PRACTICAL: 6

AIM:

A medium-sized enterprise is concerned about the security posture of its internal network after a recent breach. The IT security team uses OpenVAS to conduct a comprehensive vulnerability assessment of the network's servers and devices to identify exploitable vulnerabilities. Perform a vulnerability scan on a network using OpenVAS and analyse the results to identify and mitigate potential security risks.

THEORY:

OpenVAS is an open-source vulnerability scanning and management tool that helps to identify security issues like misconfigurations, outdated software, and weak passwords that could be exploited by attackers. OpenVAS is widely used by security professionals to assess and improve the security posture of their networks and is known for its effectiveness and flexibility.

Working of OpenVAS

OpenVAS consists of a server and various client-side tools for scanning and reporting. It uses a regularly updated database of known vulnerabilities and checks systems against these to detect potential weaknesses. The tool performs a comprehensive scan of the specified targets, identifying potential vulnerabilities such as outdated software, misconfigurations, and weak passwords and generates comprehensive reports detailing the identified vulnerabilities and provide recommendations for remediation.

A vulnerability assessment tool works in the following way as follows.

1. Classifies the system resources.
2. Allocates the enumerable values to the classified resources.
3. Detects the possible threats (vulnerabilities) in each resource.
4. Eliminates the vulnerabilities on a priority basis.

Components of OpenVAS architecture

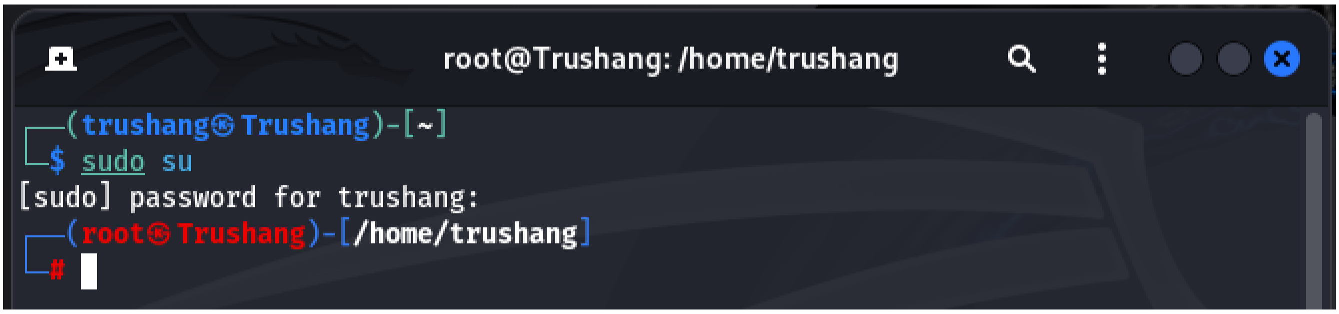
- **OpenVAS Scanner**:
  - The primary engine that performs the actual scanning of target systems. It uses Network Vulnerability Tests (NVTs) to detect security vulnerabilities.
- **OpenVAS Manager**:
  - Manages scan configurations, schedules, and stores scan results. It acts as an intermediary between the scanner and the user interfaces, handling scan requests and processing results.

- **Green bone Security Assistant (GSA)**:
  - A web-based graphical user interface (GUI) that allows users to manage scans, configure settings, and view scan results. It provides an easy-to-use platform for interacting with OpenVAS.
- **OpenVAS CLI**:
  - A command-line interface for users who prefer scripting and command-line operations. It enables management of scans, targets, and results through commands and scripts.
- **Green bone Security Feed (GSF)**:
  - A continuously updated feed that provides the latest Network Vulnerability Tests (NVTs) and security information. It ensures OpenVAS can detect the most recent vulnerabilities.
- **OpenVAS Libraries**:
  - These libraries provide essential functionalities required by the scanner and manager, such as network communication, data storage, and cryptographic operations.
- **Database**:
  - The database stores scan results, configurations, and other essential data. It ensures data persistence and retrieval for analysis and reporting purposes.

CODE:

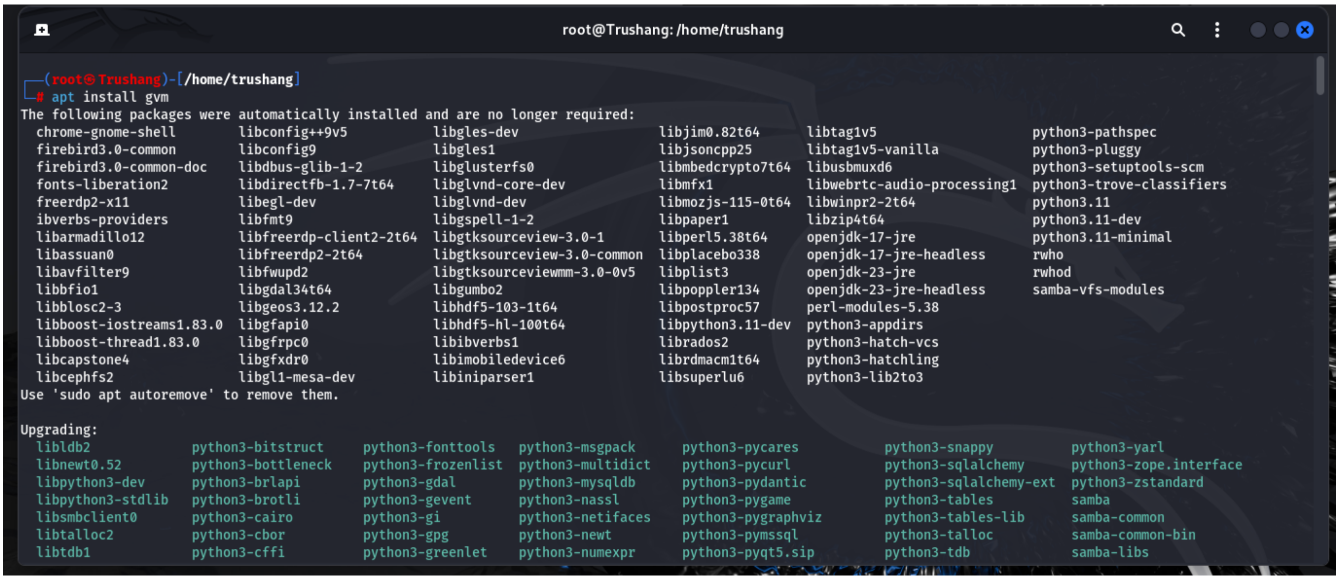
- sudo su
- apt update && apt upgrade
- apt-get update --fix-missing
- apt install gvm
-

OUTPUT:



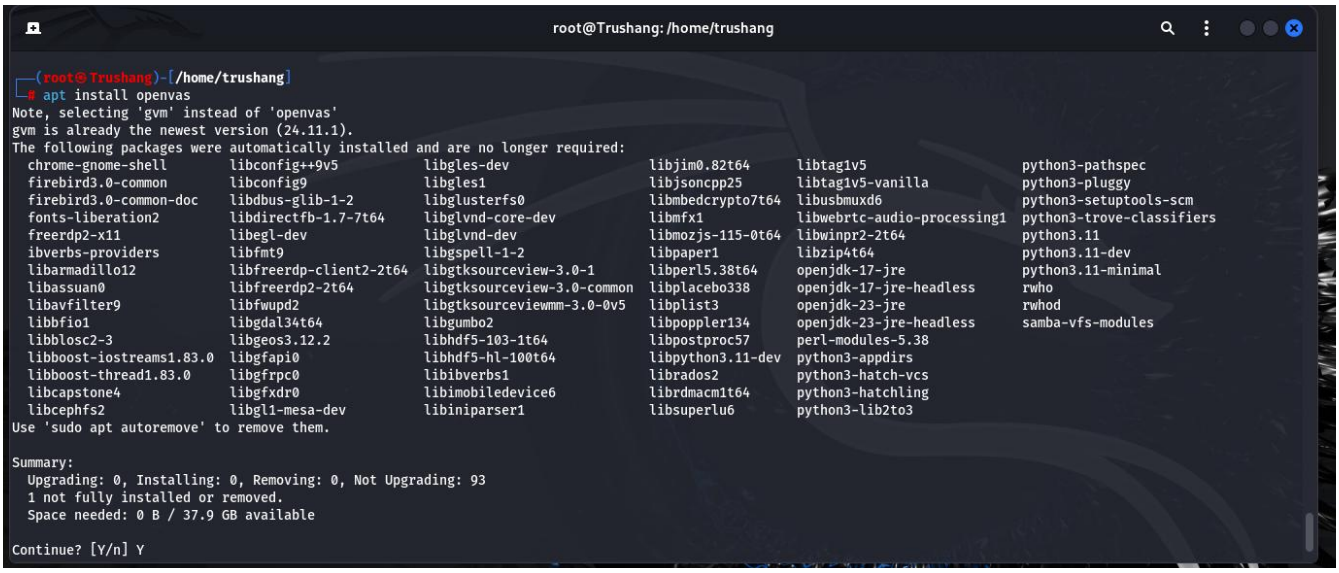
```
root@Trushang: /home/trushang
┌──(trushang㉿Trushang)-[~]
└─$ sudo su
[sudo] password for trushang:
┌──(root㉿Trushang)-[/home/trushang]
└─#
```

Figure 1: Gain root access



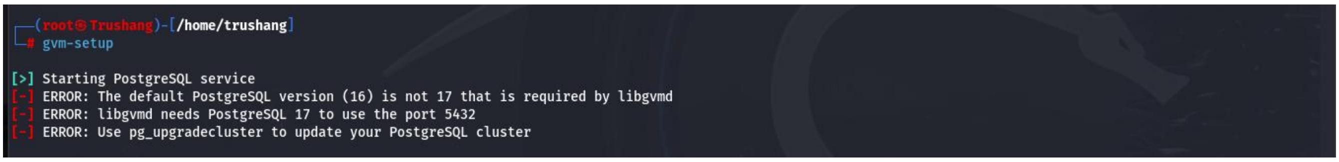
```
┌──(root㉿Trushang)-[/home/trushang]
└─# apt install gvm
The following packages were automatically installed and are no longer required:
  chrome-gnome-shell        libconfig++9v5           libgles-dev                  libjim0.82t64      libtag1v5                    python3-pathspec
  firebird3.0-common        libconfig9               libgles1                     libjsoncpp25       libtag1v5-vanilla            python3-pluggy
  firebird3.0-common-doc    libdbus-glib-1-2         libglusterfs0                libmbedcrypto7t64  libusbmuxd6                  python3-setuptools-scm
  fonts-liberation2         libdirectfb-1.7-7t64     libglvnd-core-dev            libmfx1            libwebrtc-audio-processing1  python3-trove-classifiers
  freerdp2-x11              libegl-dev               libglvnd-dev                 libmozjs-115-0t64  libwinpr2-2t64               python3.11
  ibverbs-providers         libfmt9                  libgspell-1-2                libpaper1          libzip4t64                   python3.11-dev
  libarmadillo12            libfreerdp-client2-2t64  libgtksourceview-3.0-1       libperl5.38t64     openjdk-17-jre               python3.11-minimal
  libassuan0                libfreerdp2-2t64         libgtksourceview-3.0-common  libplacebo338      openjdk-17-jre-headless      rwho
  libavfilter9              libfwupd2                libgtksourceviewmm-3.0-0v5   libplist3          openjdk-23-jre               rwhod
  libbfio1                  libgdal34t64             libgumbo2                    libpoppler134      openjdk-23-jre-headless      samba-vfs-modules
  libblosc2-3               libgeos3.12.2            libhdf5-103-1t64             libpostproc57      perl-modules-5.38
  libboost-iostreams1.83.0  libgfapi0                libhdf5-hl-100t64            libpython3.11-dev  python3-appdirs
  libboost-thread1.83.0     libgfrpc0                libibverbs1                  librados2          python3-hatch-vcs
  libcapstone4              libgfxdr0                libimobiledevice6            librdmacm1t64      python3-hatchling
  libcephfs2                libgl1-mesa-dev          libiniparser1                libsuperlu6        python3-lib2to3
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libldb2             python3-bitstruct     python3-fonttools   python3-msgpack      python3-pycares           python3-snappy          python3-yarl
  libnewt0.52         python3-bottleneck    python3-frozenlist  python3-multidict    python3-pycurl            python3-sqlalchemy      python3-zope.interface
  libpython3-dev      python3-brlapi        python3-gdal        python3-mysqldb      python3-pydantic          python3-sqlalchemy-ext  python3-zstandard
  libpython3-stdlib   python3-brotli        python3-gevent      python3-nassl        python3-pygame            python3-tables          samba
  libsmbclient0       python3-cairo         python3-gi          python3-netifaces    python3-pygraphviz        python3-tables-lib      samba-common
  libtalloc2          python3-cbor          python3-gpg         python3-newt         python3-pymssql           python3-talloc          samba-common-bin
  libtdb1             python3-cffi          python3-greenlet    python3-numexpr      python3-pyqt5.sip         python3-tdb             samba-libs
```

Figure 2: Install gvm in your system



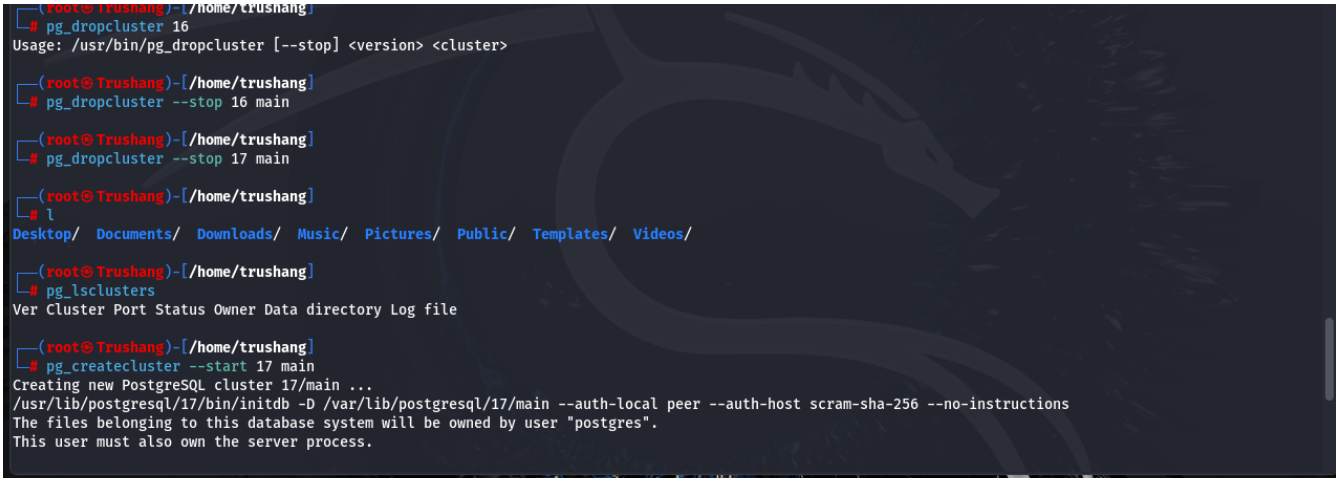
```
┌──(root㉿Trushang)-[/home/trushang]
└─# apt install openvas
Note, selecting 'gvm' instead of 'openvas'
gvm is already the newest version (24.11.1).
The following packages were automatically installed and are no longer required:
  chrome-gnome-shell        libconfig++9v5           libgles-dev                  libjim0.82t64      libtag1v5                    python3-pathspec
  firebird3.0-common        libconfig9               libgles1                     libjsoncpp25       libtag1v5-vanilla            python3-pluggy
  firebird3.0-common-doc    libdbus-glib-1-2         libglusterfs0                libmbedcrypto7t64  libusbmuxd6                  python3-setuptools-scm
  fonts-liberation2         libdirectfb-1.7-7t64     libglvnd-core-dev            libmfx1            libwebrtc-audio-processing1  python3-trove-classifiers
  freerdp2-x11              libegl-dev               libglvnd-dev                 libmozjs-115-0t64  libwinpr2-2t64               python3.11
  ibverbs-providers         libfmt9                  libgspell-1-2                libpaper1          libzip4t64                   python3.11-dev
  libarmadillo12            libfreerdp-client2-2t64  libgtksourceview-3.0-1       libperl5.38t64     openjdk-17-jre               python3.11-minimal
  libassuan0                libfreerdp2-2t64         libgtksourceview-3.0-common  libplacebo338      openjdk-17-jre-headless      rwho
  libavfilter9              libfwupd2                libgtksourceviewmm-3.0-0v5   libplist3          openjdk-23-jre               rwhod
  libbfio1                  libgdal34t64             libgumbo2                    libpoppler134      openjdk-23-jre-headless      samba-vfs-modules
  libblosc2-3               libgeos3.12.2            libhdf5-103-1t64             libpostproc57      perl-modules-5.38
  libboost-iostreams1.83.0  libgfapi0                libhdf5-hl-100t64            libpython3.11-dev  python3-appdirs
  libboost-thread1.83.0     libgfrpc0                libibverbs1                  librados2          python3-hatch-vcs
  libcapstone4              libgfxdr0                libimobiledevice6            librdmacm1t64      python3-hatchling
  libcephfs2                libgl1-mesa-dev          libiniparser1                libsuperlu6        python3-lib2to3
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 93
  1 not fully installed or removed.
  Space needed: 0 B / 37.9 GB available

Continue? [Y/n] Y
```

Figure 3: Install OpenVAS in your system



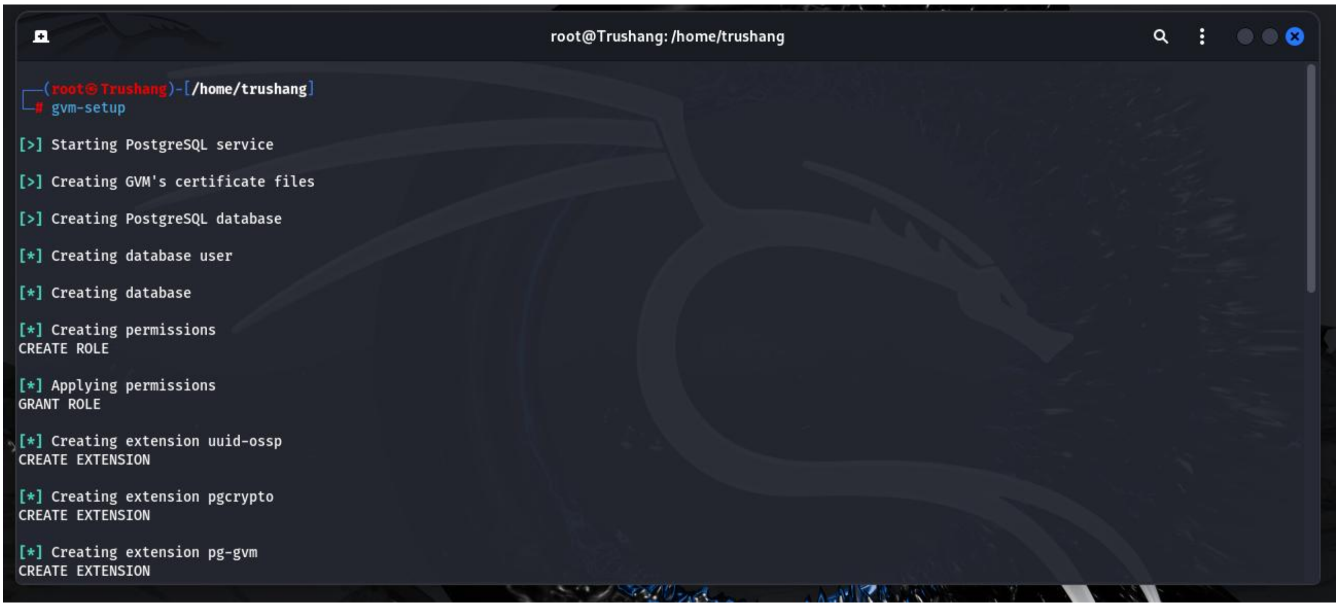
```
┌──(root㉿Trushang)-[/home/trushang]
└─# gvm-setup

[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (16) is not 17 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 17 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```

Figure 4: We have to change the port of PostgreSQL



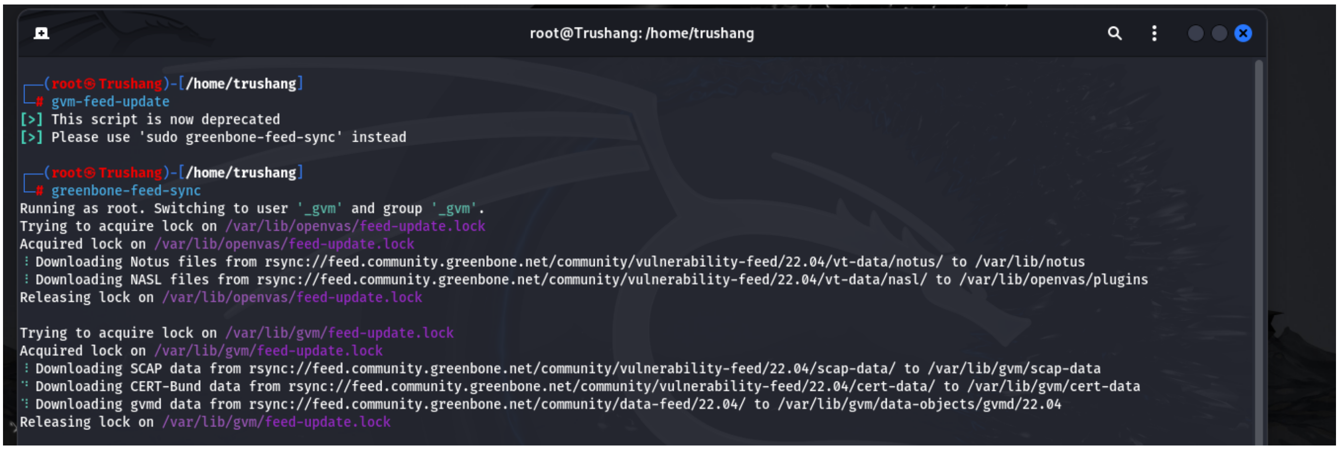
```
┌──(root㉿Trushang)-[/home/trushang]
└─# pg_dropcluster 16
Usage: /usr/bin/pg_dropcluster [--stop] <version> <cluster>

┌──(root㉿Trushang)-[/home/trushang]
└─# pg_dropcluster --stop 16 main

┌──(root㉿Trushang)-[/home/trushang]
└─# pg_dropcluster --stop 17 main

┌──(root㉿Trushang)-[/home/trushang]
└─# l
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Templates/  Videos/

┌──(root㉿Trushang)-[/home/trushang]
└─# pg_lsclusters
Ver Cluster Port Status Owner Data directory Log file

┌──(root㉿Trushang)-[/home/trushang]
└─# pg_createcluster --start 17 main
Creating new PostgreSQL cluster 17/main ...
/usr/lib/postgresql/17/bin/initdb -D /var/lib/postgresql/17/main --auth-local peer --auth-host scram-sha-256 --no-instructions
The files belonging to this database system will be owned by user "postgres".
This user must also own the server process.
```

Figure 5: Delete PostgreSQL 16 and 17 and then create 17 main cluster



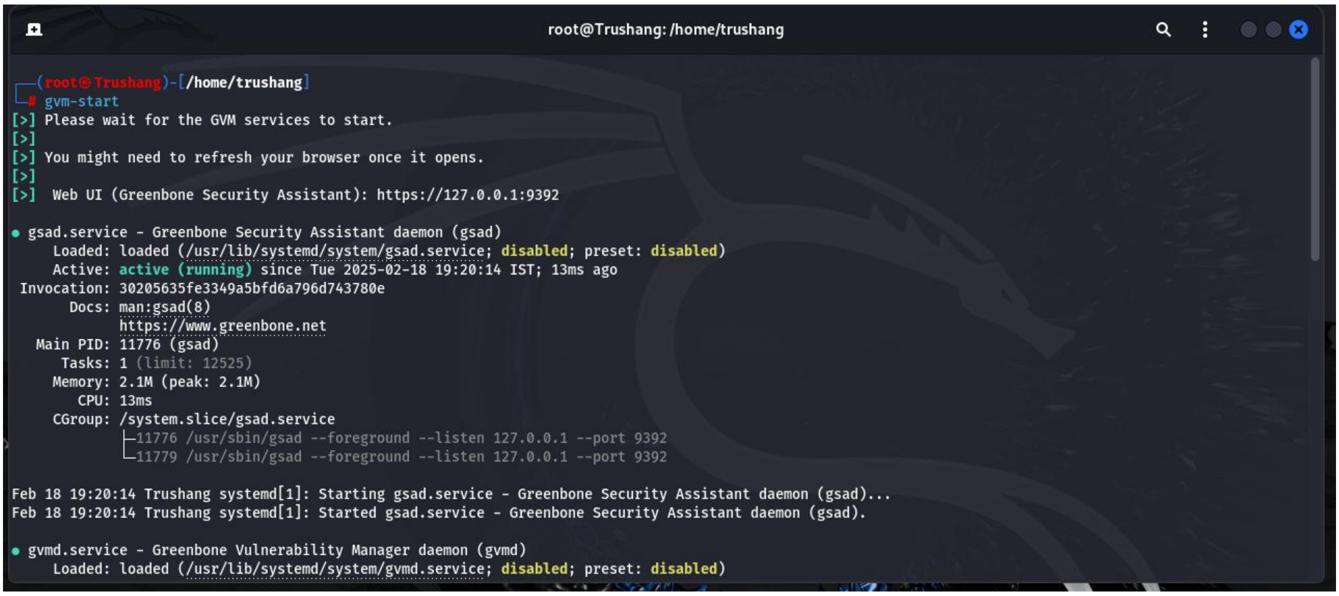
```
┌──(root㉿Trushang)-[/home/trushang]
└─# gvm-setup

[>] 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
```

Figure 6: Start GVM setup



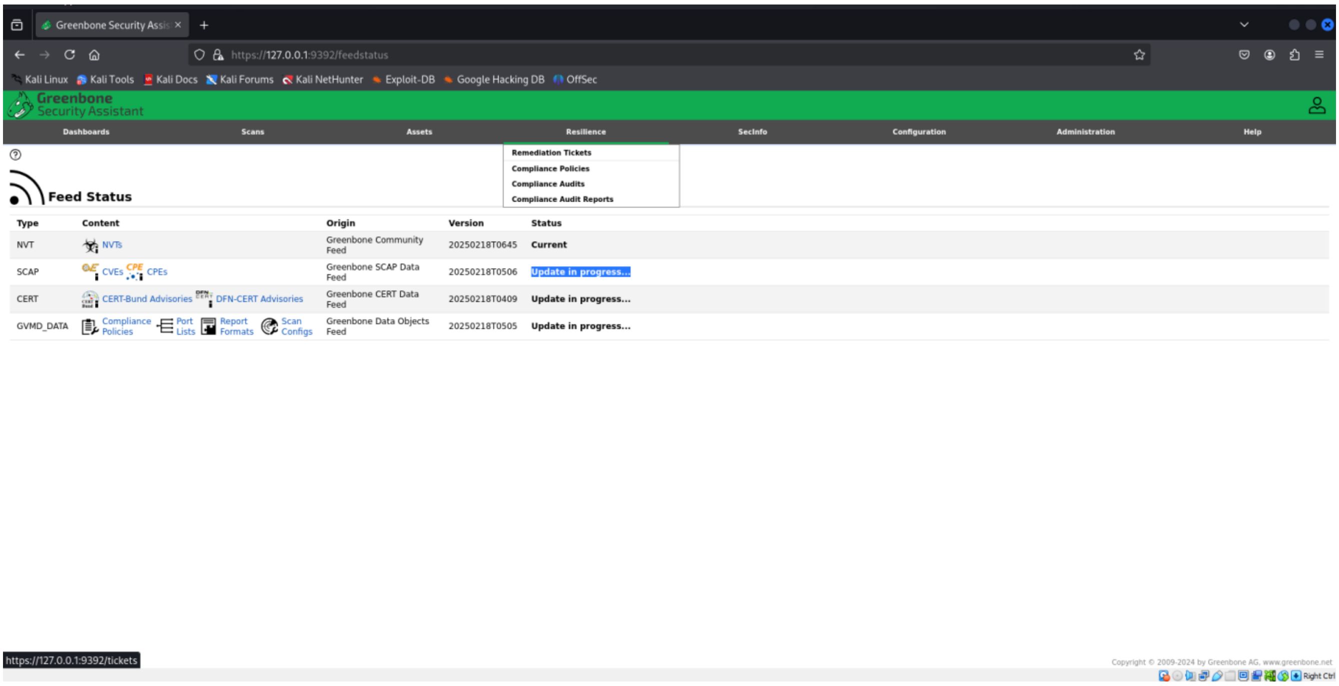
```
┌──(root㉿Trushang)-[/home/trushang]
└─# gvm-feed-update
[>] This script is now deprecated
[>] Please use 'sudo greenbone-feed-sync' instead

┌──(root㉿Trushang)-[/home/trushang]
└─# greenbone-feed-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

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
```

Figure 7: Sync NVT, SCAP, CERT, GVMD_DATA



```
┌──(root㉿Trushang)-[/home/trushang]
└─# 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

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-02-18 19:20:14 IST; 13ms ago
 Invocation: 30205635fe3349a5bfd6a796d743780e
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 11776 (gsad)
      Tasks: 1 (limit: 12525)
     Memory: 2.1M (peak: 2.1M)
        CPU: 13ms
     CGroup: /system.slice/gsad.service
             ├─11776 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
             └─11779 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Feb 18 19:20:14 Trushang systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Feb 18 19:20:14 Trushang systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
```

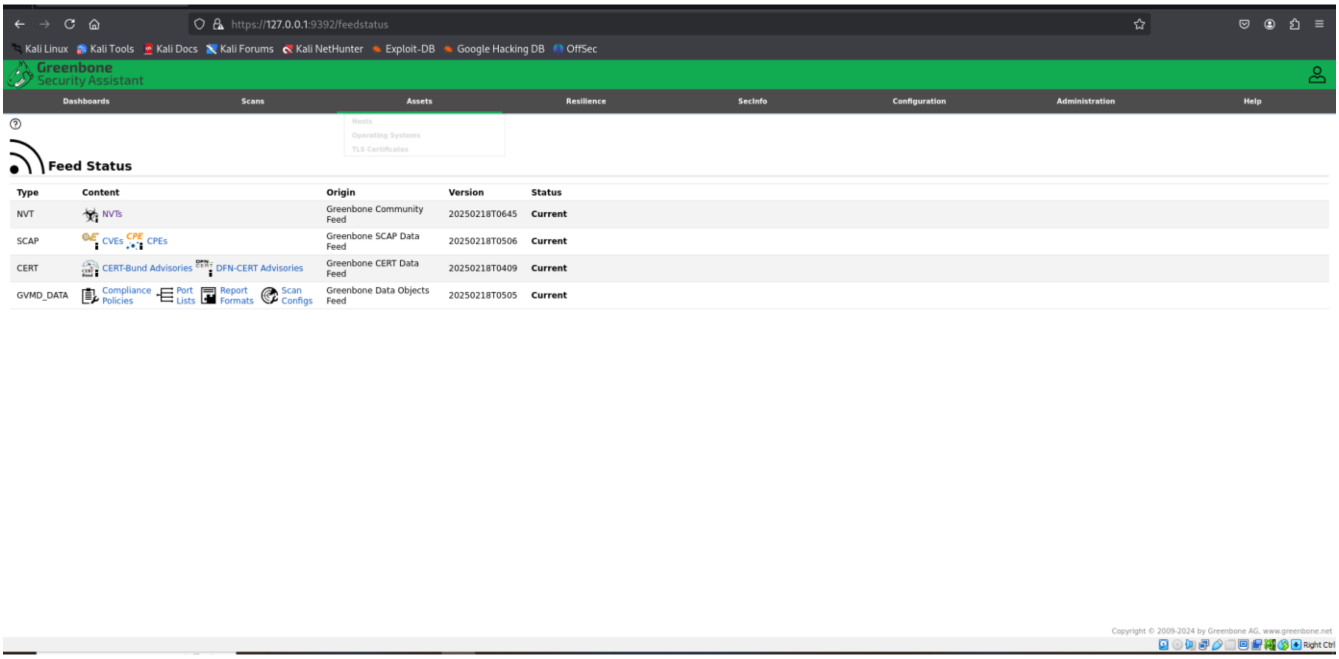
Figure 8: Start GVM



Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20250218T0645	Current
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20250218T0506	Update in progress...
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20250218T0409	Update in progress...
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20250218T0505	Update in progress...

Figure 9: Check feed status

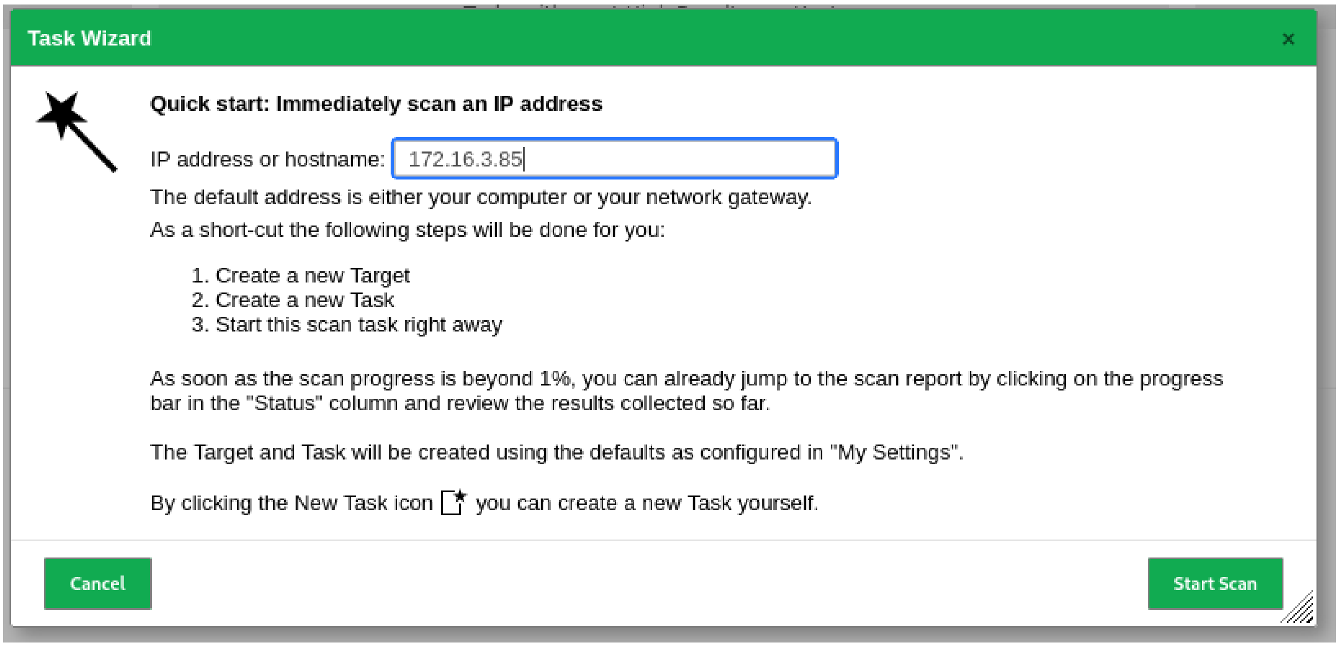


Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20250218T0645	Current
SCAP	CVEs CPEs	Greenbone SCAP Data Feed	20250218T0506	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone CERT Data Feed	20250218T0409	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Data Objects Feed	20250218T0505	Current

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Figure 10: Feed status is now current



Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 172.16.3.85

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

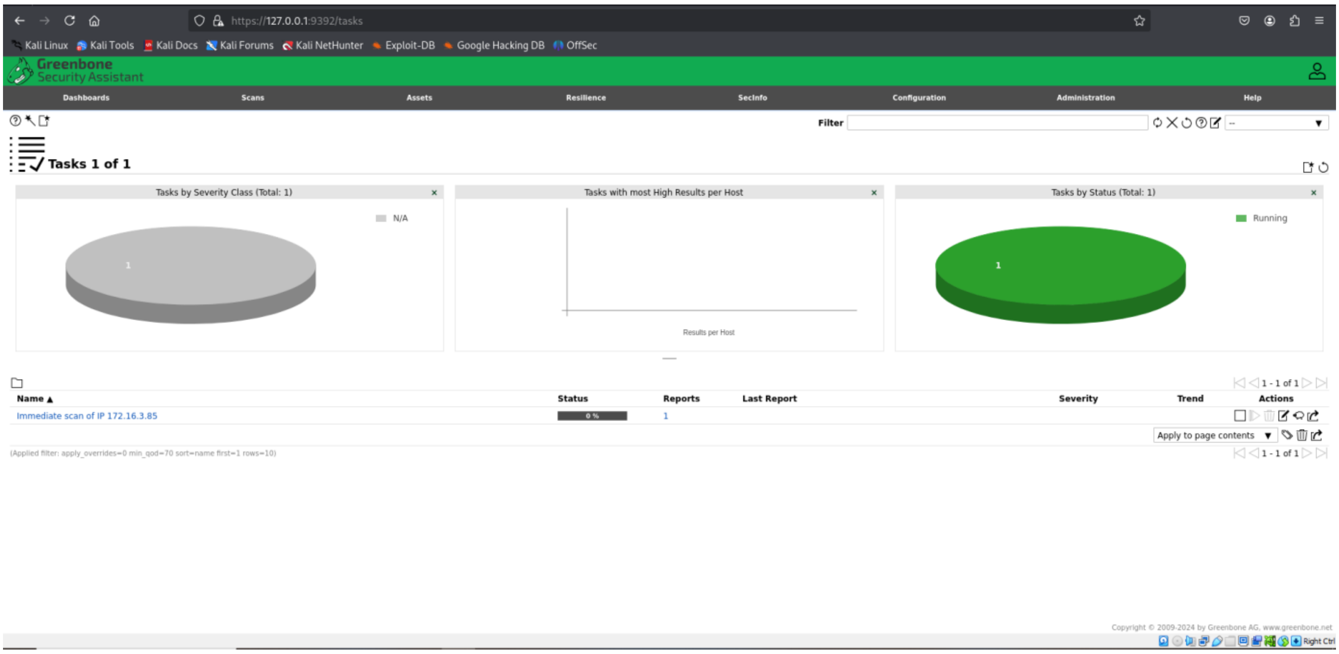
1. Create a new Target
2. Create a new Task
3. Start this scan task right away

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.

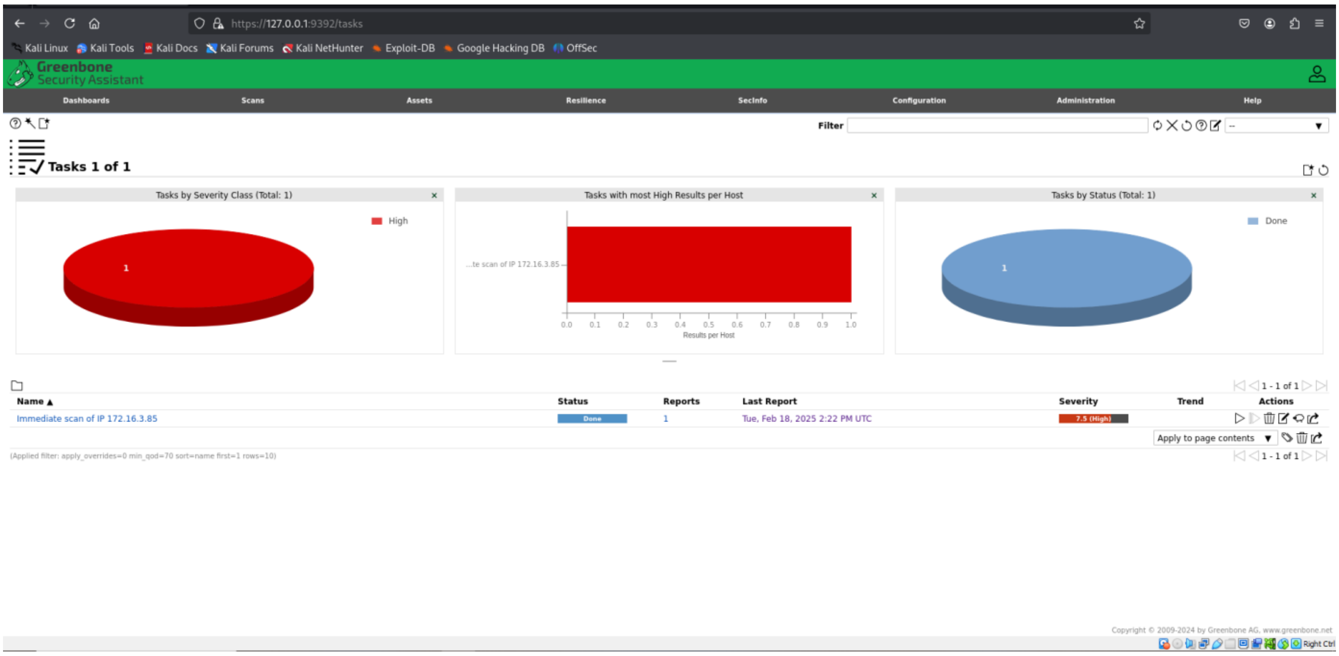
Figure 11: Write IP address for scan



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 172.16.3.85	0 %	1				

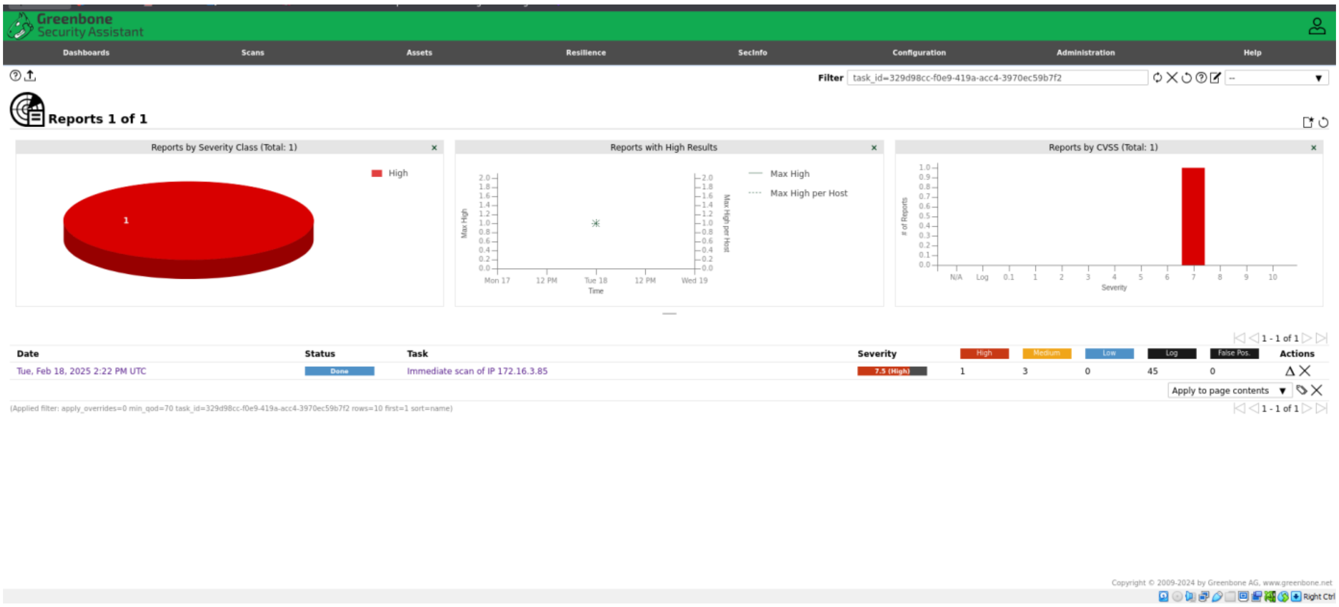
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 12: Scanning IP address



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 172.16.3.85	Done	1	Tue, Feb 18, 2025 2:22 PM UTC	7.5 (High)		

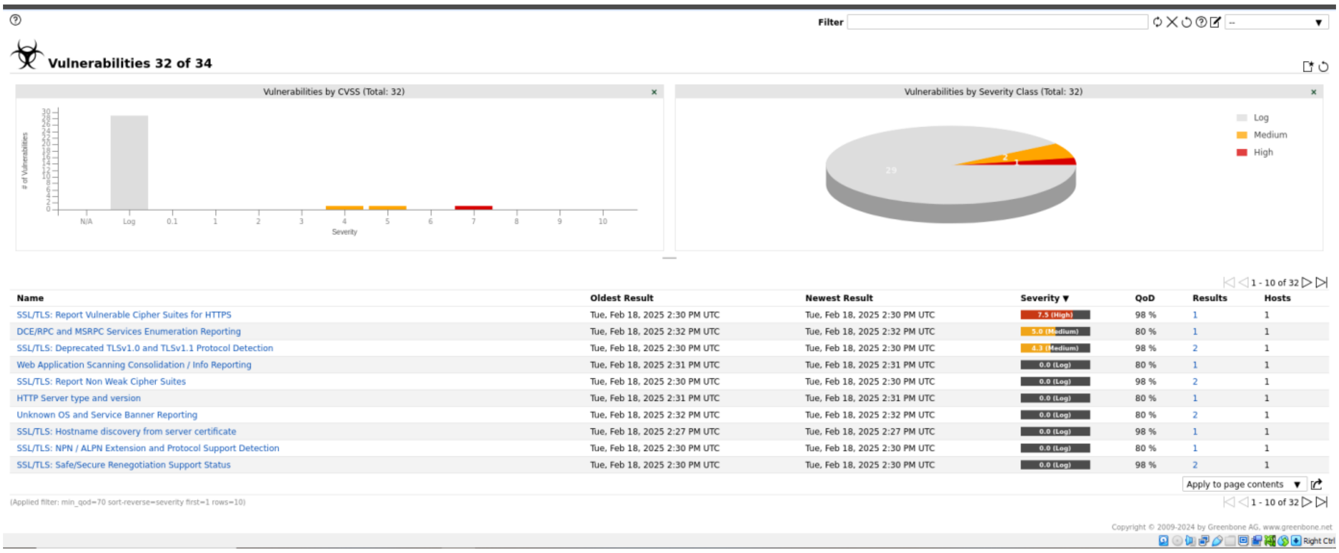
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)



Reports 1 of 1

Date	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Tue, Feb 18, 2025 2:22 PM UTC	Done	Immediate scan of IP 172.16.3.85	7.5 (High)	1	3	0	45	0	

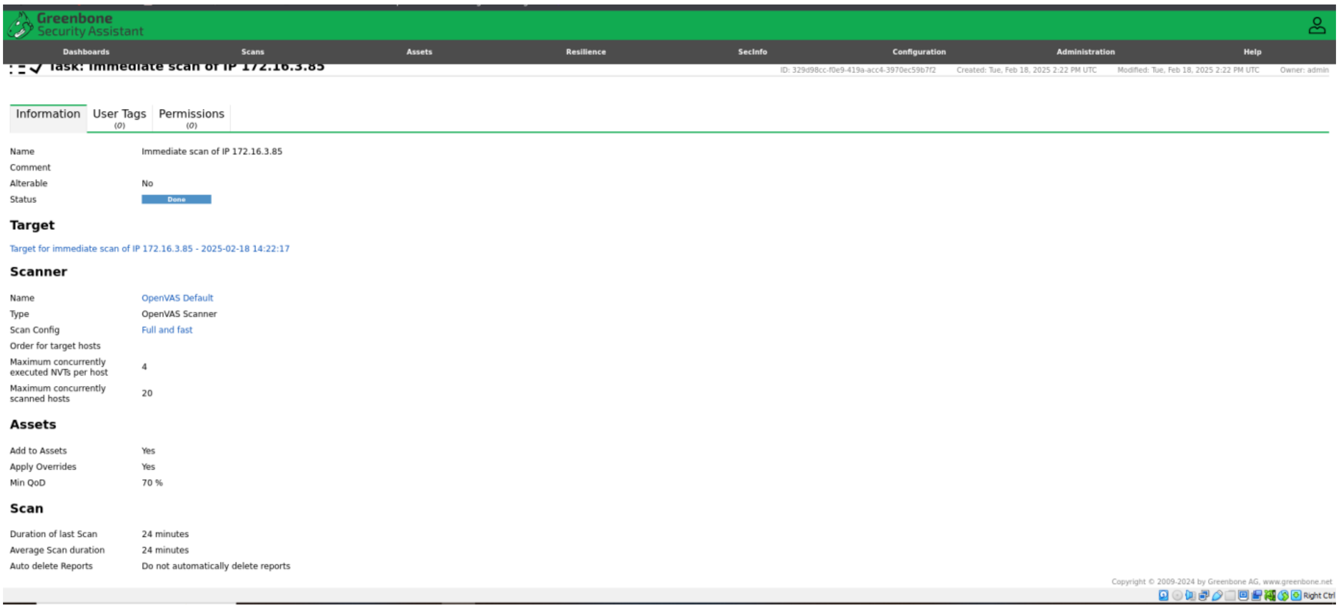
(Applied filter: apply_overrides=0 min_qod=70 task_id=329d98cc-f0e9-419a-acc4-3970ec59b7f2 rows=10 first=1 sort=name)


Filter
Vulnerabilities by CVSS (Total: 32)
# of Vulnerabilities
N/A
Log
0.1
1
2
3
4
5
6
7
8
9
10
Severity
Vulnerabilities by Severity Class (Total: 32)
Log
Medium
High
29
2
1
1 - 10 of 32
Apply to page contents
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net
Right Ctrl

Vulnerabilities 32 of 34

Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	Tue, Feb 18, 2025 2:30 PM UTC	Tue, Feb 18, 2025 2:30 PM UTC	7.5 (High)	98 %	1	1
DCE/RPC and MSRPC Services Enumeration Reporting	Tue, Feb 18, 2025 2:32 PM UTC	Tue, Feb 18, 2025 2:32 PM UTC	5.0 (Medium)	80 %	1	1
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	Tue, Feb 18, 2025 2:30 PM UTC	Tue, Feb 18, 2025 2:30 PM UTC	4.3 (Medium)	98 %	2	1
Web Application Scanning Consolidation / Info Reporting	Tue, Feb 18, 2025 2:31 PM UTC	Tue, Feb 18, 2025 2:31 PM UTC	0.0 (Log)	80 %	1	1
SSL/TLS: Report Non Weak Cipher Suites	Tue, Feb 18, 2025 2:30 PM UTC	Tue, Feb 18, 2025 2:30 PM UTC	0.0 (Log)	98 %	2	1
HTTP Server type and version	Tue, Feb 18, 2025 2:31 PM UTC	Tue, Feb 18, 2025 2:31 PM UTC	0.0 (Log)	80 %	1	1
Unknown OS and Service Banner Reporting	Tue, Feb 18, 2025 2:32 PM UTC	Tue, Feb 18, 2025 2:32 PM UTC	0.0 (Log)	80 %	2	1
SSL/TLS: Hostname discovery from server certificate	Tue, Feb 18, 2025 2:27 PM UTC	Tue, Feb 18, 2025 2:27 PM UTC	0.0 (Log)	98 %	1	1
SSL/TLS: NPN / ALPN Extension and Protocol Support Detection	Tue, Feb 18, 2025 2:30 PM UTC	Tue, Feb 18, 2025 2:30 PM UTC	0.0 (Log)	80 %	1	1
SSL/TLS: Safe/Secure Renegotiation Support Status	Tue, Feb 18, 2025 2:30 PM UTC	Tue, Feb 18, 2025 2:30 PM UTC	0.0 (Log)	98 %	2	1

(Applied filter: min_qod=70 sort-reverse=severity first=1 rows=10)



Task: Immediate scan of IP 172.16.3.85

ID: 329d98cc-f0e9-419a-acc4-3970ec59b7f2 Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:22 PM UTC Owner: admin

Name	Immediate scan of IP 172.16.3.85
Comment	
Alterable	No
Status	Done

Target

Target for immediate scan of IP 172.16.3.85 - 2025-02-18 14:22:17

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

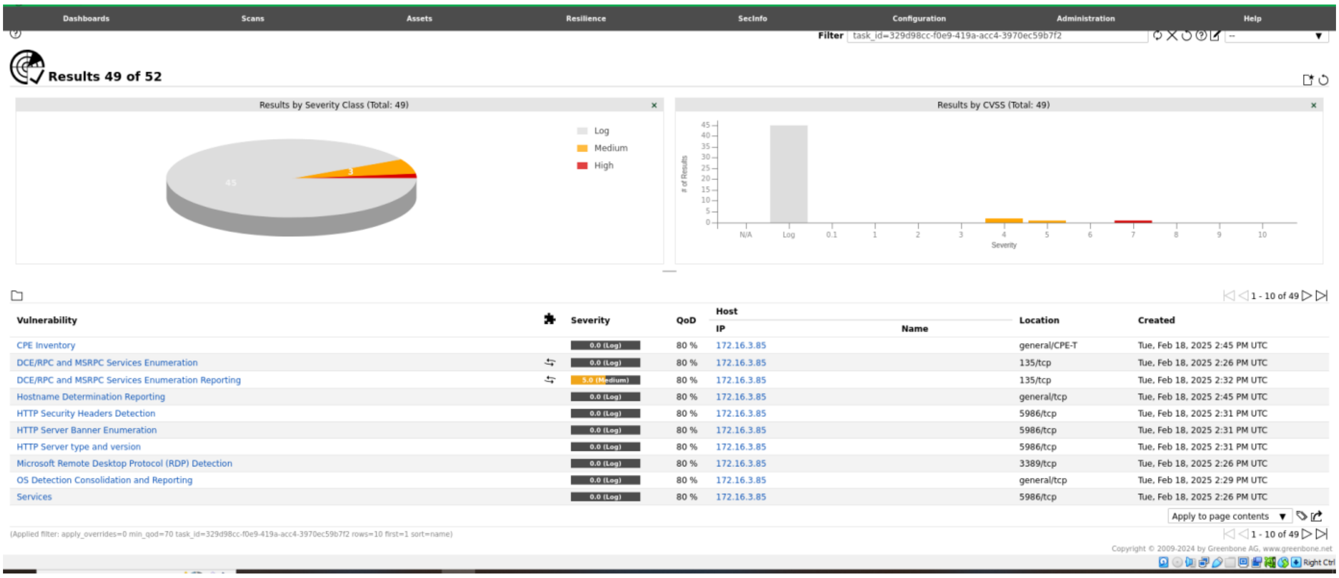
Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	24 minutes
Average Scan duration	24 minutes
Auto delete Reports	Do not automatically delete reports

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



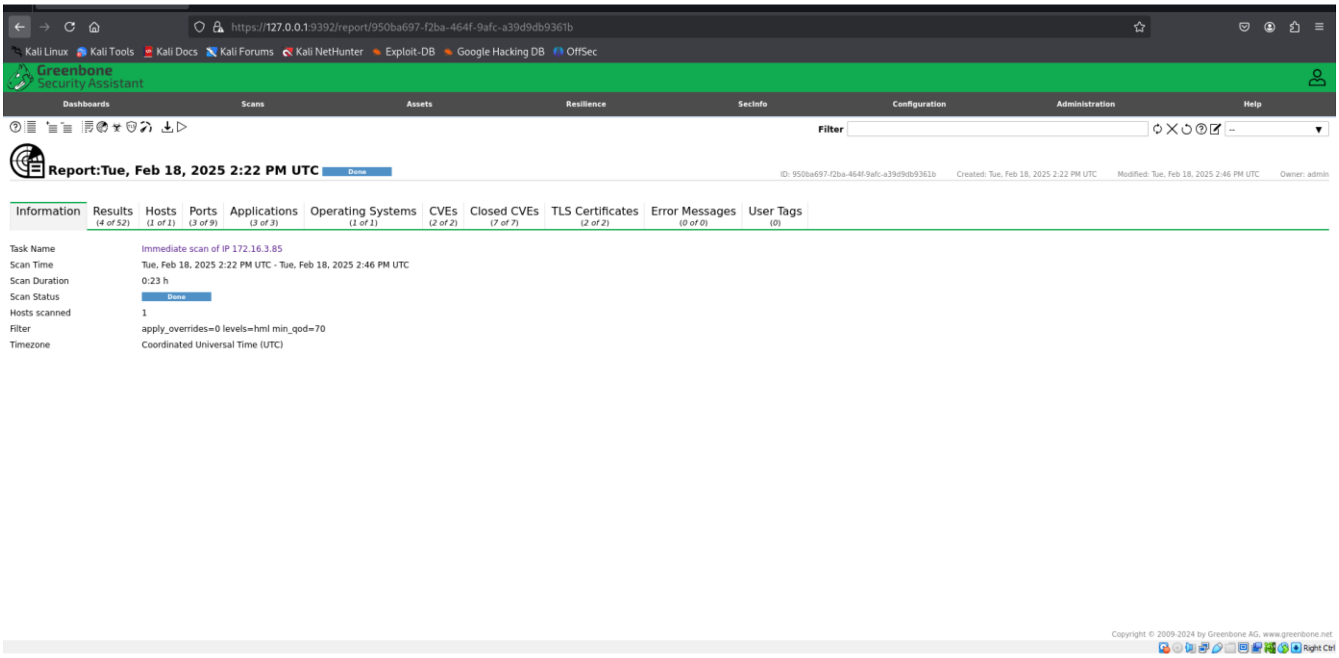
Filter: task_id=329d98cc-f0e9-419a-acc4-3970ec59b7f2

Results 49 of 52

Vulnerability	Severity	QoD	Host IP	Host Name	Location	Created
CPE Inventory	0.0 (Log)	80 %	172.16.3.85		general/CPE-T	Tue, Feb 18, 2025 2:45 PM UTC
DCE/RPC and MSRPC Services Enumeration	0.0 (Log)	80 %	172.16.3.85		135/tcp	Tue, Feb 18, 2025 2:26 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.3.85		135/tcp	Tue, Feb 18, 2025 2:32 PM UTC
Hostname Determination Reporting	0.0 (Log)	80 %	172.16.3.85		general/tcp	Tue, Feb 18, 2025 2:45 PM UTC
HTTP Security Headers Detection	0.0 (Log)	80 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:31 PM UTC
HTTP Server Banner Enumeration	0.0 (Log)	80 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:31 PM UTC
HTTP Server type and version	0.0 (Log)	80 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:31 PM UTC
Microsoft Remote Desktop Protocol (RDP) Detection	0.0 (Log)	80 %	172.16.3.85		3389/tcp	Tue, Feb 18, 2025 2:26 PM UTC
OS Detection Consolidation and Reporting	0.0 (Log)	80 %	172.16.3.85		general/tcp	Tue, Feb 18, 2025 2:29 PM UTC
Services	0.0 (Log)	80 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:26 PM UTC

(Applied filter: apply_overrides=0 min_qod=70 task_id=329d98cc-f0e9-419a-acc4-3970ec59b7f2 rows=10 first=1 sort=name)

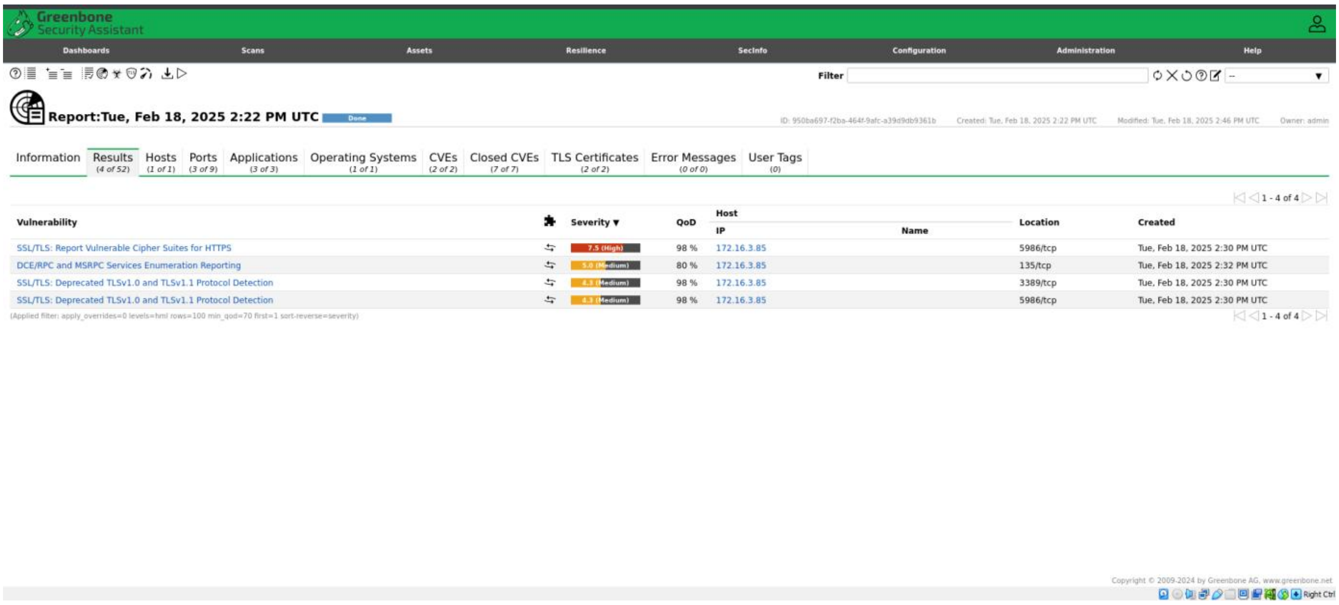
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



Report:Tue, Feb 18, 2025 2:22 PM UTC Done

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Task Name	Immediate scan of IP 172.16.3.85
Scan Time	Tue, Feb 18, 2025 2:22 PM UTC - Tue, Feb 18, 2025 2:46 PM UTC
Scan Duration	0:23 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 levels=hml min_qod=70
Timezone	Coordinated Universal Time (UTC)

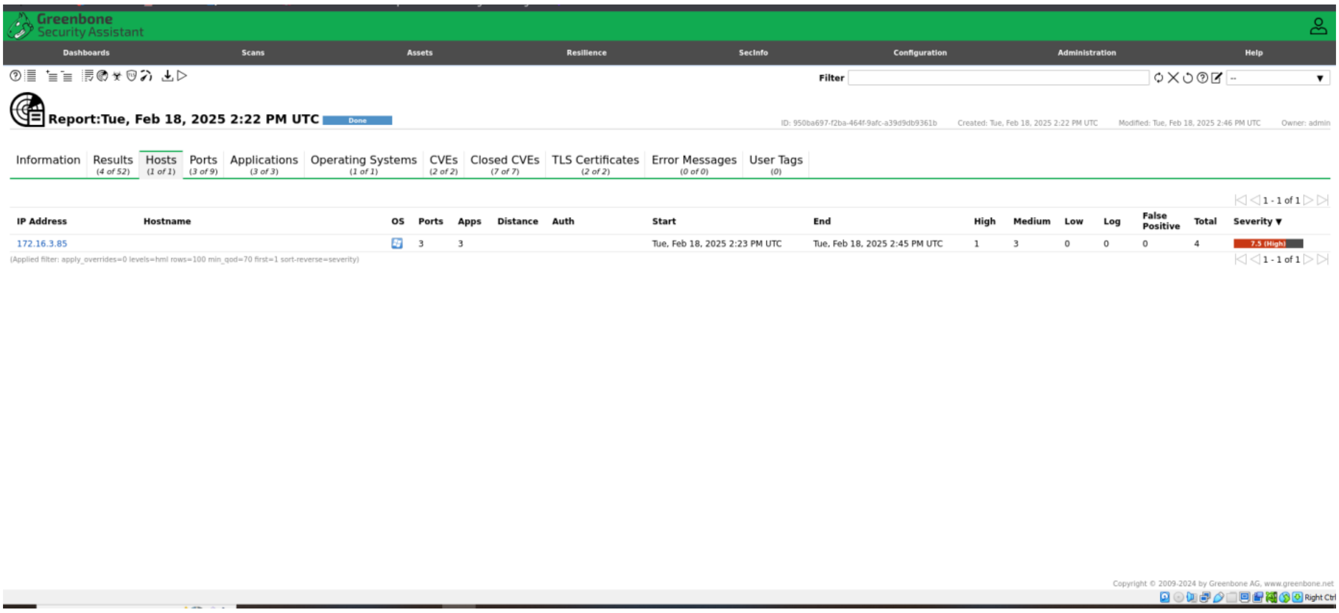


Report:Tue, Feb 18, 2025 2:22 PM UTC Done

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	⇆	7.5 (High)	98 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:30 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	172.16.3.85		135/tcp	Tue, Feb 18, 2025 2:32 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	172.16.3.85		3389/tcp	Tue, Feb 18, 2025 2:30 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	172.16.3.85		5986/tcp	Tue, Feb 18, 2025 2:30 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)



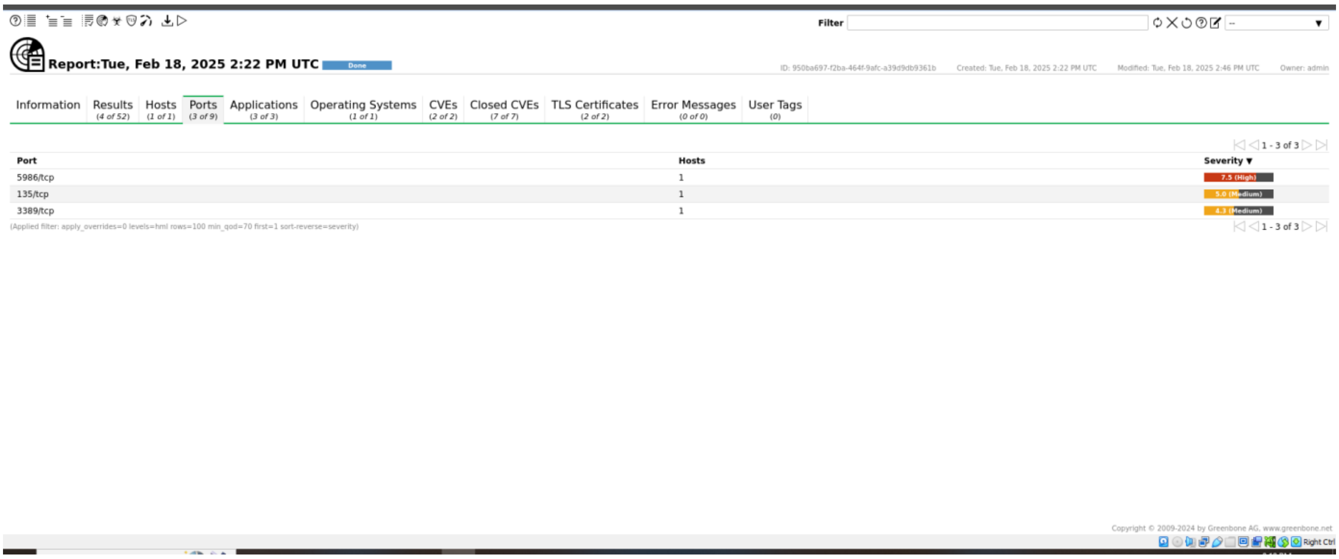
Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
172.16.3.85			3	3			Tue, Feb 18, 2025 2:23 PM UTC	Tue, Feb 18, 2025 2:45 PM UTC	1	3	0	0	0	4	7.5 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



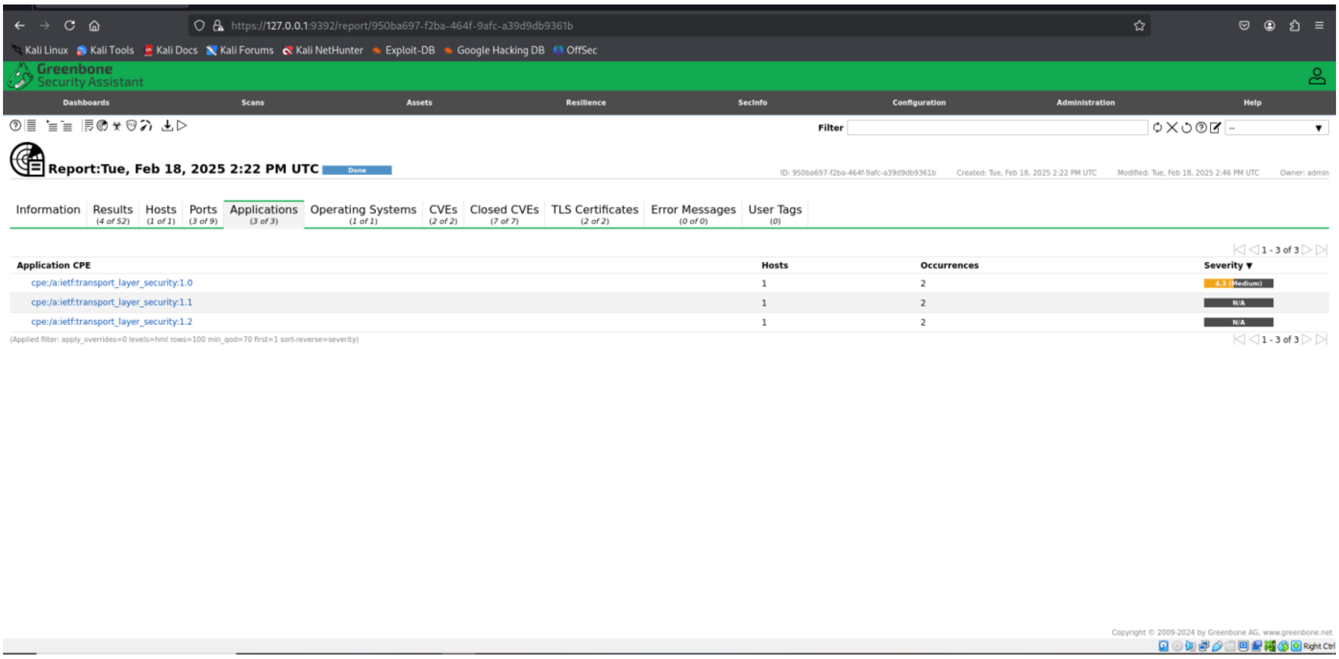
Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Port	Hosts	Severity ▼
5986/tcp	1	7.5 (High)
135/tcp	1	5.0 (Medium)
3389/tcp	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net



https://127.0.0.1:9392/report/950ba697-f2ba-464f-9afc-a39d9db9361b

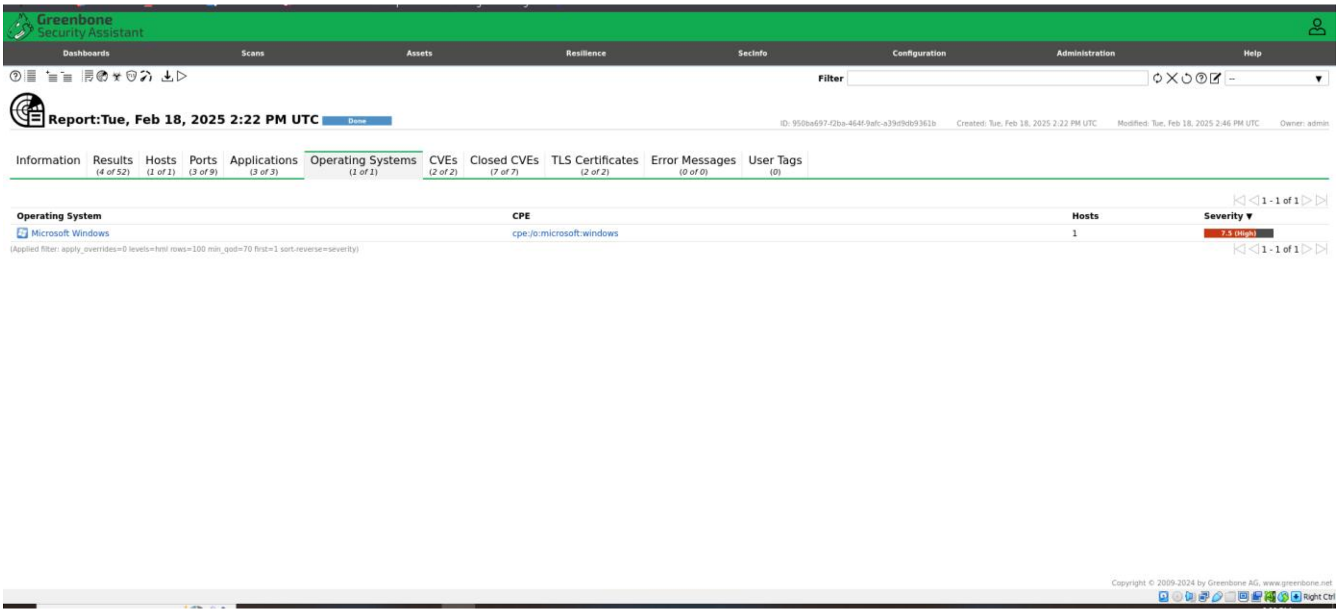
Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:ietf:transport_layer_security:1.0	1	2	4.3 (Medium)
cpe:/a:ietf:transport_layer_security:1.1	1	2	N/A
cpe:/a:ietf:transport_layer_security:1.2	1	2	N/A

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

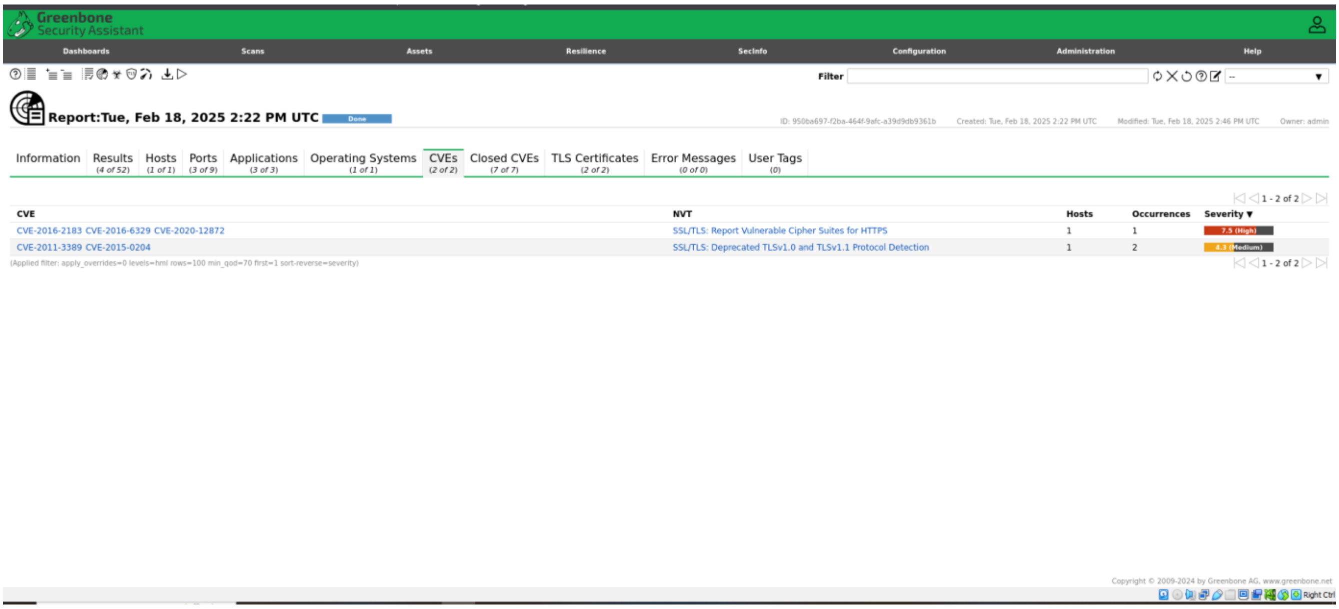


Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Operating System	CPE	Hosts	Severity ▼
Microsoft Windows	cpe:/o:microsoft:windows	1	7.5 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

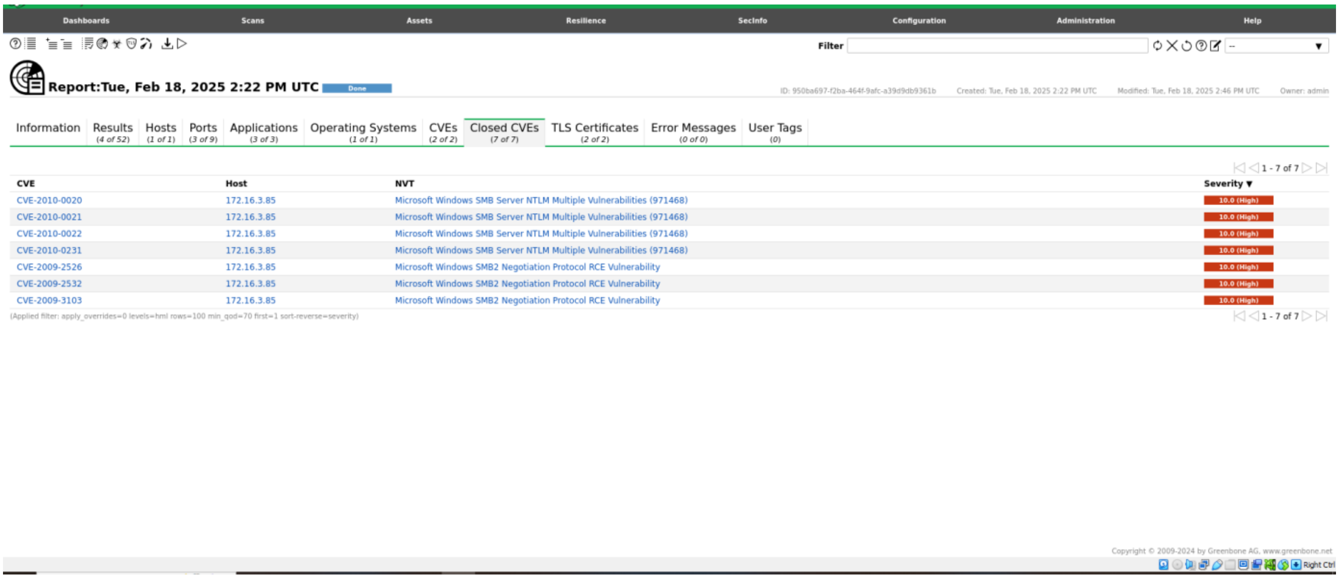


Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	1	7.5 (High)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	2	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

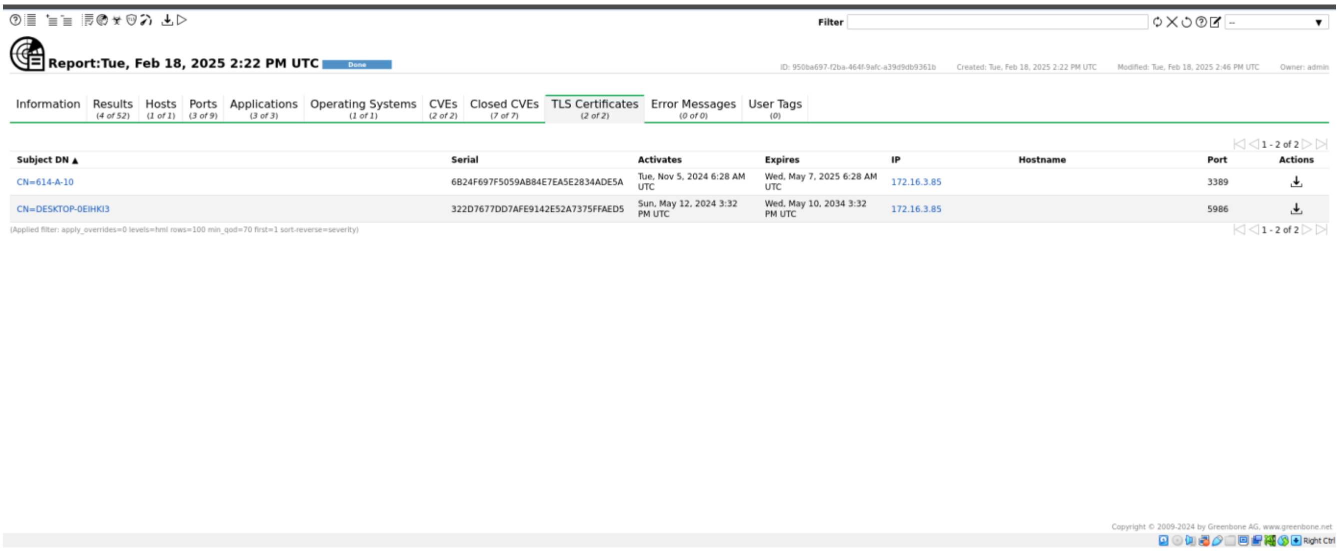


Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

CVE	Host	NVT	Severity ▼
CVE-2010-0020	172.16.3.85	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0021	172.16.3.85	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0022	172.16.3.85	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0231	172.16.3.85	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2009-2526	172.16.3.85	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)
CVE-2009-2532	172.16.3.85	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)
CVE-2009-3103	172.16.3.85	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)



Report:Tue, Feb 18, 2025 2:22 PM UTC

ID: 950ba697-f2ba-464f-9afc-a39d9db9361b Created: Tue, Feb 18, 2025 2:22 PM UTC Modified: Tue, Feb 18, 2025 2:46 PM UTC Owner: admin

Subject DN ▲	Serial	Activates	Expires	IP	Hostname	Port	Actions
CN=614-A-10	6B24F697F5059AB84E7EA5E2834ADE5A	Tue, Nov 5, 2024 6:28 AM UTC	Wed, May 7, 2025 6:28 AM UTC	172.16.3.85		3389	⤓
CN=DESKTOP-0EIHKI3	322D7677DD7AFE9142E52A7375FFAED5	Sun, May 12, 2024 3:32 PM UTC	Wed, May 10, 2034 3:32 PM UTC	172.16.3.85		5986	⤓

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

LATEST APPLICATIONS:

- Enterprise IT Security
- Cloud Security
- IoT (Internet of Things) Security
- Compliance Auditing
- Penetration Testing and Ethical Hacking
- Managed Security Service Providers (MSSPs)
- Incident Response and Forensics
- Security Automation Platforms
- Educational Institutions and Training
- Government and Defense Organizations

LEARNING OUTCOME:

In this practical, we use OpenVAS to perform vulnerability scans, analyze results, and apply security measures to protect systems from threats.

REFERENCES:

1. Open VAS: https://www.openvas.org/
2. GFG: https://www.geeksforgeeks.org/security-assessment-openvas/
3. Green bone: https://greenbone.github.io/docs/latest/22.4/kali/index.html