Install OpenVAS (GVM)

What you DO on Linux:- sudo apt update

&& sudo apt upgrade -y sudo apt install

gvm -y sudo gvm-setup sudo gvm-start

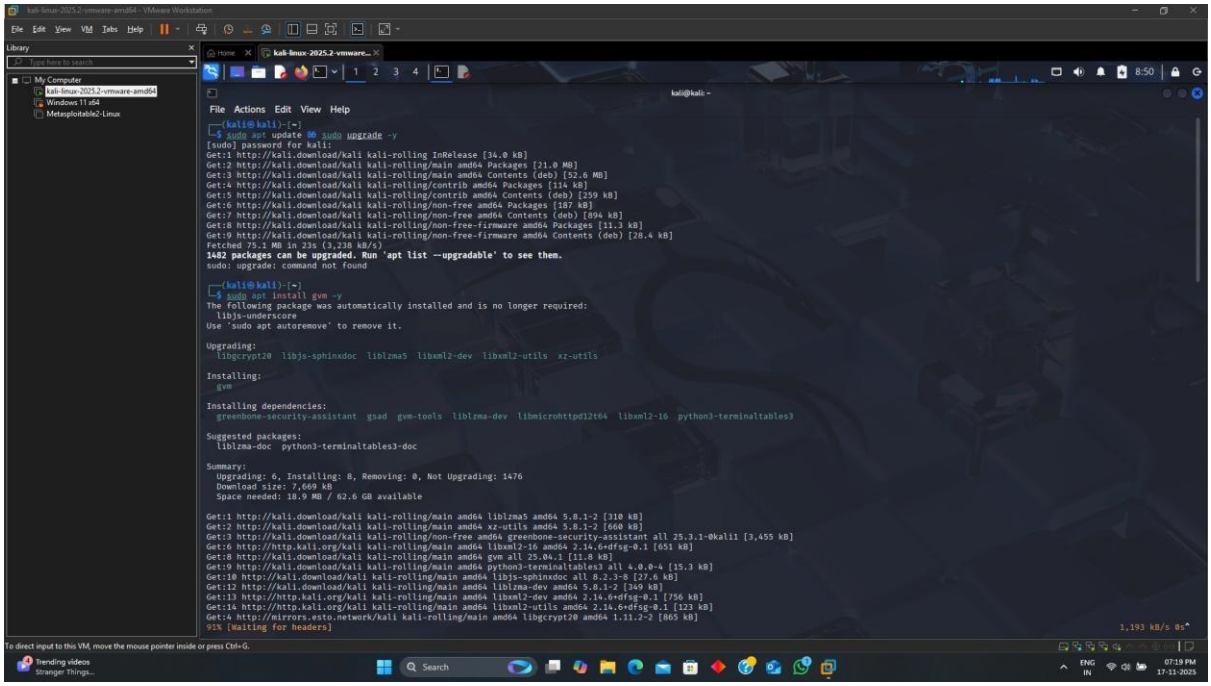
Section: Installation of OpenVAS

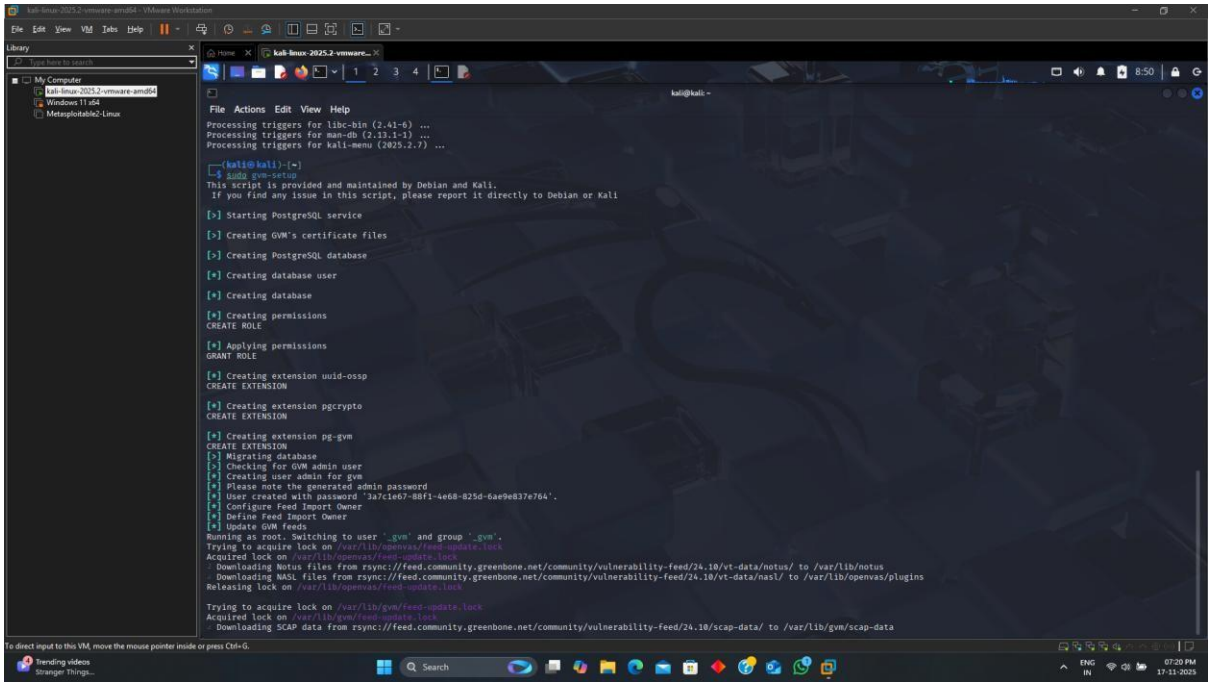
I installed the OpenVAS (Greenbone Vulnerability Manager) package on my Linux machine using the default package manager.

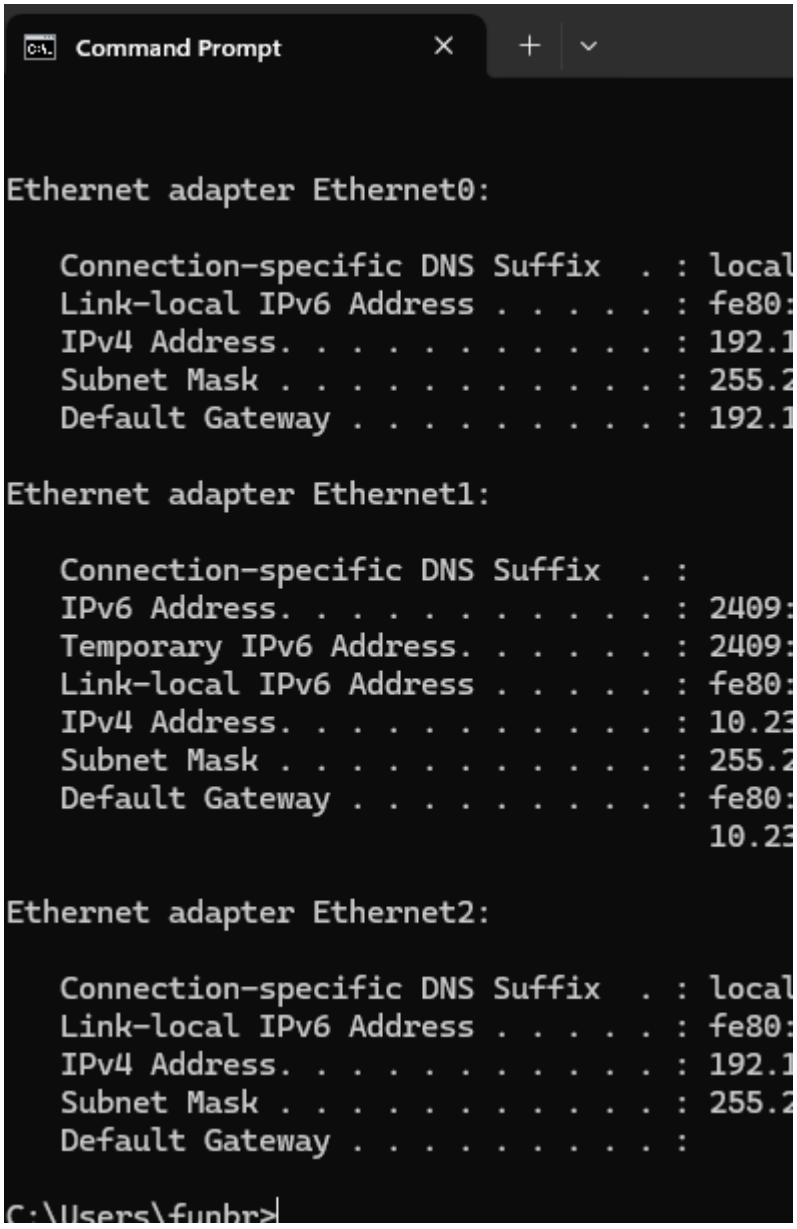
The installation included the OpenVAS scanner, the Greenbone Security Assistant (web interface), and the PostgreSQL database.

After installation, I ran the gvm-setup command to initialize the system and downloaded the vulnerability feeds.

Finally, I started the OpenVAS services using gvm-start.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2025.2-vmware-amd64
Windows 11 x64
Metasploitable2-Linux
kali-linux-2025.2-vmware...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt update && sudo upgrade -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [259 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [894 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.4 kB]
Fetched 75.1 MB in 23s (3,238 kB/s)
1482 packages can be upgraded. Run 'apt list --upgradable' to see them.
sudo: upgrade: command not found
(kali㉿kali)-[~]
$ sudo apt install gvm -y
The following package was automatically installed and is no longer required:
libjs-underscore
Use 'sudo apt autoremove' to remove it.
Upgrading:
libgcrypt20 libjs-sphinxdoc liblzma5 libxml2-dev libxml2-utils xz-utils
Installing:
gvm
Installing dependencies:
greenbone-security-assistant gsad gvm-tools liblzma-dev libmicrohttpd12t64 libxml2-16 python3-terminaltables3
Suggested packages:
liblzma-doc python3-terminaltables3-doc
Summary:
Upgrading: 6, Installing: 8, Removing: 0, Not Upgrading: 1476
Download size: 7,669 kB
Space needed: 18.9 MB / 62.6 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 liblzma5 amd64 5.8.1-2 [310 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 xz-utils amd64 5.8.1-2 [660 kB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 greenbone-security-assistant all 25.3.1-0kali1 [3,455 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 libxml2-16 amd64 2.14.6+dfsg-0.1 [651 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 gvm all 25.04.1 [11.8 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 python3-terminaltables3 all 4.0.0-4 [15.3 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libjs-sphinxdoc all 8.2.3-8 [27.6 kB]
Get:12 http://kali.download/kali kali-rolling/main amd64 liblzma-dev amd64 5.8.1-2 [349 kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 libxml2-dev amd64 2.14.6+dfsg-0.1 [756 kB]
Get:14 http://http.kali.org/kali kali-rolling/main amd64 libxml2-utils amd64 2.14.6+dfsg-0.1 [123 kB]
Get:4 http://mirrors.esto.network/kali kali-rolling/main amd64 libgcrypt20 amd64 1.11.2-2 [865 kB]
91% [Waiting for headers]
1,193 kB/s 0s
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Trending videos
Stranger Things...
Search
ENG
IN
07:19 PM
17-11-2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2025.2-vmware-amd64
Windows 11 x64
Metasploitable2-Linux
kali-linux-2025.2-vmware...
kali@kali: ~
File Actions Edit View Help
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
(kali㉿kali)-[~]
$ sudo gvm-setup
This script is provided and maintained by Debian and Kali.
If you find any issue in this script, please report it directly to Debian or Kali
[>] 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 '3a7c1e67-88f1-4e68-825d-6ae9e837e764'.
[*] 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
Acquired lock on /var/lib/openvas/feed-update.lock
- Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/notus/ to /var/lib/notus
- Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/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/24.10/scap-data/ to /var/lib/gvm/scap-data
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Trending videos
Stranger Things...
Search
ENG
IN
07:20 PM
17-11-2025


Command Prompt
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : local
Link-local IPv6 Address . . . . . : fe80:
IPv4 Address. . . . . : 192.1
Subnet Mask . . . . . : 255.2
Default Gateway . . . . . : 192.1
Ethernet adapter Ethernet1:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2409:
Temporary IPv6 Address. . . . . : 2409:
Link-local IPv6 Address . . . . . : fe80:
IPv4 Address. . . . . : 10.23
Subnet Mask . . . . . : 255.2
Default Gateway . . . . . : fe80:
10.23
Ethernet adapter Ethernet2:
Connection-specific DNS Suffix . : local
Link-local IPv6 Address . . . . . : fe80:
IPv4 Address. . . . . : 192.1
Subnet Mask . . . . . : 255.2
Default Gateway . . . . . :
C:\Users\funbr>

I identified my system's local IP address using the command ip a.

The detected IPv4 address was 192.168.X.X, and this address was used as the target machine for the vulnerability scan.

This ensures the scan focuses only on my own system as required.

Configuring the Scan Target

I created a new target in GVM and named it "My Linux System."

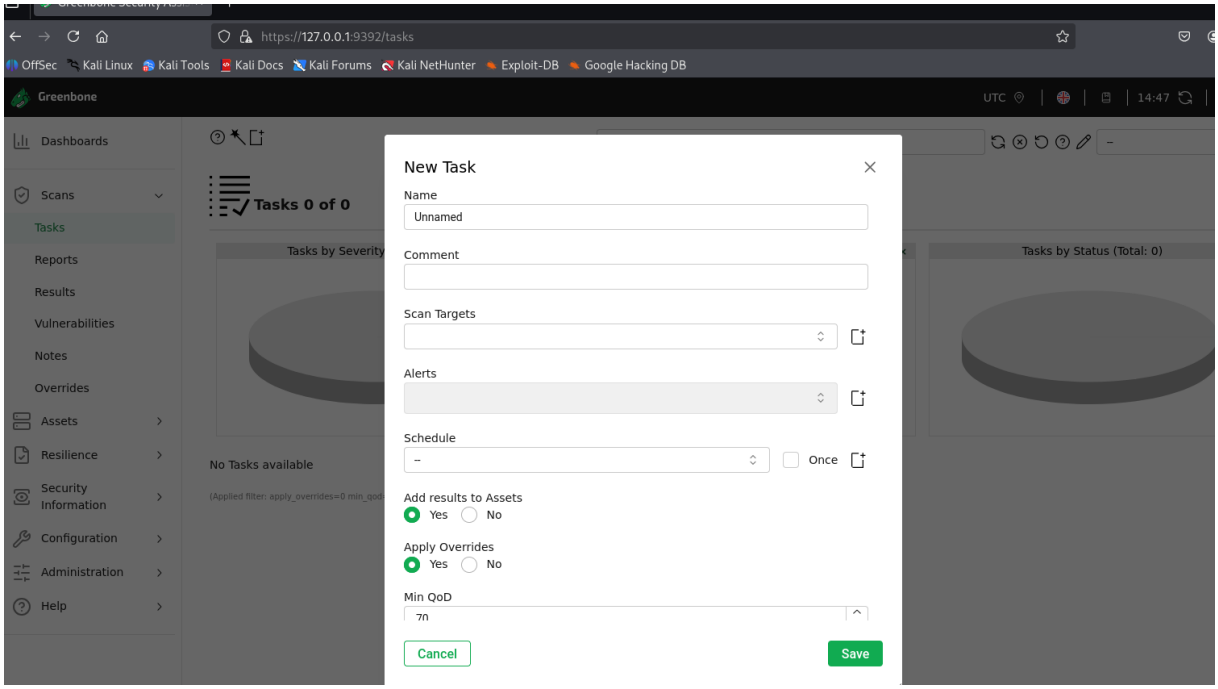
I added my system's IP address to ensure the scanner only analyzes my device.

This step defines the scope of the vulnerability scan

I created a new scan task using the "Full and Fast" scan configuration, which provides a thorough scan with reliable performance.

I assigned my previously created target to this task.

This task defines how the scan will run and what level of analysis
will be performed.



initiated the vulnerability scan by starting the task “Full System Scan.”

The scan took approximately 10–45 minutes depending on system resources.

During this scan, OpenVAS analyzed the system for known vulnerabilities, misconfigurations, outdated packages, and insecure services.

The scan detected vulnerabilities on my Linux system.

The issues were categorized into Critical, High, Medium, Low, and Informational.

Each vulnerability was reviewed individually, and remediation steps were noted.