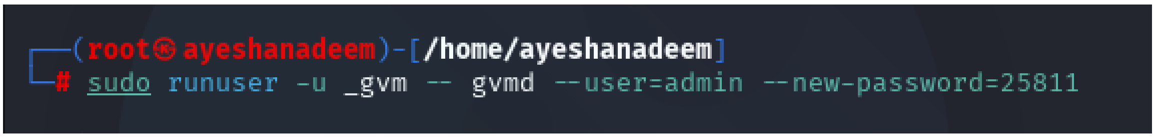
```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# sudo gvmd --user=admin --new-password=2581
```

To create a new user:



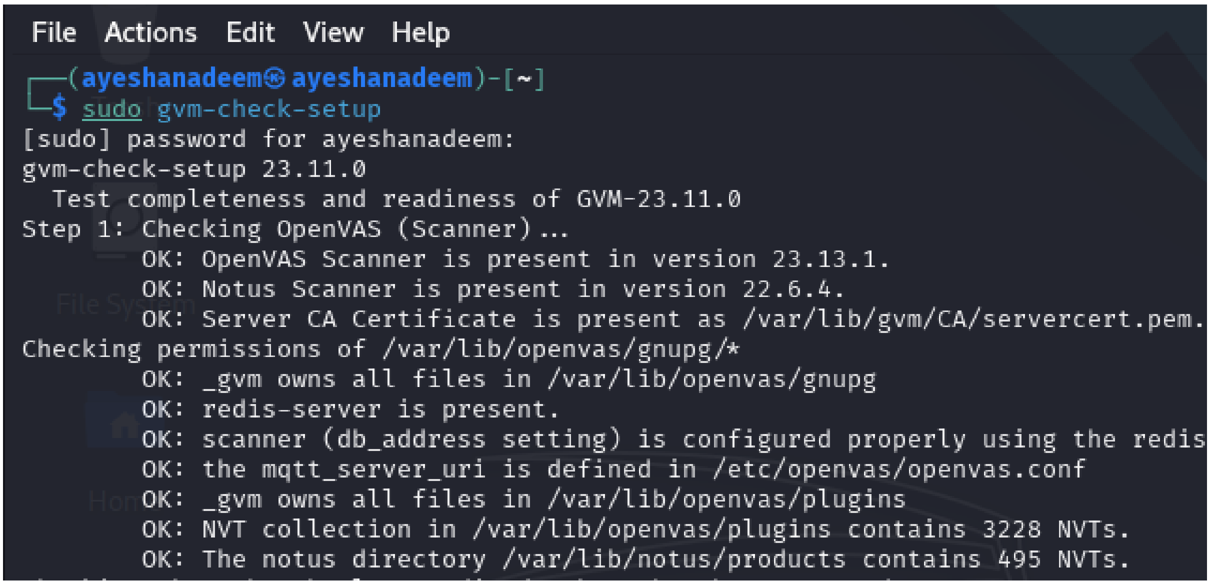
```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# sudo runuser -u _gvm -- gvmd --create-user=user1 --new-password=12345
```

Admin Password Change:

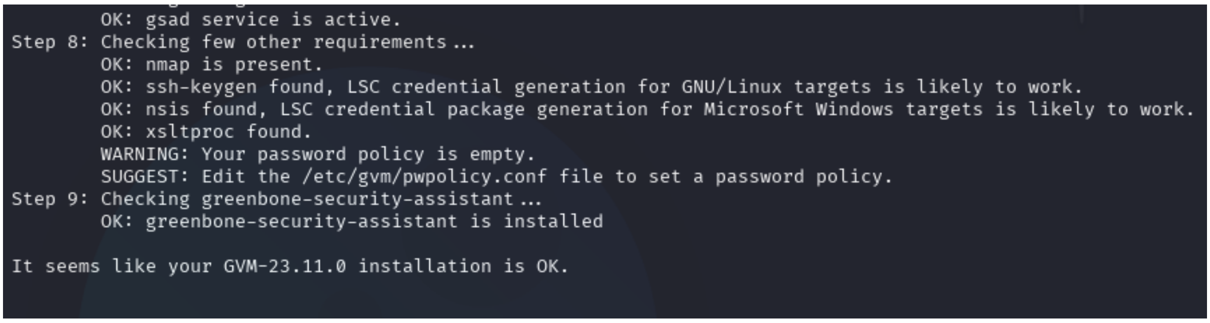


```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# sudo runuser -u _gvm -- gvmd --user=admin --new-password=25811
```

Verifying Installation:

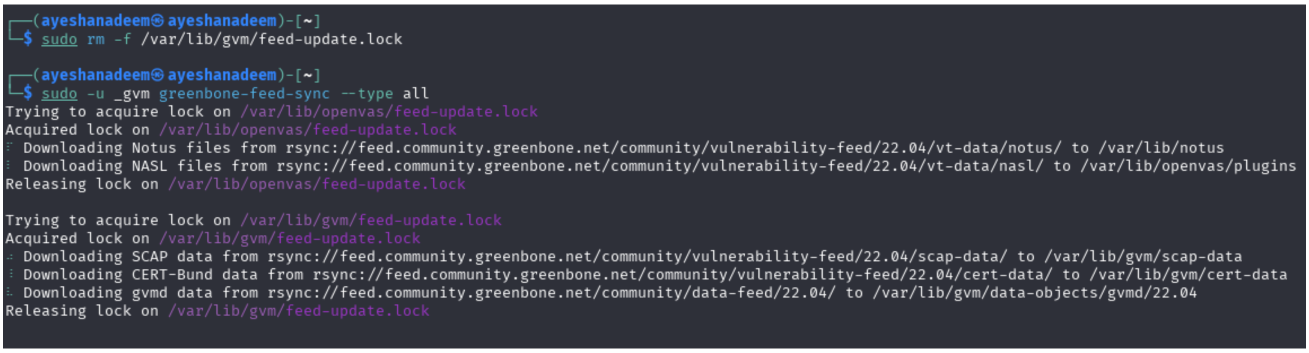


```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ sudo gvm-check-setup
[sudo] password for ayeshanadeem:
gvm-check-setup 23.11.0
  Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 23.13.1.
        OK: Notus Scanner is present in version 22.6.4.
        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
        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 3228 NVTs.
        OK: The notus directory /var/lib/notus/products contains 495 NVTs.
```

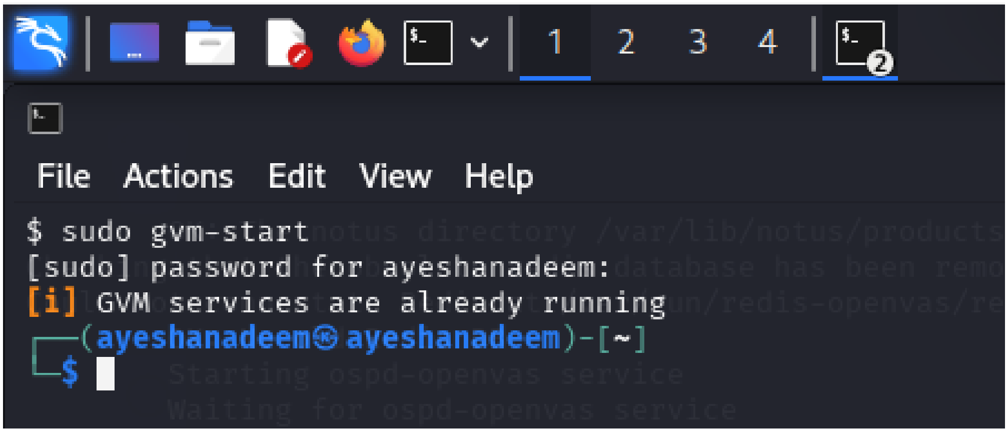


```
        OK: gsad service is active.
Step 8: Checking few other requirements...
        OK: nmap is present.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
        OK: xsltproc found.
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant...
        OK: greenbone-security-assistant is installed

It seems like your GVM-23.11.0 installation is OK.
```

Starting GVM:



```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ sudo rm -f /var/lib/gvm/feed-update.lock

┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ sudo -u _gvm greenbone-feed-sync --type all
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

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
⠇ Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
⠧ Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to /var/lib/gvm/data-objects/gvmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock
```

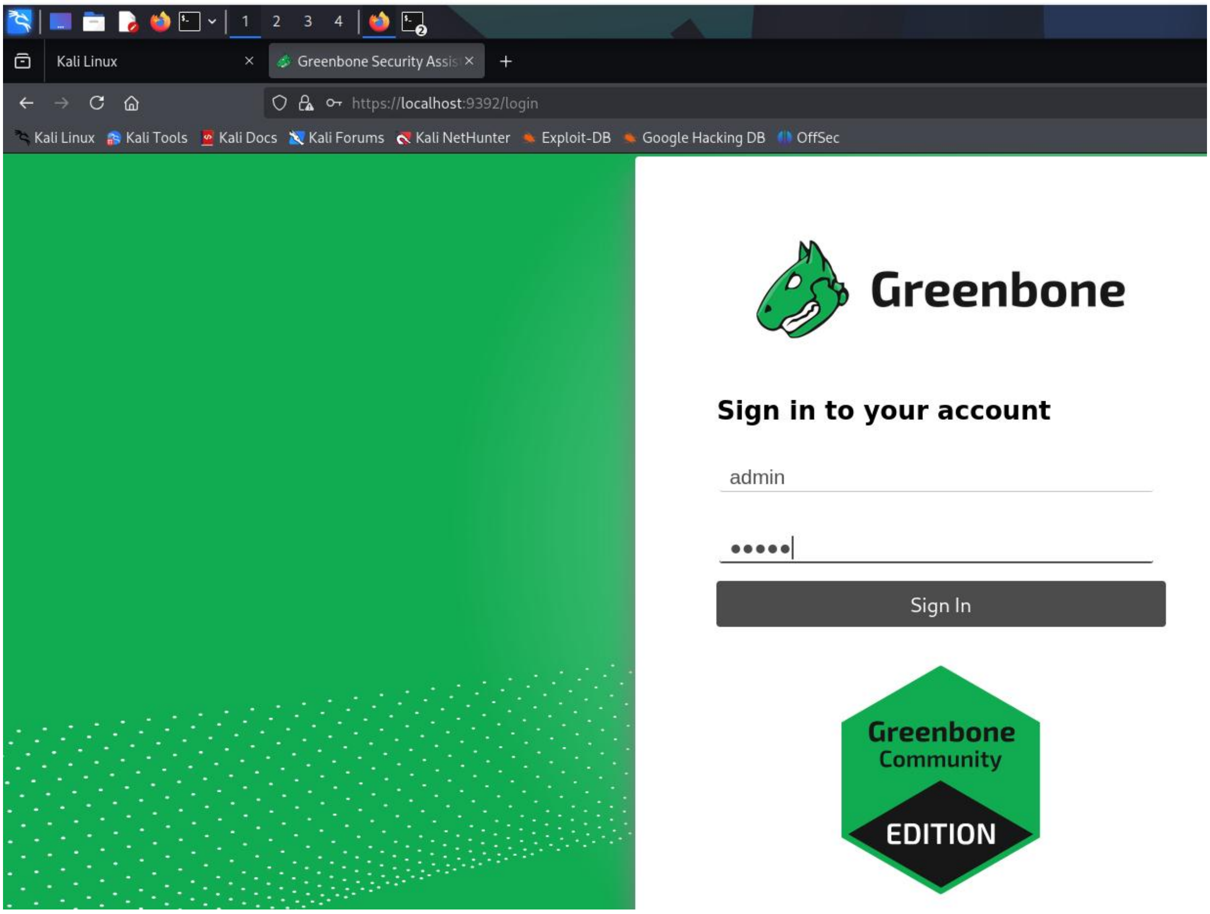


```
$ sudo gvm-start
[sudo] password for ayeshanadeem:
[i] GVM services are already running
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ 
```

If not start automatically, type https://localhost:9392

Greenbone Log-in

Add admin credentials that you set above



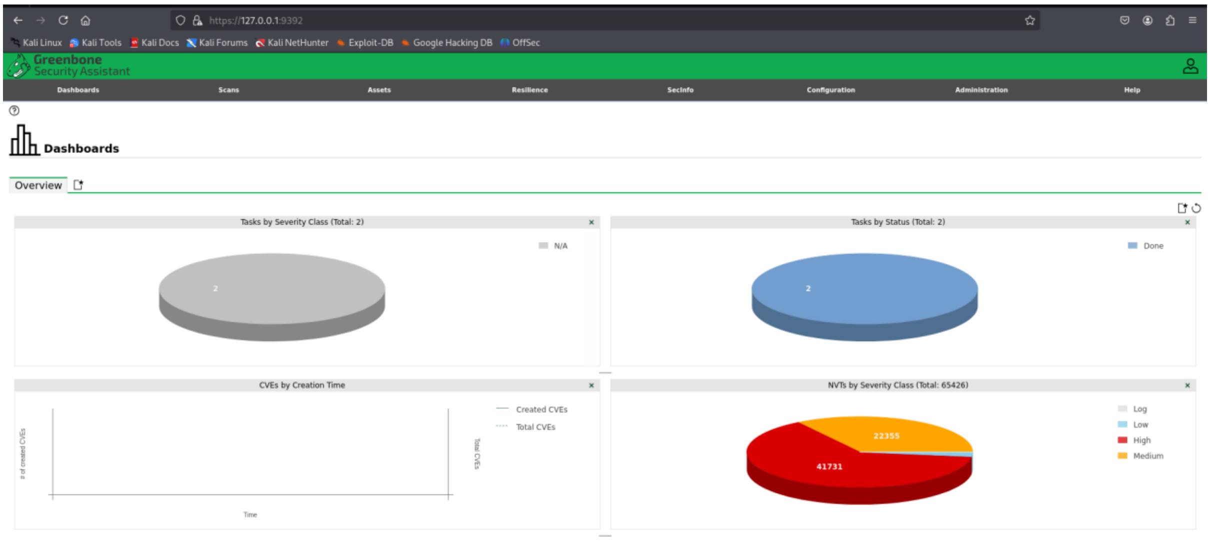
https://localhost:9392/login

Sign in to your account

admin

•••••

Greenbone Dashboard

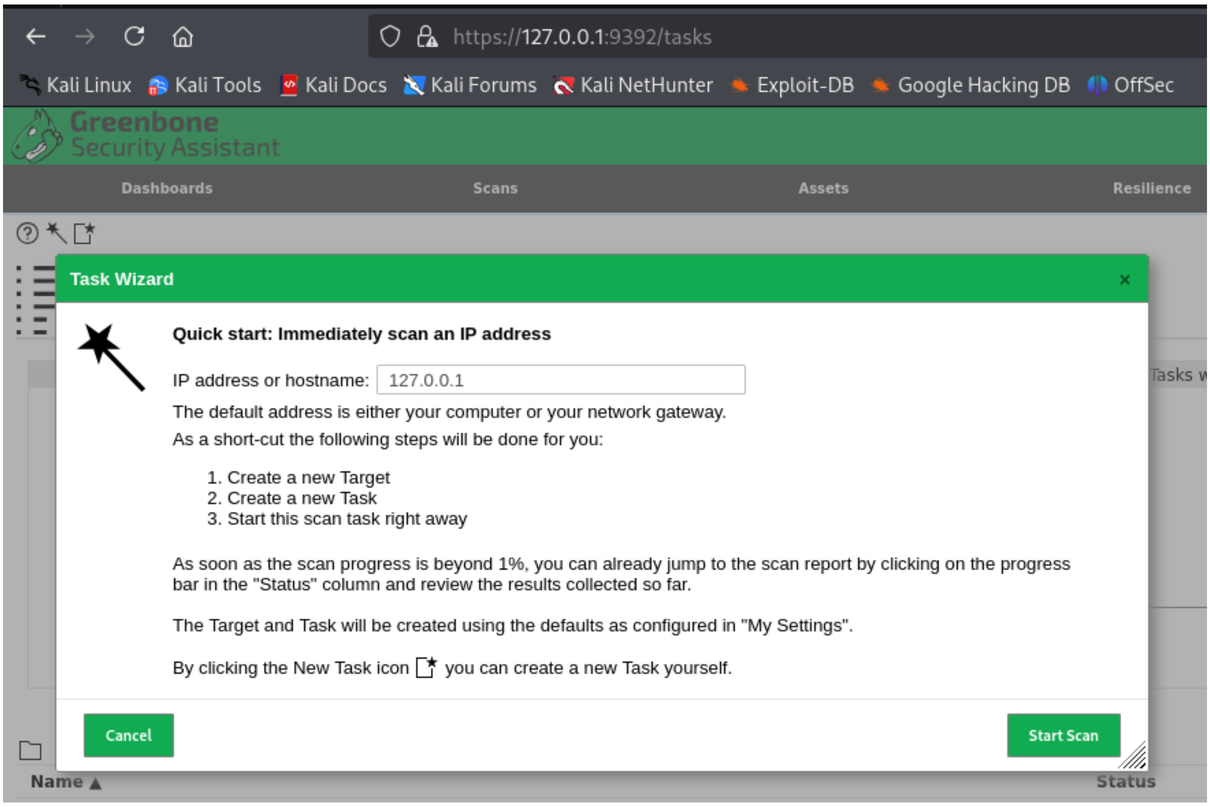


https://127.0.0.1:9392

Task 3

Perform a basic scanning:

Local Host Scan



Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1

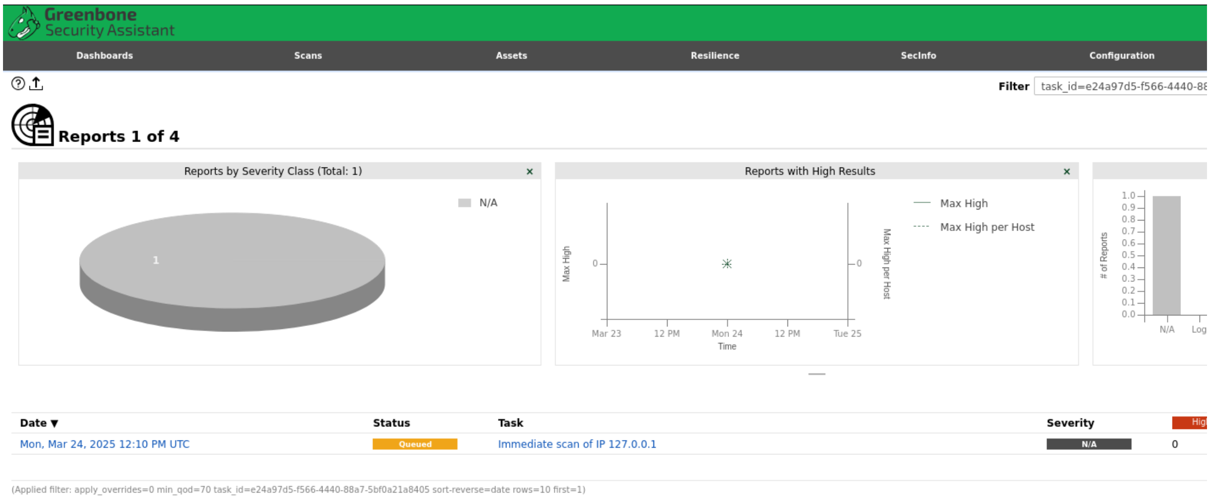
The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.



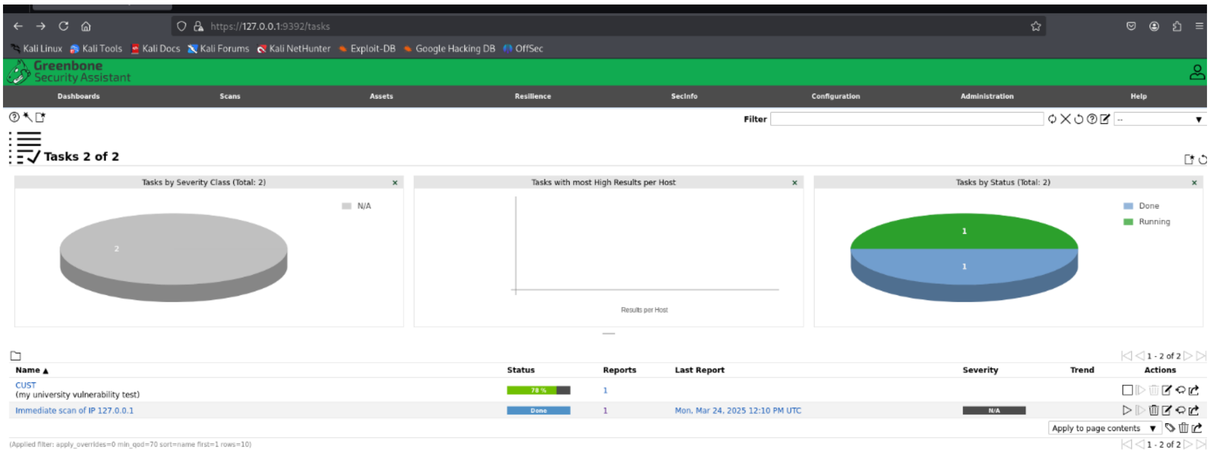
Filter task_id=e24a97d5-f566-4440-88

Reports 1 of 4

Date ▼	Status	Task	Severity	Hig
Mon, Mar 24, 2025 12:10 PM UTC	Queued	Immediate scan of IP 127.0.0.1	N/A	0

(Applied filter: apply_overrides=0 min_qod=70 task_id=e24a97d5-f566-4440-88a7-5bf0a21a8405 sort-reverse=date rows=10 first=1)

Cust IP scan



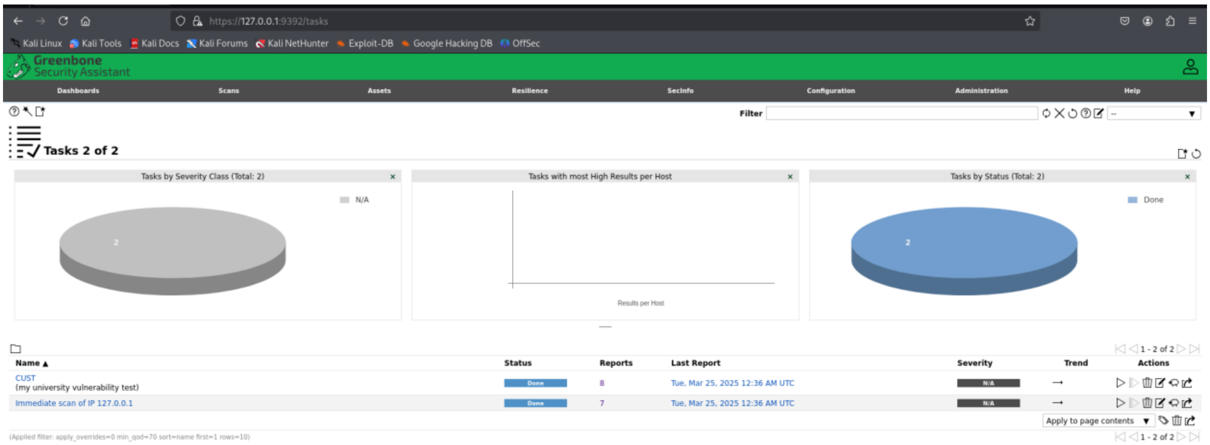
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
CUST (my university vulnerability test)	78 %	1				
Immediate scan of IP 127.0.0.1	Done	1	Mon, Mar 24, 2025 12:10 PM UTC	N/A		

Apply to page contents

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

1 - 2 of 2

Scanned Done (of both CUST IP and local host)



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
CUST (my university vulnerability test)	Done	8	Tue, Mar 25, 2025 12:36 AM UTC	N/A	→	
Immediate scan of IP 127.0.0.1	Done	7	Tue, Mar 25, 2025 12:36 AM UTC	N/A	→	

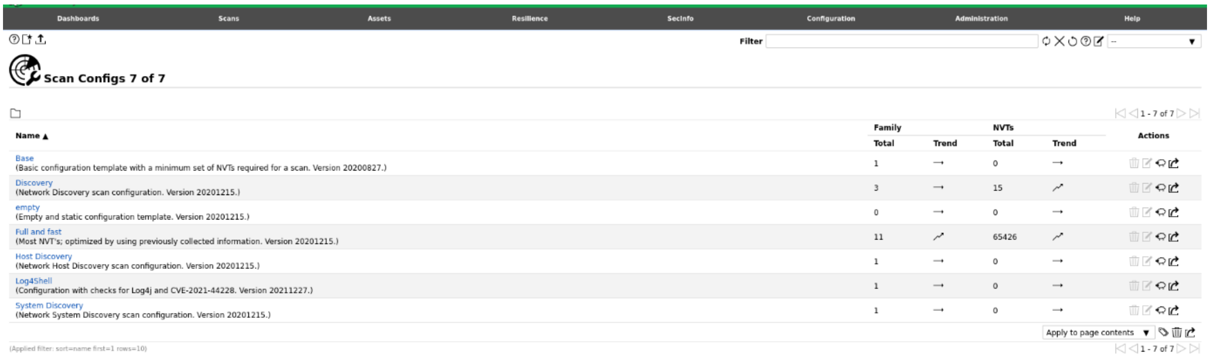
Apply to page contents

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

1 - 2 of 2

Additional screen shots:

Scan Config:



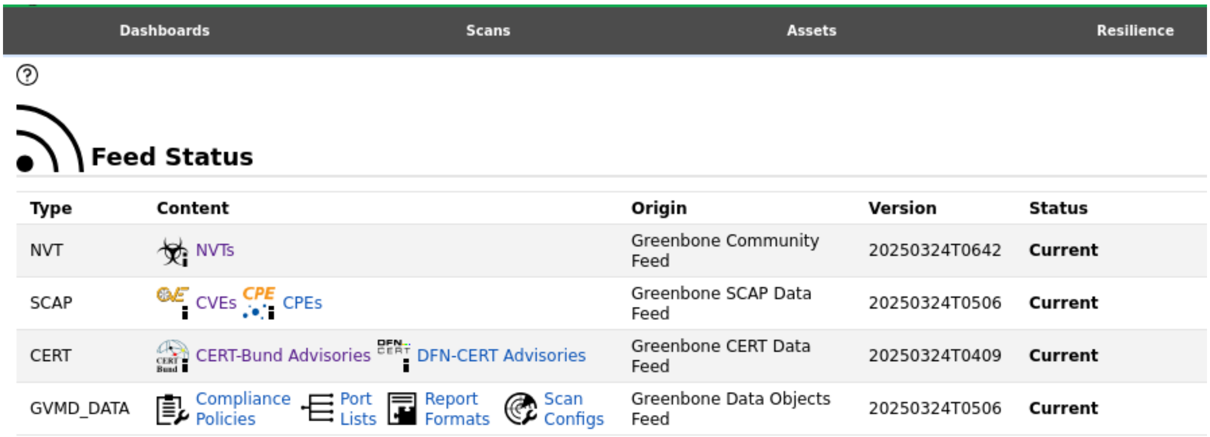
Name ▲	Family		NVTs		Actions
	Total	Trend	Total	Trend	
Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)	1	→	0	→	
Discovery (Network Discovery scan configuration. Version 20201215.)	3	→	15	↗	
empty (Empty and static configuration template. Version 20201215.)	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.)	11	↗	65426	↗	
Host Discovery (Network Host Discovery scan configuration. Version 20201215.)	1	→	0	→	
Log4Shell (Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.)	1	→	0	→	
System Discovery (Network System Discovery scan configuration. Version 20201215.)	1	→	0	→	

Apply to page contents

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

1 - 7 of 7

Feed Status



Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20250324T0642	**Current**
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20250324T0506	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20250324T0409	**Current**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20250324T0506	**Current**