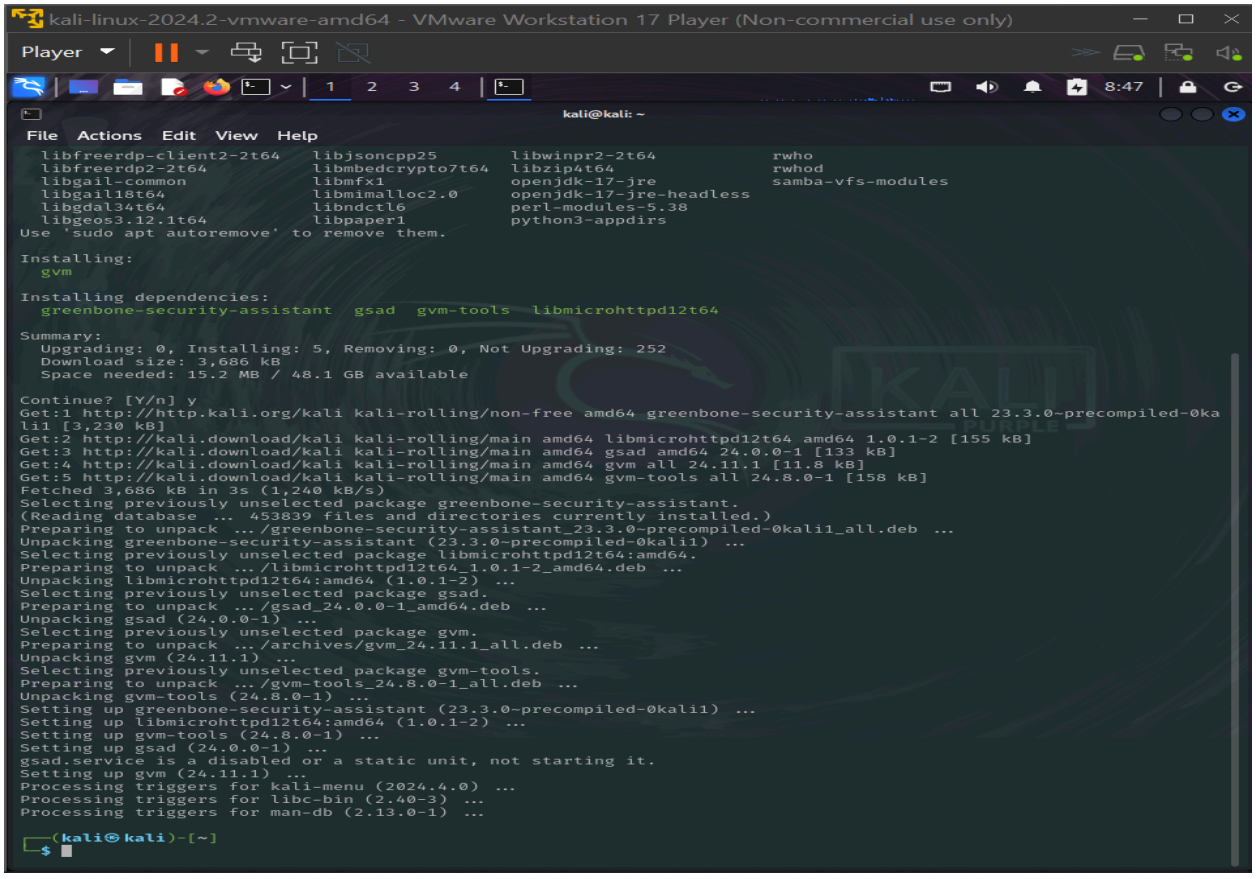
PERFORMING A NETWORK VULNERABILITY SCAN WITH OPENVAS

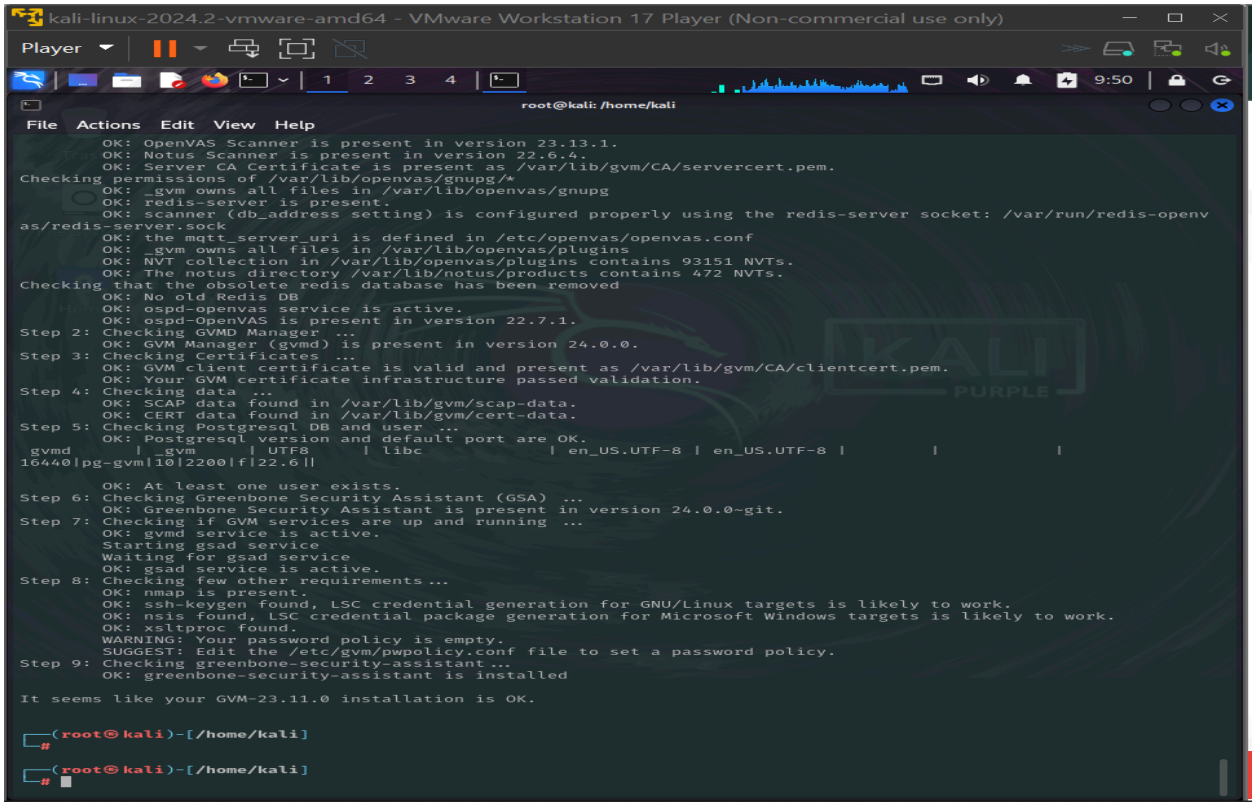
Tools : KALI LINUX

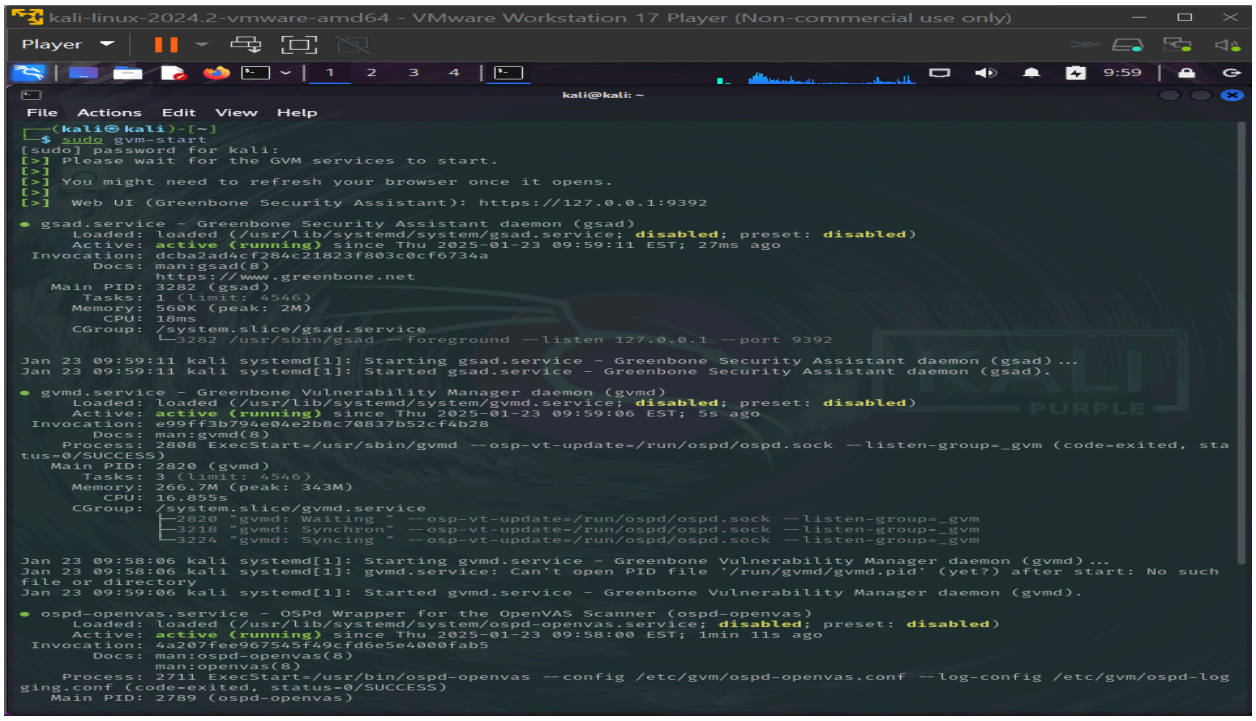
Site : https://127.0.0.1:9392

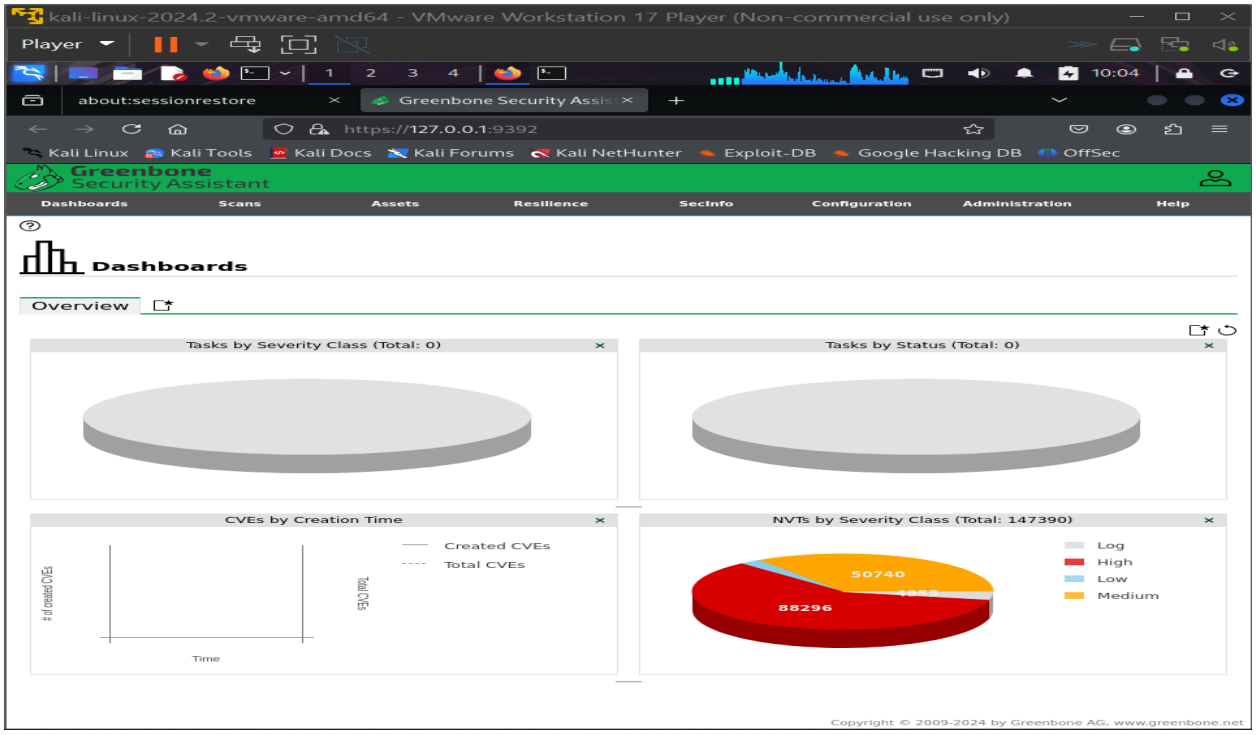
OpenVAS (Open Vulnerability Assessment System) is an open-source framework for vulnerability scanning and management. It's part of the Greenbone Vulnerability Manager (GVM) suite, often used to assess systems for vulnerabilities and ensure network security.

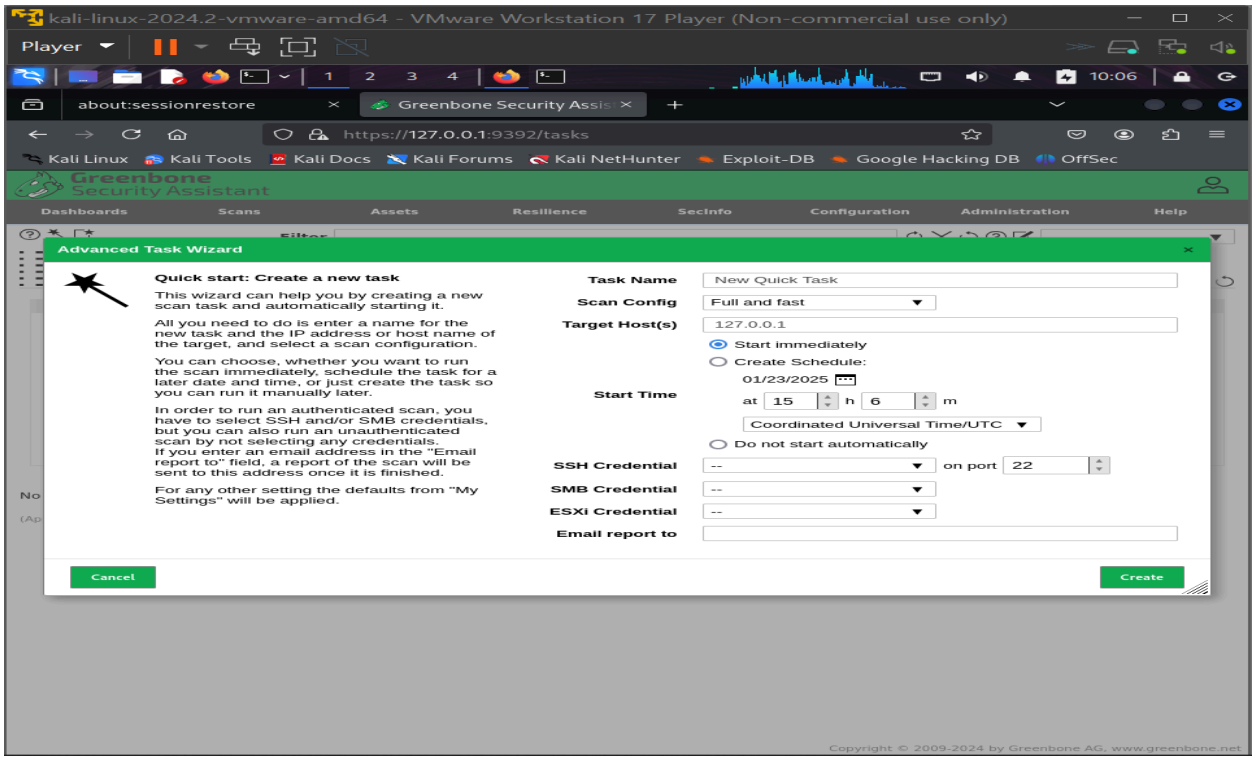
Input from kali :

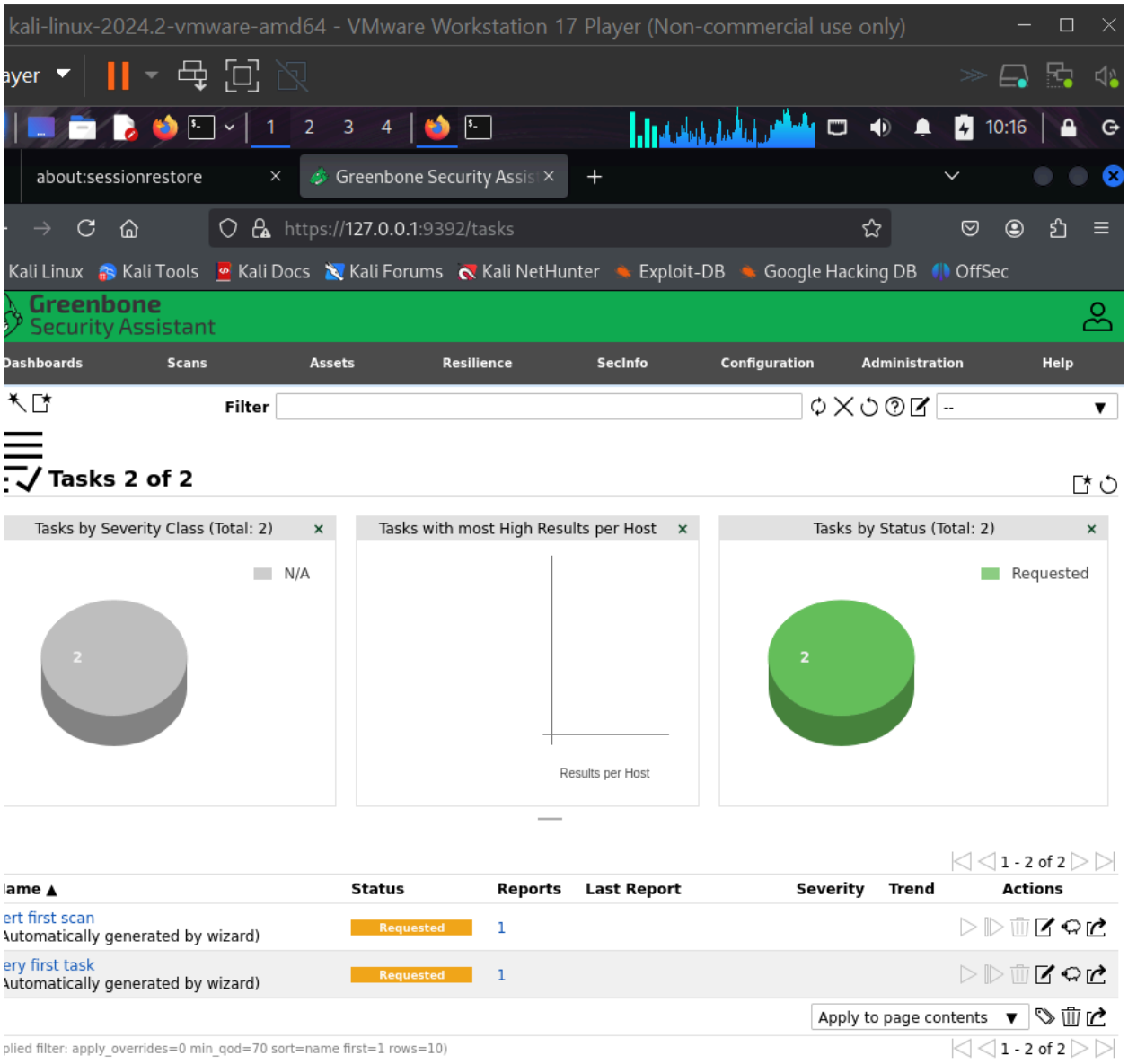



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
9:50
root@kali: /home/kali
File Actions Edit View Help
OK: OpenVAS Scanner is present in version 23.13.1.
OK: Notus Scanner is present in version 22.6.4.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
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-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 93151 NVTs.
OK: The notus directory /var/lib/notus/products contains 472 NVTs.
Checking that the obsolete redis database has been removed
OK: No old Redis DB
OK: ospd-openvas service is active.
OK: ospd-OpenVAS is present in version 22.7.1.
Step 2: Checking GVMD Manager ...
OK: GVM Manager (gvmd) is present in version 24.0.0.
Step 3: Checking Certificates ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.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.
Step 5: Checking Postgresql DB and user ...
OK: Postgresql version and default port are OK.
gvmd | _gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | |
16440|pg-gvm|10|2200|f|22.6||
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 24.0.0~git.
Step 7: Checking if GVM services are up and running ...
OK: gvmd service is active.
Starting gsad service
Waiting for gsad service
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.
(root@kali)-[/home/kali]
#
(root@kali)-[/home/kali]
#


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
9:59
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo gvm-start
[sudo] password for kali:
[>] 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 Thu 2025-01-23 09:59:11 EST; 27ms ago
Invocation: dcba2ad4cf284c21823f803c0cf6734a
Docs: man:gsad(8)
https://www.greenbone.net
Main PID: 3282 (gsad)
Tasks: 1 (limit: 4546)
Memory: 560K (peak: 2M)
CPU: 18ms
CGroup: /system.slice/gsad.service
└─3282 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
Jan 23 09:59:11 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Jan 23 09:59:11 kali 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)
Active: active (running) since Thu 2025-01-23 09:59:06 EST; 5s ago
Invocation: e99ff3b794e04e2b8c70837b52cf4b28
Docs: man:gvmd(8)
Process: 2808 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
Main PID: 2820 (gvmd)
Tasks: 3 (limit: 4546)
Memory: 266.7M (peak: 343M)
CPU: 16.855s
CGroup: /system.slice/gvmd.service
├─2820 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
├─3218 "gvmd: Synchron" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
└─3224 "gvmd: Syncing " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
Jan 23 09:58:06 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Jan 23 09:58:06 kali systemd[1]: gvmd.service: Can't open PID file '/run/gvmd/gvmd.pid' (yet?) after start: No such file or directory
Jan 23 09:59:06 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
Active: active (running) since Thu 2025-01-23 09:58:00 EST; 1min 11s ago
Invocation: 4a207fee967545f49cfd6e5e4000fab5
Docs: man:ospd-openvas(8)
man:openvas(8)
Process: 2711 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
Main PID: 2789 (ospd-openvas)


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
10:04
about:sessionrestore
Greenbone Security Assis
https://127.0.0.1:9392
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
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
Created CVEs
Total CVEs
# of created CVEs
Total CVEs
Time
NVTs by Severity Class (Total: 147390)
50740
88296
Log
High
Low
Medium
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
10:06
about:sessionrestore
Greenbone Security Assis
https://127.0.0.1:9392/tasks
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Advanced Task Wizard
Quick start: Create a new task
This wizard can help you by creating a new scan task and automatically starting it.
All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.
You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.
In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.
If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.
For any other setting the defaults from "My Settings" will be applied.
Task Name
New Quick Task
Scan Config
Full and fast
Target Host(s)
127.0.0.1
Start immediately
Create Schedule:
Start Time
01/23/2025
at 15 h 6 m
Coordinated Universal Time/UTC
Do not start automatically
SSH Credential
on port 22
SMB Credential
ESXi Credential
Email report to
Cancel
Create
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
about:sessionrestore
Greenbone Security Assis
https://127.0.0.1:9392/tasks
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
N/A
2
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 2)
Requested
2
1 - 2 of 2
lame ▲
Status
Reports
Last Report
Severity
Trend
Actions
ert first scan
Automatically generated by wizard)
Requested
1
ery first task
Automatically generated by wizard)
Requested
1
Apply to page contents
plied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
1 - 2 of 2
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Here we would be using openvas to perform a quick network vulnerability scan.

Installing and Setting Up OpenVAS (GVM)

Install OpenVAS
Run the following command to install OpenVAS:

```
sudo apt install openvas
```

1.

View Help Screen
Check the help options with:

```
openvas -h
```

2.

Initialize GVM
Since OpenVAS is now Greenbone Vulnerability Manager (GVM), initialize it with:

```
sudo gvm-setup
```

3.
    - This downloads necessary plugins and may take some time.
    - After installation, the terminal will display the admin password. Save this password securely.

Verify Installation
Run the following to ensure the installation is complete:

```
sudo gvm-check-setup
```

4.
    - If everything is OK, reboot your system.

Start GVM
Use the command below to start GVM:

```
sudo gvm-start
```

5.
    - Firefox will launch automatically at `https://127.0.0.1:9392`.
    - Accept the self-signed certificate warning.
    - Login using the username `admin` and the saved password.

Running a Network Vulnerability Scan

1. **Access the Dashboard**
    - Once logged in, hover over the **Scans** tab and click **Tasks**.
2. **Create a Scan Task**
    - Click the wand icon at the top-left corner and select **Advanced Task Wizard**.
    - Provide a name for the task and input your local network's subnet.
    - Click **Create** to initiate the scan.
3. **View Results**
    - After the scan completes, hover over the **Scans** tab and select **Results**.
    - Review the vulnerabilities and their detailed descriptions, including remediation steps.