



OpenVAS S.O.P.

By: Cpl Jimenez

3rd PLT DCO-IDM

LU: 20231117

This document will serve as the guide to OpenVAS installation and usage for operations.

| | |
|---------------------------|---|
| OpenVAS Overview..... | 1 |
| OpenVAS Installation..... | 2 |
| OpenVAS Set-Up..... | 2 |
| OpenVAS Baselining..... | 2 |

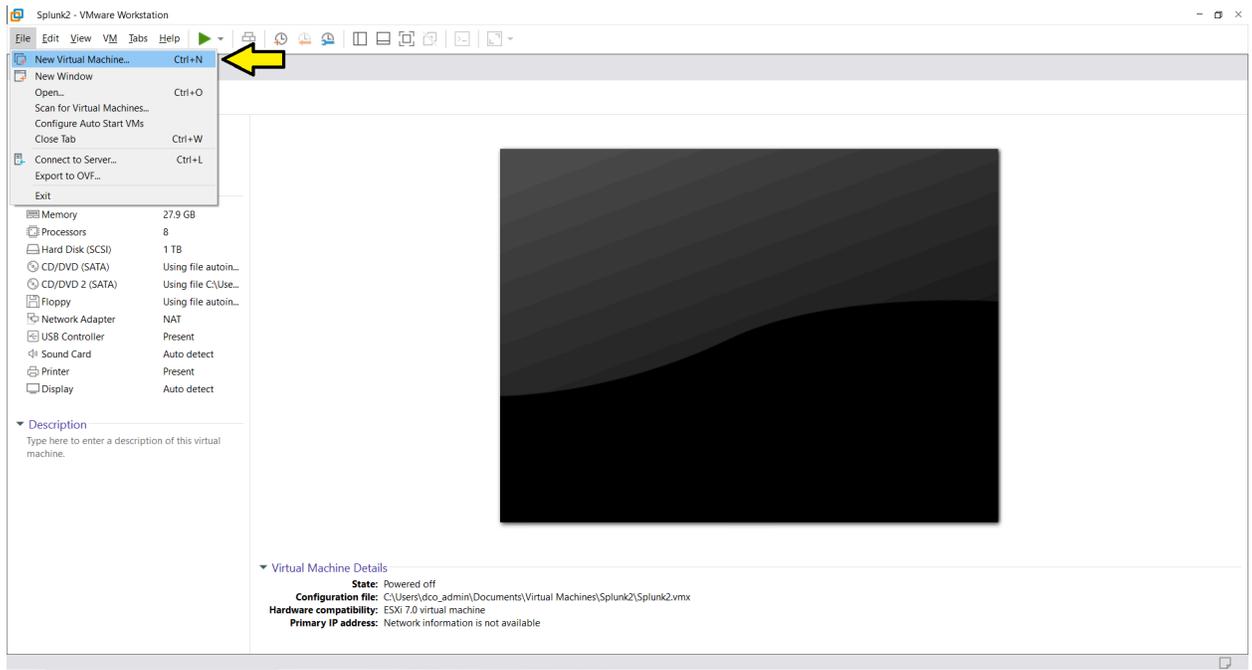
OpenVAS Overview

OpenVAS is an open source Linux-based vulnerability scanner. The intent of OpenVAS usage is to scan the network for vulnerabilities and thereby become aware of certain weaknesses in the network, which can then be turned into an RFI request. You can schedule scans as well so that you always have a relatively recent scan that has up to date information regarding the network. In our network, we typically install it on top of a Kali VM, which itself is hosted on ESXI which is on a CyberPac. Once properly configured, you can launch OpenVAS either via the Terminal or the browser. The terminal method requires you to type in the **'gvm-start'** command (which must be run as sudo) to start the openvas daemon. The browser method will require you to type in **https://127.0.0.1:9392** into the URL bar. Make sure you prepend the url with **https://** otherwise it will not work if you simply type in 127.0.0.1:9392. Note that OpenVAS installation will not work at all if your VM isn't connected to the internet. Also keep in mind that without a license, OpenVAS only lets you scan networks up to a size of /20. If you need to scan a network larger than that, you will have to subnet and create multiple target profiles.

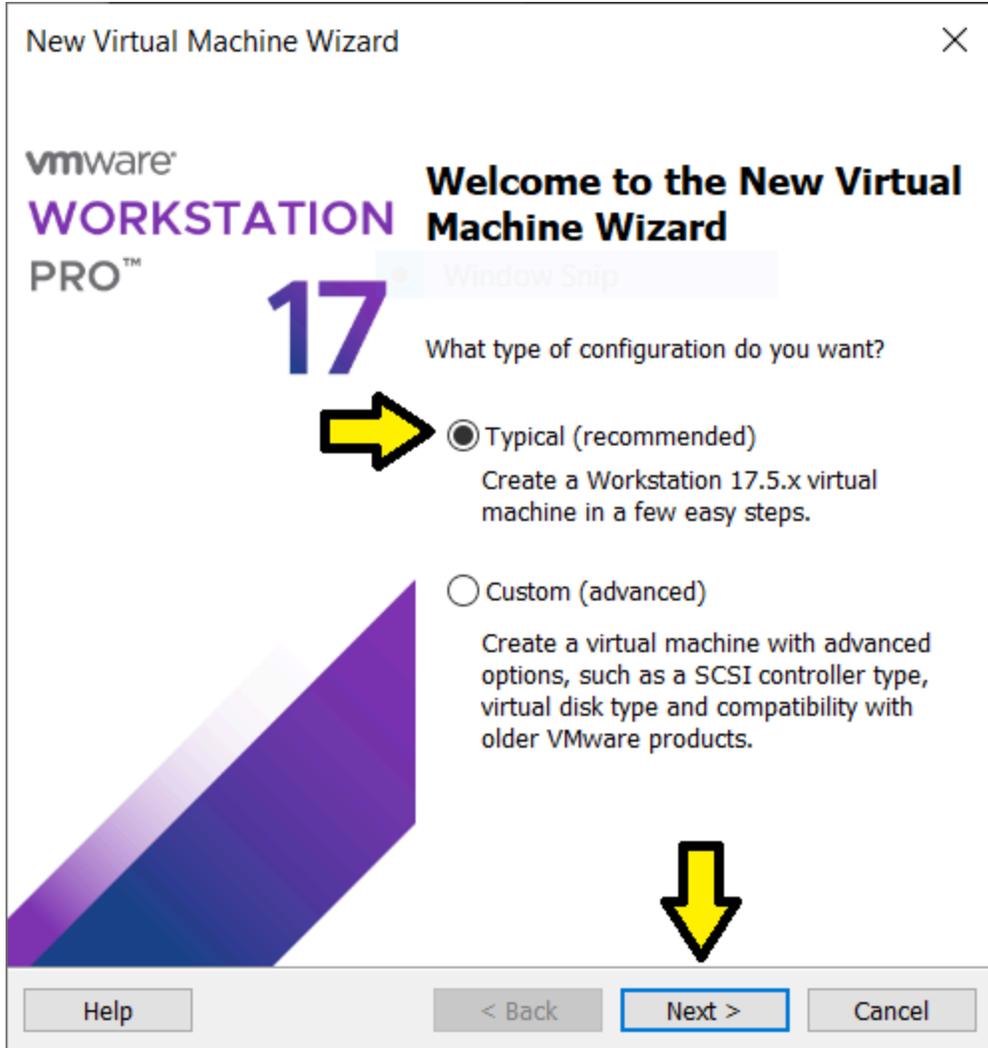


OpenVAS (and Kali Linux) Installation

- ❖ *****Make sure you build your VM on VMWare Workstation Pro*****
 - ESXI doesn't play nice with .ova's generated from VirtualBox
- ❖ Start with a fresh Kali Linux image (Installation instructions below)
- ❖ Open up VMWare Workstation Pro and select File -> New Virtual Machine



- ❖
- ❖ Select 'Typical Installation'



- ❖
- ❖ Next, pick your .iso file's location



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

Window Snip

Installer disc:

No drives available

Installer disc image file (iso):

D:\kali-linux-2022.3-installer-amd64.iso

Browse...

⚠ Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.

I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

- ❖
- ❖ Tell VMWare what operating system you're installing if it hasn't auto-detected it



New Virtual Machine Wizard ✕

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system

Microsoft Windows Window Snip

Linux

VMware ESX

Other

Version

Ubuntu 64-bit



Help < Back Next > Cancel

- ❖
- ❖ Name the virtual machine, and select where it should be saved. The directory you're saving it in should have plenty of space. Keep in mind that the VM itself will be about 70GB when completed.



New Virtual Machine Wizard ✕

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name: Window Snip

Location:

The default location can be changed at Edit > Preferences.

- ❖
- ❖ Make sure that your VM has plenty of space (at least 100GB). You will need a decent chunk of this space in order for the next steps to go smoothly and avoid crashing your VM due to a lack of space. Select 'Store virtual disk as a single file' as well.



New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): ←

Recommended size for Ubuntu 64-bit: 20 GB

Store virtual disk as a single file ←
 Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

↓

Help < Back **Next >** Cancel

- ❖
- ❖ Verify your settings are correct. If they aren't, click on the Customize Hardware button and select the appropriate settings. At least 16GB of memory (more memory = faster scans) and four hyperthreaded cores for eight cores total are required.



New Virtual Machine Wizard

Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Ubuntu 64-bit.

The virtual machine will be created with the following settings:

| | |
|-------------------|---|
| Name: | OpenVAS |
| Location: | C:\Users\dco_admin\Documents\Virtual Machines\Open... |
| Version: | Workstation 17.5.x |
| Operating System: | Ubuntu 64-bit |
| Hard Disk: | 100 GB |
| Memory: | 4096 MB |
| Network Adapter: | NAT |
| Other Devices: | 2 CPU cores, CD/DVD, USB Controller, Sound Card |

Customize Hardware... ←

↓

< Back Finish Cancel





Hardware

| Device | Summary |
|-------------------|------------------------------------|
| Memory | 16 GB |
| Processors | 8 |
| New CD/DVD (SATA) | Using file X:\KaliTest\kali-lin... |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Display | Auto detect |

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 16384 MB

128 GB -
64 GB -
32 GB -
16 GB -
8 GB -
4 GB -
2 GB -
1 GB -
512 MB -
256 MB -
128 MB -
64 MB -
32 MB -
16 MB -
8 MB -
4 MB -

■ Maximum recommended memory
(Memory swapping may occur beyond this size.)
27.9 GB

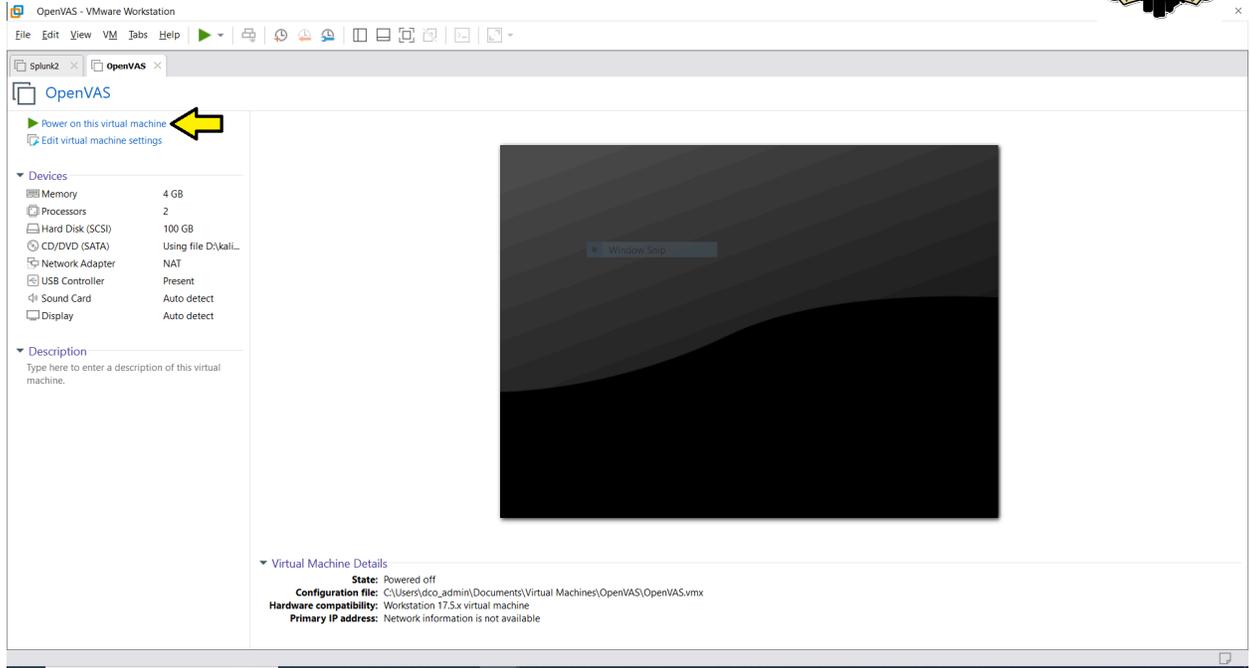
■ Recommended memory
4 GB

■ Guest OS recommended minimum
2 GB

Add... Remove

Close Help

- ❖
- ❖ Next, power on the virtual machine



- ❖
- ❖ When you boot up the machine for the first time, select 'Graphical Install'. This is the GUI guided installation which is much more user-friendly



- ❖
- ❖ Select your system language, keyboard layout and timezone



KALI

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

- | | |
|-----------------------|------------------|
| Chinese (Simplified) | - 中文(简体) |
| Chinese (Traditional) | - 中文(繁體) |
| Croatian | - Hrvatski |
| Czech | - Čeština |
| Danish | - Dansk |
| Dutch | - Nederlands |
| Dzongkha | - ཇོང་ཁཱ་ |
| English | - English |
| Esperanto | - Esperanto |
| Estonian | - Eesti |
| Finnish | - Suomi |
| French | - Français |
| Galician | - Galego |
| Georgian | - ქართული |
| German | - Deutsch |

Screenshot

Go Back

Continue



KALI

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

- India
- Ireland
- Israel
- New Zealand
- Nigeria
- Philippines
- Seychelles
- Singapore
- South Africa
- United Kingdom
- United States**
- Zambia
- Zimbabwe
- other

Screenshot

Go Back

Continue



KALI

Configure the keyboard

Keymap to use:

- American English
- Albanian
- Arabic
- Asturian
- Bangladesh
- Belarusian
- Bengali
- Belgian
- Berber (Latin)
- Bosnian
- Brazilian
- British English
- Bulgarian (BDS layout)
- Bulgarian (phonetic layout)
- Burmese
- Canadian French
- Croatian (Latin)

Screenshot

Go Back Continue

❖ Create a hostname for the machine



KALI

Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:



Screenshot

Go Back

Continue

- ❖
- ❖ Enter a domain if you wish. You can also leave it blank.

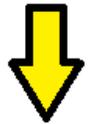


KALI

Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:



Screenshot

Go Back

Continue

- ❖
- ❖ Enter the full name of the primary user



KALI

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:



Screenshot

Go Back

Continue

- ❖
- ❖ Create a username for the machine



KALI

Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:



Screenshot

Go Back

Continue

- ❖
- ❖ Configure your passwords. For simplicity's sake, I use the Kali default username/password of kali/kali



KALI

Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

kali

Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

kali

Show Password in Clear

Screenshot

Go Back

Continue

- ❖
- ❖ Set up the system clock



KALI

Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

| |
|--------------|
| Eastern |
| Central |
| Mountain |
| Pacific |
| Alaska |
| Hawaii |
| Arizona |
| East Indiana |
| Samoa |

Screenshot

Go Back

Continue

- ❖
- ❖ Next you will be asked how you want to partition your installation. Stick with the default options
- ❖



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk** ←
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual



Screenshot

Go Back

Continue





Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI33 (0,0,0) (sda) - 107.4 GB VMware, VMware Virtual S



Screenshot

Go Back

Continue





Partition disks

Selected for partitioning:

SCSI33 (0,0,0) (sda) - VMware, VMware Virtual S: 107.4 GB

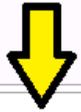
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)

Separate /home partition

Separate /home, /var, and /tmp partitions



Screenshot

Go Back

Continue





KALI

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Guided partitioning

Configure software RAID

Configure the Logical Volume Manager

Configure encrypted volumes

Configure iSCSI volumes

SCSI33 (0,0,0) (sda) - 107.4 GB VMware, VMware Virtual S

| | | | | | | |
|---|----|---------|----------|---|------|------|
| > | #1 | primary | 106.3 GB | f | ext4 | / |
| > | #5 | logical | 1.0 GB | f | swap | swap |

Undo changes to partitions

Finish partitioning and write changes to disk



Screenshot

Help

Go Back

Continue



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI33 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI33 (0,0,0) (sda) as ext4
partition #5 of SCSI33 (0,0,0) (sda) as swap

Write the changes to disks?

No

Yes 



[Screenshot](#)

[Continue](#)

- ❖
- ❖ The system will eventually prompt you to install additional software options. Simply hit continue to continue, unless you want the extra stuff.



KALI

Software selection

At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

Choose software to install:

- Desktop environment [selecting this item has no effect]
- ... Xfce (Kali's default desktop environment)
- ... GNOME
- ... KDE Plasma
- Collection of tools [selecting this item has no effect]
- ... top10 -- the 10 most popular tools
- ... default -- recommended tools (available in the live system)



Screenshot

Continue

- ❖
- ❖ Install the GRUB bootloader



KALI

Install the GRUB boot loader

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to your primary drive?

No

Yes



Screenshot

Go Back

Continue



Install the GRUB boot loader

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Enter device manually

`/dev/sda` ←

↓

Screenshot

Go Back

Continue

- ❖
- ❖ Press Continue to reboot and finish the Kali install



Finish the installation

i *Installation complete*
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.



- ❖
- ❖ Once you boot up into Kali, open up the terminal. You will need to run many of these commands as super user, so use the **'sudo su'** command so that you don't have to preface every command with 'sudo'

```
File Actions Edit View Help
(kali@OpenVAS)-[~]
$ sudo su
[sudo] password for kali:
(root@OpenVAS)-[/home/kali]
#
```

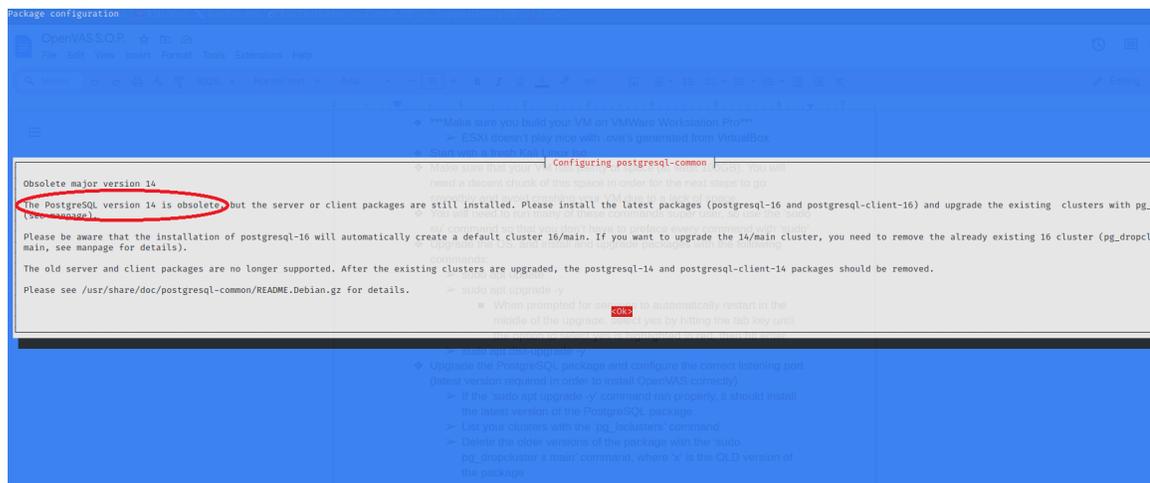
- ❖
- ❖ Upgrade the OS, and install and upgrade packages with the following commands:
 - **sudo apt update -y**
 - **sudo apt upgrade -y**



- When prompted for services to automatically restart in the middle of the upgrade, select yes by hitting the tab key until the option to select yes is highlighted in red, then hit enter.



- You will also be alerted to an obsolete version of the PostgreSQL daemon. This will come into play later.



- **sudo apt dist-upgrade -y**
- You can chain these three command together using '&&' as pictured below

```
(root@OpenVAS)-[/home/kali]
# apt upgrade -y && apt update -y && apt dist-upgrade -y
```

- You will eventually be prompted for what you'd like to do concerning the `/etc/gprofng.rc` file. It isn't really relevant to the OpenVAS installation and you can pick yes or no, it doesn't matter



```
# FILE LOCATIONS

# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/16/main'          # use data in another directory
                                                         # (change requires restart)
hba_file = '/etc/postgresql/16/main/pg_hba.conf'       # host-based authentication file
                                                         # (change requires restart)
ident_file = '/etc/postgresql/16/main/pg_ident.conf'   # ident configuration file
                                                         # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/16-main.pid'  # write an extra PID
                                                         # (change requires restart)

# CONNECTIONS AND AUTHENTICATION

# - Connection Settings -

#listen_addresses = 'localhost'                       # what IP address(es) to listen on;
                                                         # comma-separated list of addresses;
                                                         # defaults to 'localhost'; use '*' for all
                                                         # (change requires restart)
port = 5433                                           # (change requires restart)
max_connections = 100                                 # (change requires restart)
#reserved_connections = 0                             # (change requires restart)
#superuser_reserved_connections = 3                   # (change requires restart)
unix_socket_directories = '/var/run/postgresql'       # comma-separated list of directories
                                                         # (change requires restart)
#unix_socket_group = ''                               # (change requires restart)
#unix_socket_permissions = 0777                      # begin with 0 to use octal notation
                                                         # (change requires restart)
#bonjour = off                                        # advertise server via Bonjour
                                                         # (change requires restart)
#bonjour_name = ''                                   # defaults to the computer name
                                                         # (change requires restart)
```

```
(root@OpenVAS)-[/home/kali]
# pg_ctlcluster 16 main start

(root@OpenVAS)-[/home/kali]
# service postgresql restart
```

❖ Install OpenVAS with the **'sudo apt install openvas'** command



automatically generate a password for this account which is displayed in the last section of the setup output

- ❖ Verify that everything installed correctly by running the **'sudo gvm-check-setup'** command. If something did not install correctly, this command gives you instructions as to what to run to fix the issue(s).

```
root@OpenVAS: /etc/postgresql/16/main
File Actions Edit View Help
└─* gvm-check-setup [Desktop/ventoy-1.0.96 X] [Full OpenVAS -- Desktop/ventoy-1.0.96 X]
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner) ...
OK: OpenVAS Scanner is present in version 22.7.5.
OK: Notus Scanner is present in version 22.6.0.
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 87063 NVTs.
OK: The notus directory /var/lib/notus/products contains 451 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 22.6.0.
Step 2: Checking GVMd Manager ...
OK: GVM Manager (gvm) is present in version 22.9.0.
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.
gvm | _gvm | UTF8 | libc | en_US.UTF-8 | en_US.UTF-8 | | |
16436|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 22.06.0-git.
Step 7: Checking if GVM services are up and running ...
Starting gvm service
Waiting for gvm service
OK: gvm 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-22.5.0 installation is OK.
```

- ❖ Once you have verified that the installation is good, start the OpenVAS daemon with the **'sudo gvm-start'** command (if the OpenVAS daemon and the web interface didn't start upon completion of the 'gvm-setup' command). If this command isn't run, OpenVAS will not work and you will not be able to access it at all.
- ❖ If you want to change the password use the **'sudo gvm --user=admin --new-password=<passwd>'**
 - If the above command doesn't work, try **'sudo -E -u _gvm gvm --user=admin --new-password=admin'**



- ❖ Shut down the VM and export it into an .ova format so you can put it onto ESXI.

OpenVAS Set-Up

Before you start scanning, you need to make target profiles. You can do this either by going to Configuration -> Targets or by going to the Scans -> Tasks tab and creating a new task and then making the target profile from there. The below screenshot shows the easier option; Configuration -> Targets

It is best practice to name the target profile after the subnet you are scanning (for example, 10.1.5.11-10.1.5.20). Make sure that you do **NOT** put spaces in the subnet range when you are specifying it under the manual option. You can also specify multiple specific IPs by putting them in a .csv file and selecting the “from file” option. If you are using this option, put only one IP per line, like so:

10.1.5.11
10.1.4.22
10.1.3.33

The screenshot shows the Greenbone Security Assistant (GSA) web interface. The main page displays a list of targets, with one target named '10.1.5.0-10.1.5.11'. A 'New Target' dialog box is open, allowing the user to create a new target profile. The dialog box contains the following fields and options:

- Name:** 10.1.5.11-10.1.5.20
- Comment:** (empty)
- Hosts:** Manual 10.1.5.11-10.1.5.20; From file [Browse...] No file selected.
- Exclude Hosts:** Manual (empty); From file [Browse...] No file selected.
- Allow simultaneous scanning via multiple IPs:** Yes; No
- Port List:** All IANA assigned TCP ar
- Alive Test:** ICMP & TCP-ACK Service
- Credentials for authenticated checks:** SSH -- on port 22; SMB --

The 'Save' button is highlighted in green, indicating it is the primary action.

In order to run your scans, click on the play button on the right hand side of the screen. You can also pause, stop, delete, edit, clone or export your



scans. These buttons are in the middle right of the screen, under the **TASKS** tab, as pictured below:

| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|-----------|--------|---------|-------------|----------|-------|---------|
| Test Scan | New | | | | | |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Once your scans are done, you can view the associated report by clicking on the date under the Last Report section.

-Alternatively, if you want to view earlier reports, click on the number of reports, and then click on the report you wish to see.

-Once you pull up a report, you can view specific results like what hosts the scan found, what ports are open, and what CVEs it caught by navigating to the specific tab. Alternatively, you may find the 'Corresponding Results' and 'Corresponding Vulnerabilities' sections useful. These are the buttons in the upper left hand corner shaped like a radar and a biohazard icon respectively.

Screenshot depicting how to pull up the most recent report:



Tasks 1 of 1

Tasks by Severity Class (Total: 1)

Tasks with most High Results per Host

Tasks by Status (Total: 1)

| Name | Status | Reports | Last Report | Severity | Trend | Actions |
|-----------|--------|---------|---|--------------|-------|---------|
| Test Scan | Done | 1 | Tue, Nov 7, 2023 11:03 AM EST | 5.8 (Medium) | | |

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=100)

<https://127.0.0.1:9392/report/13cc83cf-93ff-42de-afb4-6dc33f60c7b9>

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Screenshot depicting Results tab once the report has been pulled up:

Report: Tue, Nov 7, 2023 11:03 AM EST

ID: 13cc83cf-93ff-42de-afb4-6dc33f60c7b9 Created: Tue, Nov 7, 2023 11:03 AM EST Modified: Tue, Nov 7, 2023 1:15 PM EST Owner: admin

| Information | Results (16 of 121) | Hosts (3 of 3) | Ports (5 of 8) | Applications (2 of 2) | Operating Systems (3 of 3) | CVEs (4 of 4) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (8 of 8) | User Tags (0) |
|---|---------------------|----------------|----------------|-----------------------|----------------------------|-------------------------------|----------------------|---------------------------|-------------------------|---------------|
| Vulnerability | Severity | QoD | Host IP | Name | Location | Created | | | | |
| SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555) | 5.8 (Medium) | 70 % | 10.1.5.11 | | 9080/tcp | Tue, Nov 7, 2023 11:24 AM EST | | | | |
| Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5.3 (Medium) | 80 % | 10.1.5.1 | | 22/tcp | Tue, Nov 7, 2023 12:39 PM EST | | | | |
| SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5.0 (Medium) | 70 % | 10.1.5.11 | | 9080/tcp | Tue, Nov 7, 2023 11:24 AM EST | | | | |
| SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 5.0 (Medium) | 70 % | 10.1.5.11 | | 443/tcp | Tue, Nov 7, 2023 11:24 AM EST | | | | |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 10.1.5.1 | | 80/tcp | Tue, Nov 7, 2023 12:40 PM EST | | | | |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 10.1.5.0 | | 80/tcp | Tue, Nov 7, 2023 11:27 AM EST | | | | |
| Telnet Unencrypted Cleartext Login | 4.8 (Medium) | 70 % | 10.1.5.1 | | 23/tcp | Tue, Nov 7, 2023 12:35 PM EST | | | | |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.3 (Medium) | 98 % | 10.1.5.1 | | 443/tcp | Tue, Nov 7, 2023 12:39 PM EST | | | | |
| SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 4.2 (Medium) | 98 % | 10.1.5.0 | | 443/tcp | Tue, Nov 7, 2023 11:23 AM EST | | | | |
| SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4.0 (Medium) | 80 % | 10.1.5.0 | | 443/tcp | Tue, Nov 7, 2023 11:23 AM EST | | | | |
| SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4.0 (Medium) | 80 % | 10.1.5.1 | | 443/tcp | Tue, Nov 7, 2023 12:39 PM EST | | | | |
| TCP Timestamps Information Disclosure | 2.6 (Low) | 80 % | 10.1.5.0 | | general/tcp | Tue, Nov 7, 2023 11:20 AM EST | | | | |
| TCP Timestamps Information Disclosure | 2.6 (Low) | 80 % | 10.1.5.11 | | general/tcp | Tue, Nov 7, 2023 11:12 AM EST | | | | |
| Weak MAC Algorithm(s) Supported (SSH) | 2.6 (Low) | 80 % | 10.1.5.1 | | 22/tcp | Tue, Nov 7, 2023 12:39 PM EST | | | | |
| ICMP Timestamp Reply Information Disclosure | 2.1 (Low) | 80 % | 10.1.5.0 | | general/icmp | Tue, Nov 7, 2023 11:25 AM EST | | | | |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

This is a screenshot of the associated CVEs pulled from a report. Notice



on the right hand side it depicts the Severity levels and the name of the CVEs so you can do further research on them if required:

The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo', 'Configuration', 'Administration', and 'Help'. Below the navigation bar, there is a report summary for 'Report: Tue, Nov 7, 2023 11:03 AM EST'. The report details include ID: 13cc83cf-93ff-42de-afb4-6dc33f60c7b9, Created: Tue, Nov 7, 2023 11:03 AM EST, Modified: Tue, Nov 7, 2023 1:15 PM EST, and Owner: admin. The report is categorized into several sections: Information (16 of 121), Results (3 of 3), Hosts (5 of 8), Ports (2 of 2), Applications (3 of 3), Operating Systems (4 of 4), CVEs (4 of 4), Closed CVEs (0 of 0), TLS Certificates (4 of 4), Error Messages (8 of 8), and User Tags (0). The CVEs section is highlighted with a yellow arrow. Below the report summary, there is a table of CVEs with columns for CVE, NVT, Hosts, Occurrences, and Severity. The table lists four CVEs: CVE-2009-3555 (Severity 5.8 Medium), CVE-2011-1473 and CVE-2011-5094 (Severity 5.0 Medium), CVE-2011-3389 and CVE-2015-0204 (Severity 4.3 Medium), and CVE-1999-0524 (Severity 2.1 Low). The table also includes a filter bar and pagination controls.

| CVE | NVT | Hosts | Occurrences | Severity |
|-----------------------------|---|-------|-------------|--------------|
| CVE-2009-3555 | SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555) | 1 | 1 | 5.8 (Medium) |
| CVE-2011-1473 CVE-2011-5094 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 1 | 2 | 5.0 (Medium) |
| CVE-2011-3389 CVE-2015-0204 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 2 | 2 | 4.3 (Medium) |
| CVE-1999-0524 | ICMP Timestamp Reply Information Disclosure | 2 | 2 | 2.1 (Low) |

Click here to view the Corresponding Vulnerabilities

The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo', 'Configuration', 'Administration', and 'Help'. Below the navigation bar, there is a report summary for 'Report: Tue, Nov 7, 2023 11:03 AM EST'. The report details include ID: 13cc83cf-93ff-42de-afb4-6dc33f60c7b9, Created: Tue, Nov 7, 2023 11:03 AM EST, Modified: Tue, Nov 7, 2023 1:15 PM EST, and Owner: admin. The report is categorized into several sections: Information (16 of 121), Results (3 of 3), Hosts (5 of 8), Ports (2 of 2), Applications (3 of 3), Operating Systems (4 of 4), CVEs (4 of 4), Closed CVEs (0 of 0), TLS Certificates (4 of 4), Error Messages (8 of 8), and User Tags (0). The CVEs section is highlighted with a yellow arrow. Below the report summary, there is a table of CVEs with columns for CVE, NVT, Hosts, Occurrences, and Severity. The table lists four CVEs: CVE-2009-3555 (Severity 5.8 Medium), CVE-2011-1473 and CVE-2011-5094 (Severity 5.0 Medium), CVE-2011-3389 and CVE-2015-0204 (Severity 4.3 Medium), and CVE-1999-0524 (Severity 2.1 Low). The table also includes a filter bar and pagination controls. A yellow arrow points to the 'Corresponding Vulnerabilities' link in the report summary.

https://127.0.0.1:9392/vulnerabilities?filter=report_id=13cc83cf-93ff-42de-afb4-6dc33f60c7b9



Another object of note is the 'Download Filtered Report' button, which looks like a downward facing arrow pointing into an open box.

Clicking this button will let you download your results into one of several formats. I recommend the .pdf format because it takes all the important information the scan found and formats it into an interactable .pdf file. It has a table of contents, which you can click on to navigate around the document.

Pictured below is where you go to download said reports and the drop down menu to select the PDFs, as well as an example of the report it generates:

The screenshot shows the Greenbone Security Assistant web interface. A yellow arrow points to the 'Download filtered Report' button, which is a downward arrow pointing into a box. Below the button is a table with the following data:

| Information | Results (16 of 121) | Hosts (3 of 3) | Ports (5 of 8) | Applications (2 of 2) | Operating Systems (3 of 3) | CVEs (4 of 4) | Closed CVEs (0 of 0) | TLS Certificates (4 of 4) | Error Messages (8 of 8) | User Tags (0) |
|---------------|--|-------------------|-------------------|--------------------------|-------------------------------|------------------|-------------------------|------------------------------|----------------------------|------------------|
| Task Name | Test Scan | | | | | | | | | |
| Scan Time | Tue, Nov 7, 2023 11:03 AM EST - Tue, Nov 7, 2023 1:15 PM EST | | | | | | | | | |
| Scan Duration | 2:12 h | | | | | | | | | |
| Scan Status | Done | | | | | | | | | |
| Hosts scanned | 3 | | | | | | | | | |
| Filter | apply_overrides=0 levels=hml_min_god=70 | | | | | | | | | |
| Timezone | America/New_York (EST) | | | | | | | | | |



Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Scan Report

November 7, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "America/New_York", which is abbreviated "EST". The task was "Test Scan". The scan started at Tue, Nov 7 11:03:37 2023 EST and ended at Tue, Nov 7 15:39 2023 EST. The report first summarises the results found. Then, for each host, the

Contents

| | | |
|-------|------------------|----|
| 1 | Result Overview | 2 |
| 2 | Results per Host | 2 |
| 2.1 | 10.1.5.11 | 2 |
| 2.1.1 | Medium 443/tcp | 2 |
| 2.1.2 | Medium 9080/tcp | 4 |
| 2.1.3 | Low general/tcp | 9 |
| 2.2 | 10.1.5.1 | 10 |
| 2.2.1 | Medium 443/tcp | 10 |
| 2.2.2 | Medium 80/tcp | 15 |
| 2.2.3 | Medium 23/tcp | 16 |
| 2.2.4 | Medium 22/tcp | 16 |
| 2.2.5 | Low general/icmp | 17 |

Another area of note is under the Assets tab under Hosts. This tab will show you a network map of your host topology which is color coded with their corresponding vulnerabilities' levels. Red is severe, orange is medium, blue is low, and gray is not vulnerable or not applicable. It will also



show you a list of scanned hosts, their IP address, their OS and the CVE severity level.

A picture of the Assets -> Hosts tab and the results:

The screenshot shows the Greenbone Security Assistant interface. The 'Assets' tab is selected, and the 'Hosts' sub-tab is active. A yellow arrow points to the 'Hosts 3 of 3' header. The interface displays three charts and a table of host data.

| Name | Hostname | IP Address | OS | Severity | Modified | Actions |
|-----------|----------|------------|--------|--------------|------------------------------|---------|
| 10.1.5.11 | | 10.1.5.11 | Ubuntu | 5.8 (Medium) | Tue, Nov 7, 2023 1:15 PM EST | ✕ 📄 🔄 |
| 10.1.5.1 | | 10.1.5.1 | Ubuntu | 5.3 (Medium) | Tue, Nov 7, 2023 1:15 PM EST | ✕ 📄 🔄 |
| 10.1.5.0 | | 10.1.5.0 | Ubuntu | 4.8 (Medium) | Tue, Nov 7, 2023 1:15 PM EST | ✕ 📄 🔄 |

Further areas of interest are under SecInfo->NVTs, SecInfo->CVEs, Scans->Reports, Scans->Results and Scans->Vulnerabilities.

A picture of SecInfo -> NVTs



| Name | Family | Created | Modified | CVE | Severity | QoD |
|--|------------------------------|--------------------------------|--------------------------------|---|--------------|------|
| Ubuntu: Security Advisory (USN-6456-1) | Ubuntu Local Security Checks | Mon, Oct 30, 2023 4:50 AM EDT | Mon, Oct 30, 2023 4:50 AM EDT | CVE-2023-5721 CVE-2023-5722 CVE-2023-5723 CVE-2023-5724 CVE-2023-5725 CVE-2023-5728 CVE-2023-5729 CVE-2023-5730 CVE-2023-5731 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3637) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2023-5721 CVE-2023-5724 CVE-2023-5725 CVE-2023-5728 CVE-2023-5730 CVE-2023-5732 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3635) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2023-46234 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3634) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2020-25648 CVE-2023-4423 | 7.5 (High) | 97 % |

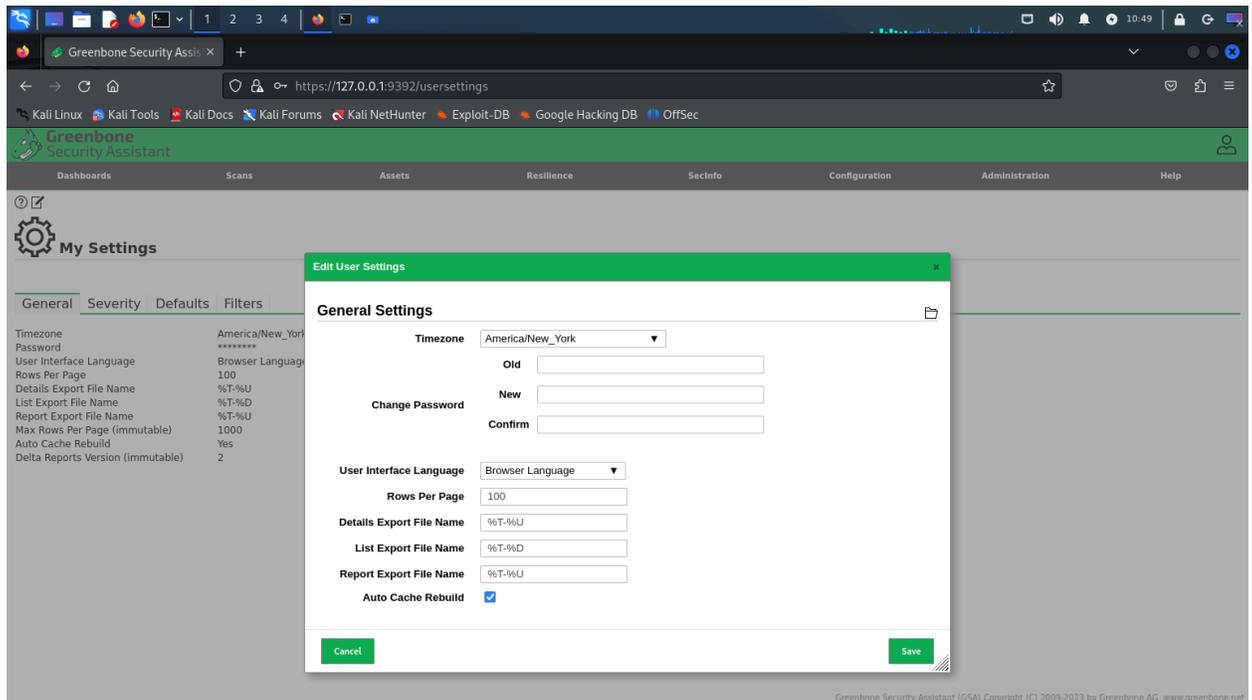
A picture of SecInfo -> CVEs

| Name | Family | Created | Modified | CVE | Severity | QoD |
|--|------------------------------|--------------------------------|--------------------------------|---|--------------|------|
| Ubuntu: Security Advisory (USN-6456-1) | Ubuntu Local Security Checks | Mon, Oct 30, 2023 4:50 AM EDT | Mon, Oct 30, 2023 4:50 AM EDT | CVE-2023-5721 CVE-2023-5722 CVE-2023-5723 CVE-2023-5724 CVE-2023-5725 CVE-2023-5728 CVE-2023-5729 CVE-2023-5730 CVE-2023-5731 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3637) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2023-5721 CVE-2023-5724 CVE-2023-5725 CVE-2023-5728 CVE-2023-5730 CVE-2023-5732 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3635) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2023-46234 | 5.0 (Medium) | 97 % |
| Debian: Security Advisory (DLA-3634) | Debian Local Security Checks | Mon, Oct 30, 2023 12:23 AM EDT | Mon, Oct 30, 2023 12:23 AM EDT | CVE-2020-25648 CVE-2023-4423 | 7.5 (High) | 97 % |

If you need to change the password from the GUI, you can do so by clicking the 'My Settings' icon in the upper right hand corner which looks like a person. Then click the edit settings button in the top left, which looks



like a page with a star on it. From here you can change several options in addition to the password like your timezone and how many rows OpenVAS should display at once when showing results. Click 'Save' to save changes. Pictured below is what it should look like.



OpenVAS Baselining

- ❖ Create a baseline by running your scans at least a few times. You can schedule your scans to run them at specific times. Once you have a few reports generated (around 3 - 5 for each target profile) look at the reports to see if the number of CVEs has changed. This will give you a good idea of what your baseline is.

gvm-check-setup command

Below is a screenshot of the gvm-check-setup command. Notice that the command has failed and notified you that the setup is not complete. When the setup is not good, it will tell you



exactly what commands to run. Keep in mind that the gvm-check-setup command must be run as sudo.

```
File Actions Edit View Help
(root@OpenVAS)-[~] Desktop/ventoy-1.0.96 x kali@OpenVAS: ~/Desktop/ventoy-1.0.96
# gvm-check-setup
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner) ...
    OK: OpenVAS Scanner is present in version 22.7.5.
    OK: Notus Scanner is present in version 22.6.0.
    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 87063 NVTs.
    OK: The notus directory /var/lib/notus/products contains 451 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
    OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
    OK: ospd-openvas service is active.
    OK: ospd-OpenVAS is present in version 22.6.0.
Step 2: Checking GVM Manager ...
    OK: GVM Manager (gvm) is present in version 22.9.0.
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 ...
Starting postgresql service
    OK: PostgreSQL version and default port are OK.
psql: error: connection to server on socket "/var/run/postgresql/.s.PGSQL.5432" failed: No such file or directory
Is the server running locally and accepting connections on that socket?
    ERROR: The PostgreSQL DB does not exist.
    FIX: Run 'sudo runuser -u postgres -- /usr/share/gvm/create-postgresql-database'
ERROR: Your GVM-22.5.0 installation is not yet complete!

Please follow the instructions marked with FIX above and run this script again.
```



Below is an example of a good gvm-check-setup command

```
root@OpenVAS: /etc/postgresql/16/main
File Actions Edit View Help
└─# gvm-check-setup /Desktop/ventoy-1.0.96 X kalla@OpenVAS: ~/Desktop/ventoy-1.0.96 X
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner) ...
  OK: OpenVAS Scanner is present in version 22.7.5.
  OK: Notus Scanner is present in version 22.6.0.
  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 87063 NVTs.
  OK: The notus directory /var/lib/notus/products contains 451 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 22.6.0.
Step 2: Checking GVM Manager ...
  OK: GVM Manager (gvm) is present in version 22.9.0.
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.
  gvm      | _gvm      | UTF8      | libc      | en_US.UTF-8 | en_US.UTF-8 | | |
16436|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 22.06.0-git.
Step 7: Checking if GVM services are up and running ...
  Starting gvm service
  Waiting for gvm service
  OK: gvm 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-22.5.0 installation is OK.
```