OpenVAS S.O.P.

By: Cpl Jimenez
3rd PLT DCO-IDM
LU: 20231117

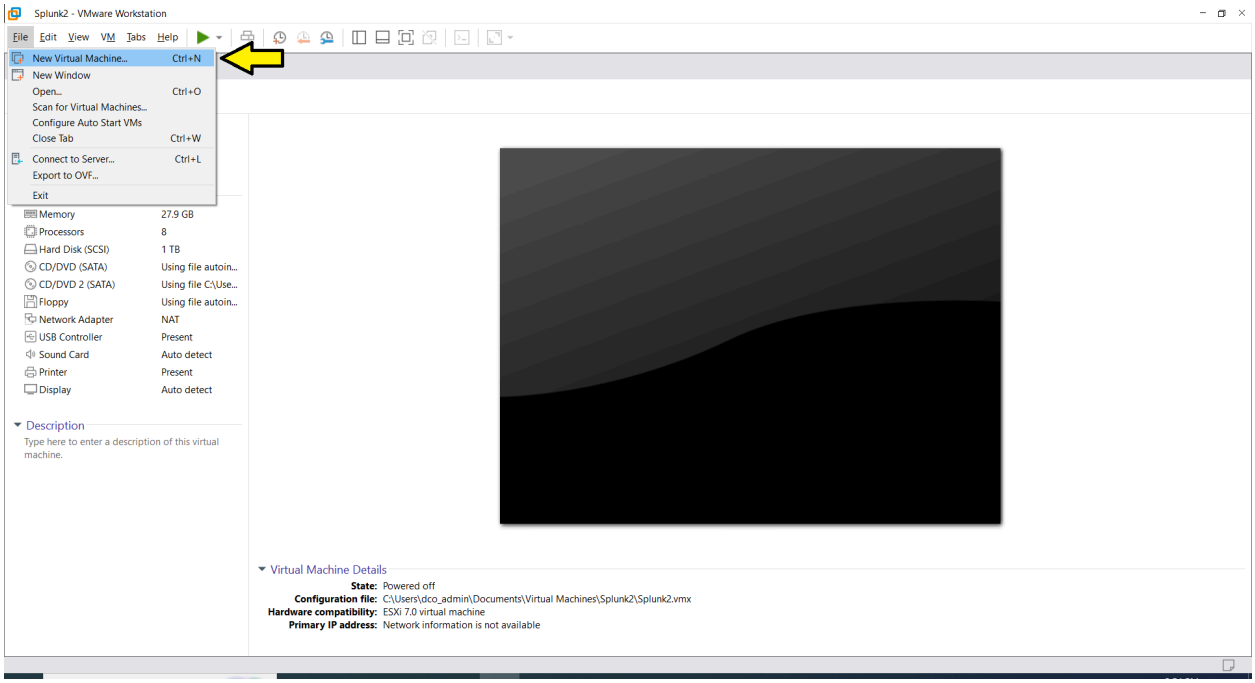
This document will serve as the guide to OpenVAS installation and usage for operations.

OpenVAS Overview

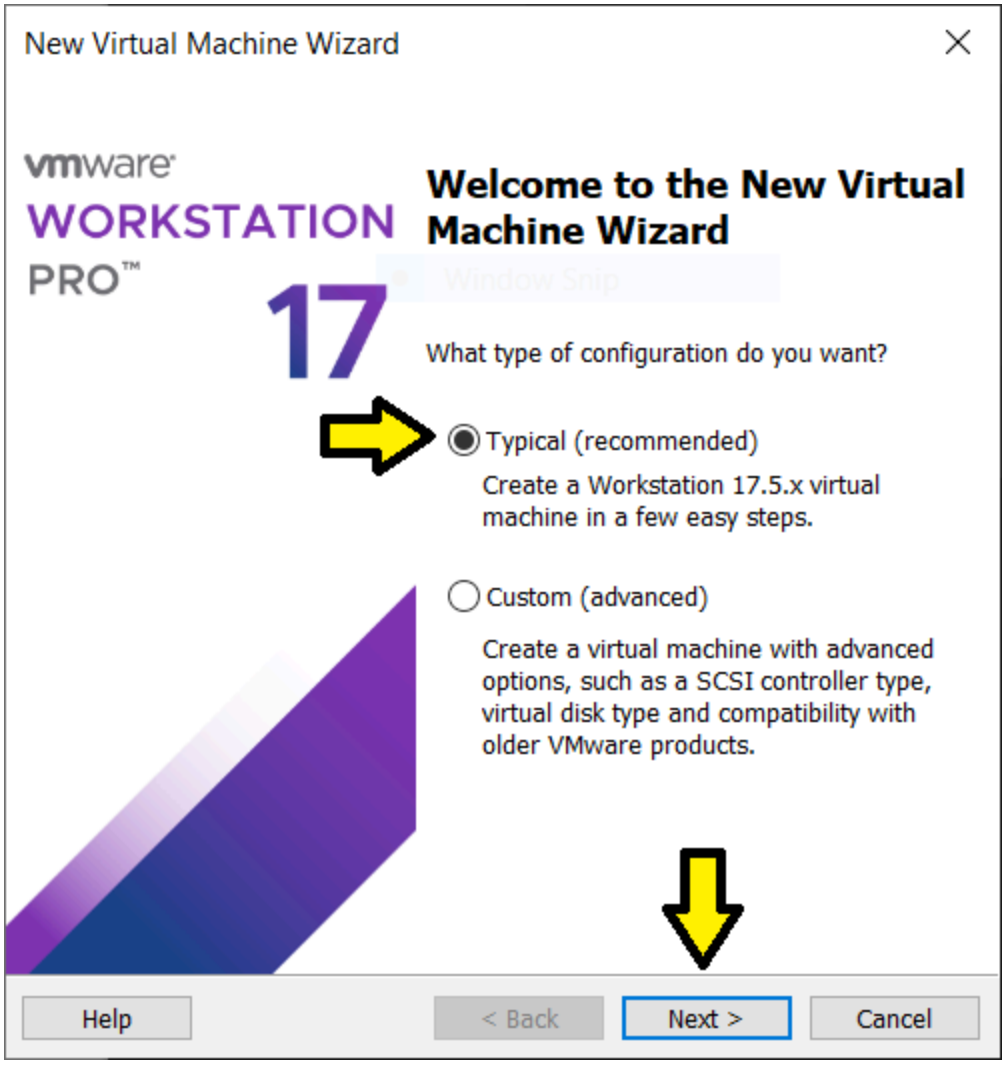
OpenVAS is an open source Linux-based vulnerability scanner. The intent of OpenVAS usage is to scan the network for vulnerabilities and thereby become aware of certain weaknesses in the network, which can then be turned into an RFI request. You can schedule scans as well so that you always have a relatively 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

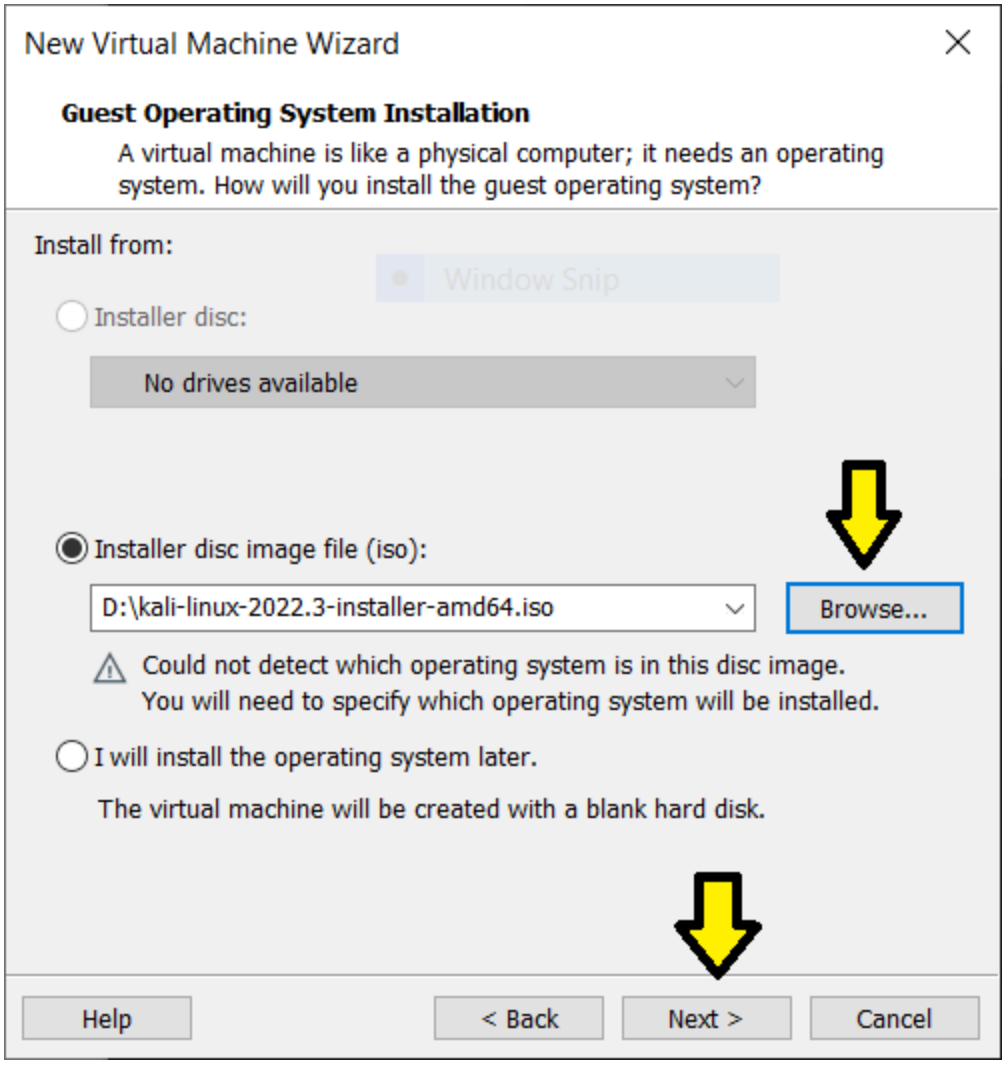
- ***Make sure you build your VM on VMWare Workstation Pro***
  - ➢ ESXI doesn't play nice with .ova's generated from VirtualBox
- Start with a fresh Kali Linux image (Installation instructions below)
- Open up VMWare Workstation Pro and select File -> New Virtual Machine



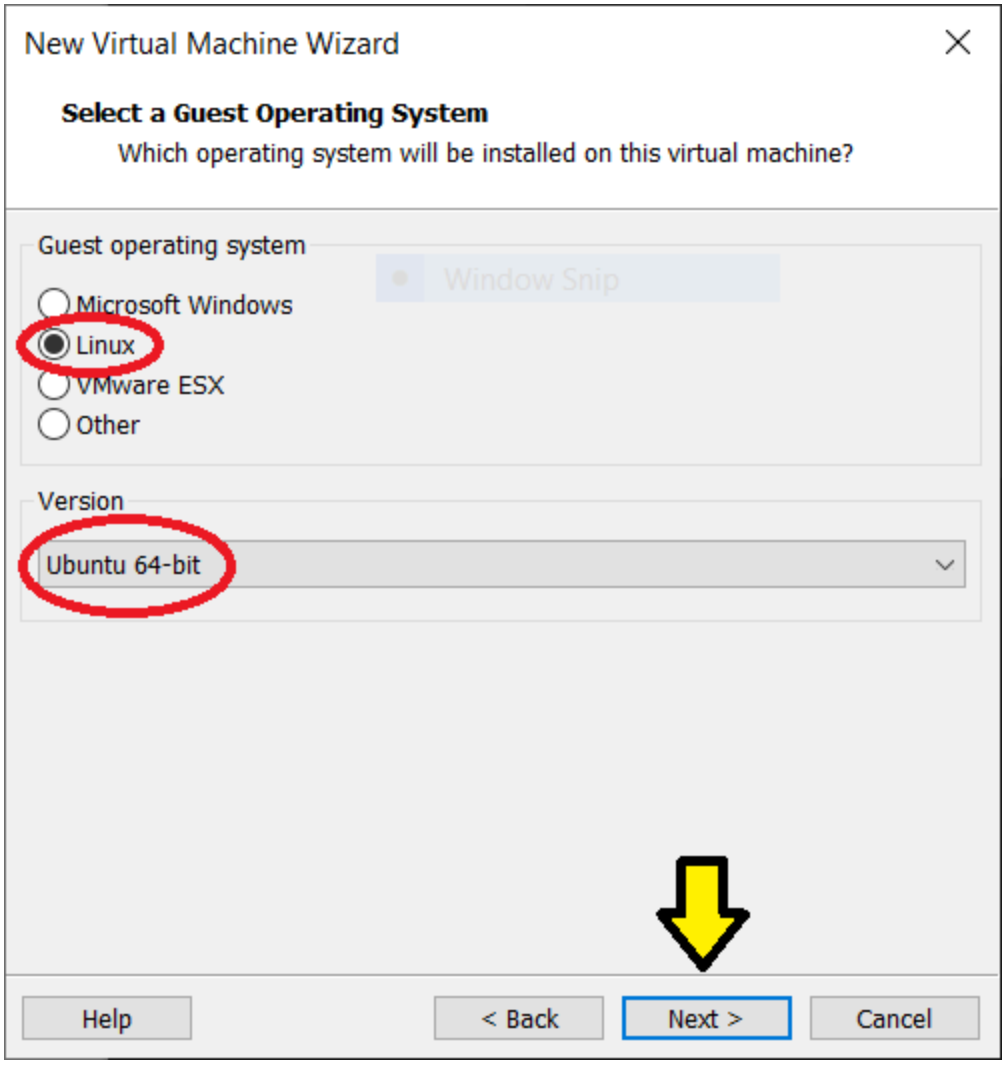
- Select 'Typical Installation'



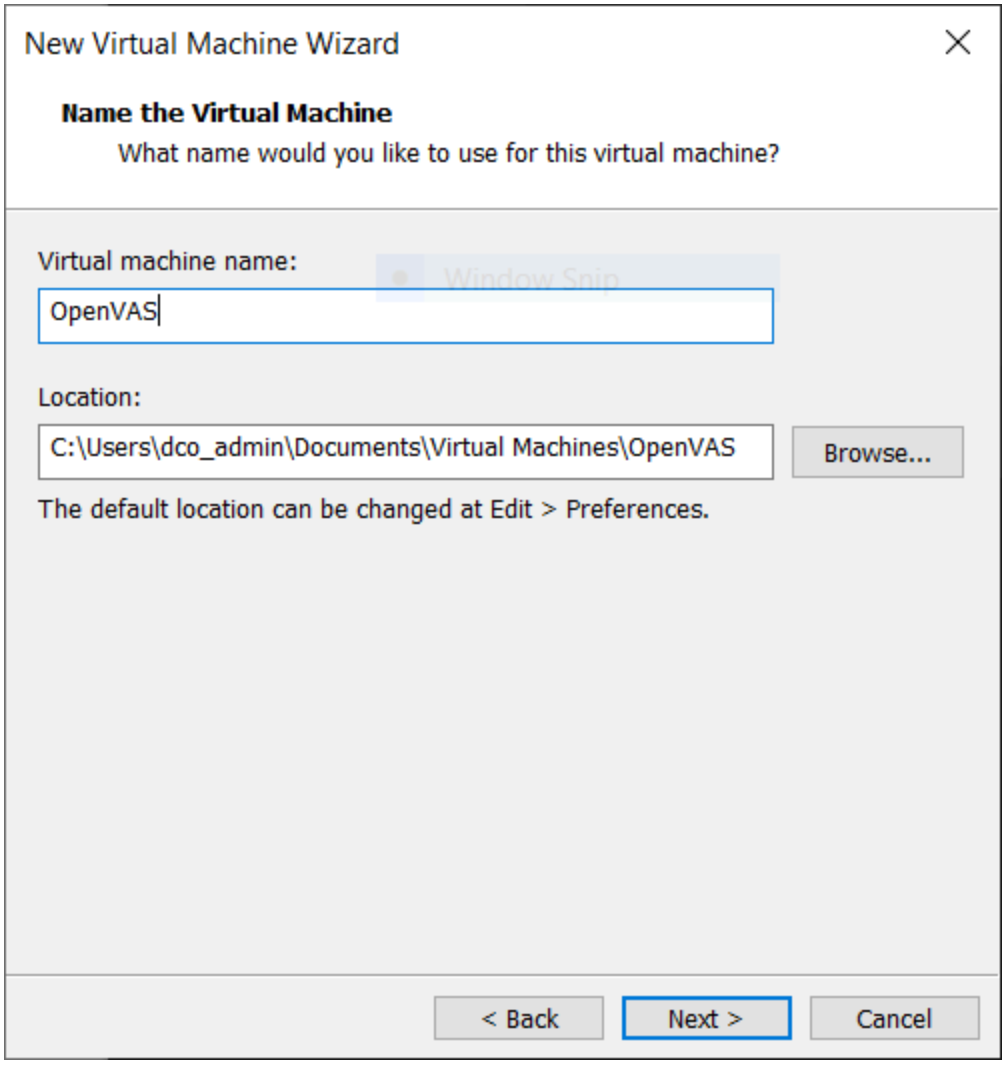
- Next, pick your .iso file's location



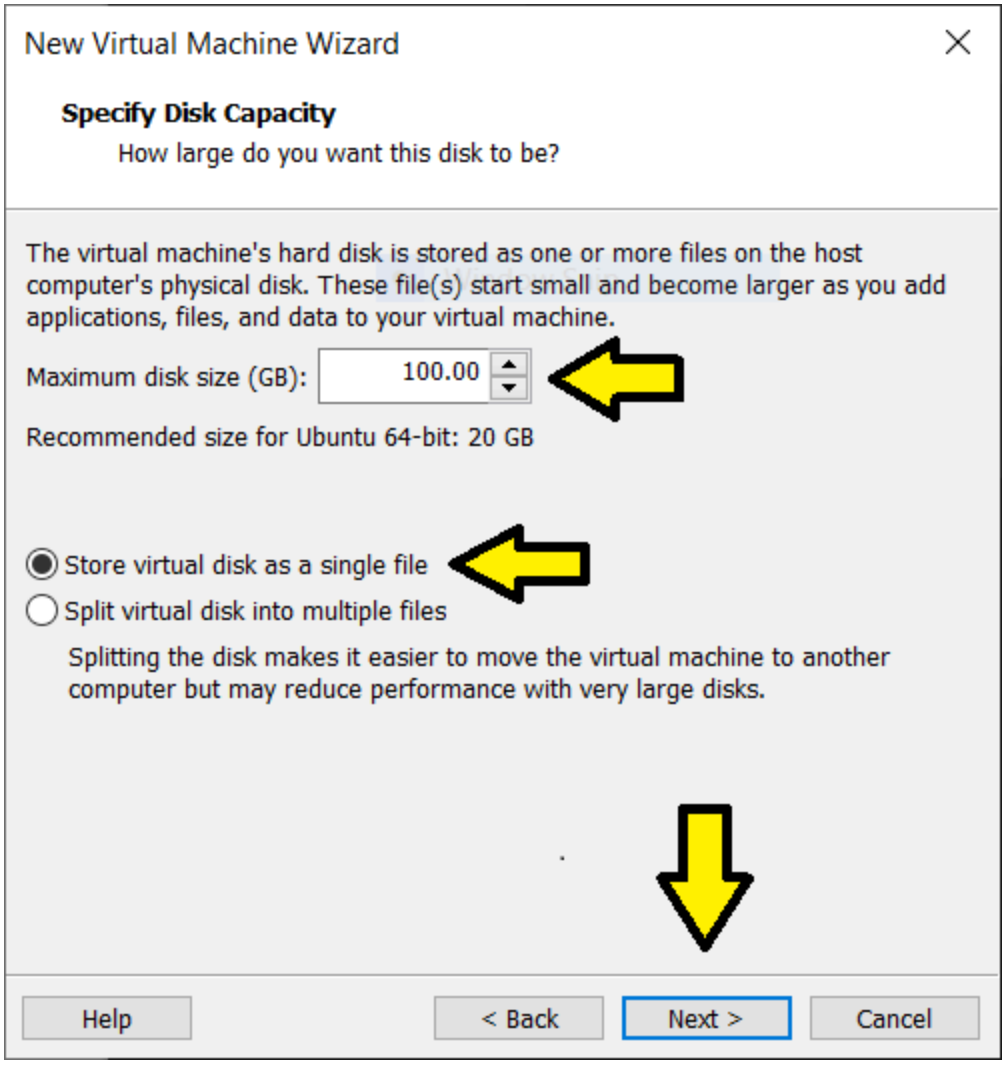
- Tell VMWare what operating system you're installing if it hasn't auto-detected it



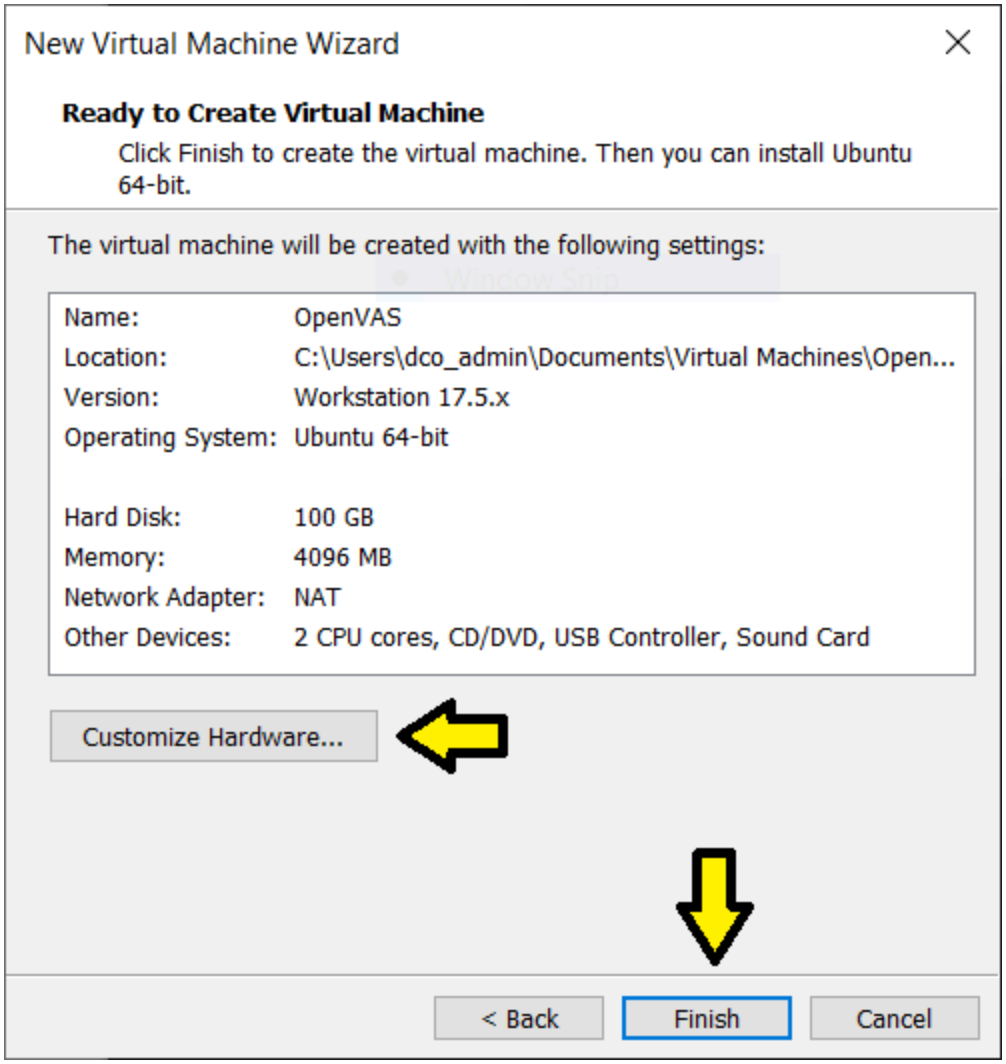
- Name the virtual machine, and select where it should be saved. The directory you're saving it in should have plenty of space. Keep in mind that the VM itself will be about 70GB when completed.



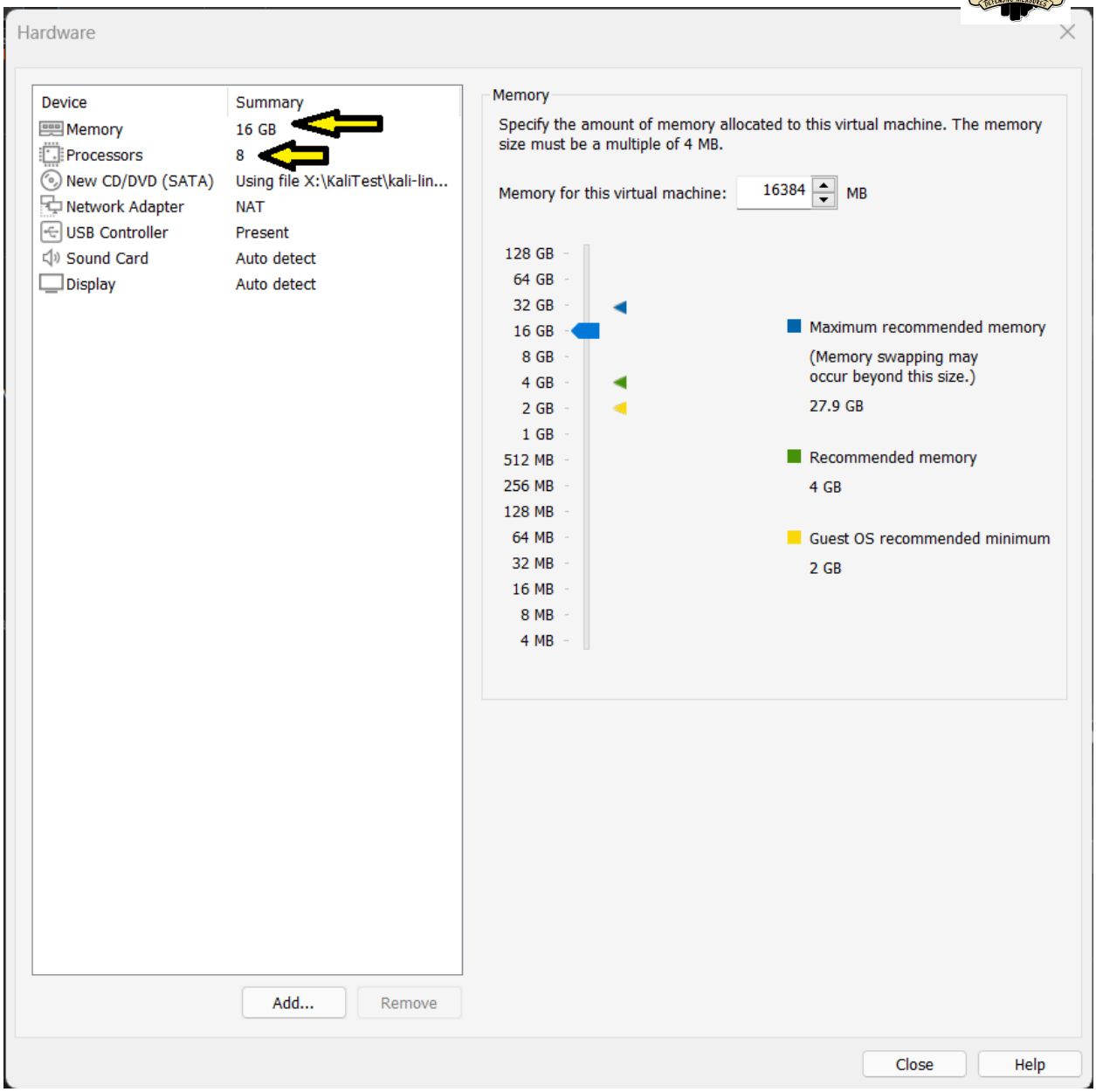
- Make sure that your VM has plenty of space (at least 100GB). You will need a decent chunk of this space in order for the next steps to go smoothly and avoid crashing your VM due to a lack of space. Select ‘Store virtual disk as a single file’ as well.



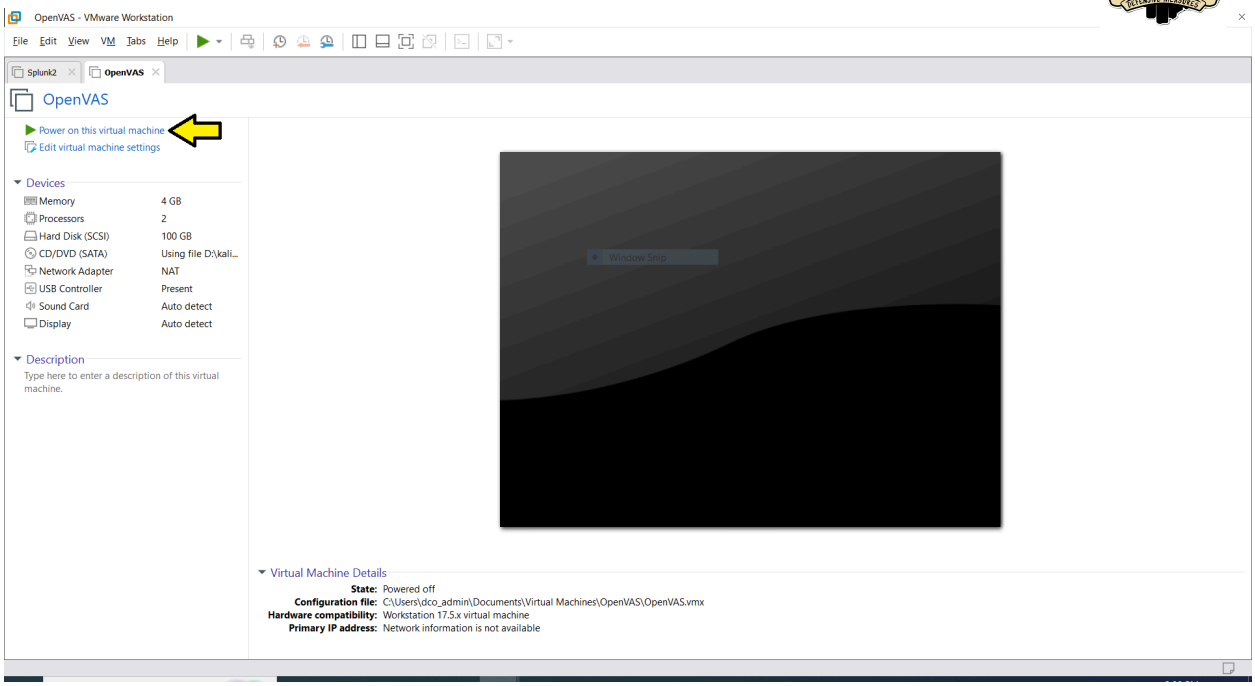
- Verify your settings are correct. If they aren't, click on the Customize Hardware button and select the appropriate settings. At least 16GB of memory (more memory = faster scans) and four hyperthreaded cores for eight cores total are required.


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

❖



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

Screenshot

Go Back

Continue

KALI

Select your location

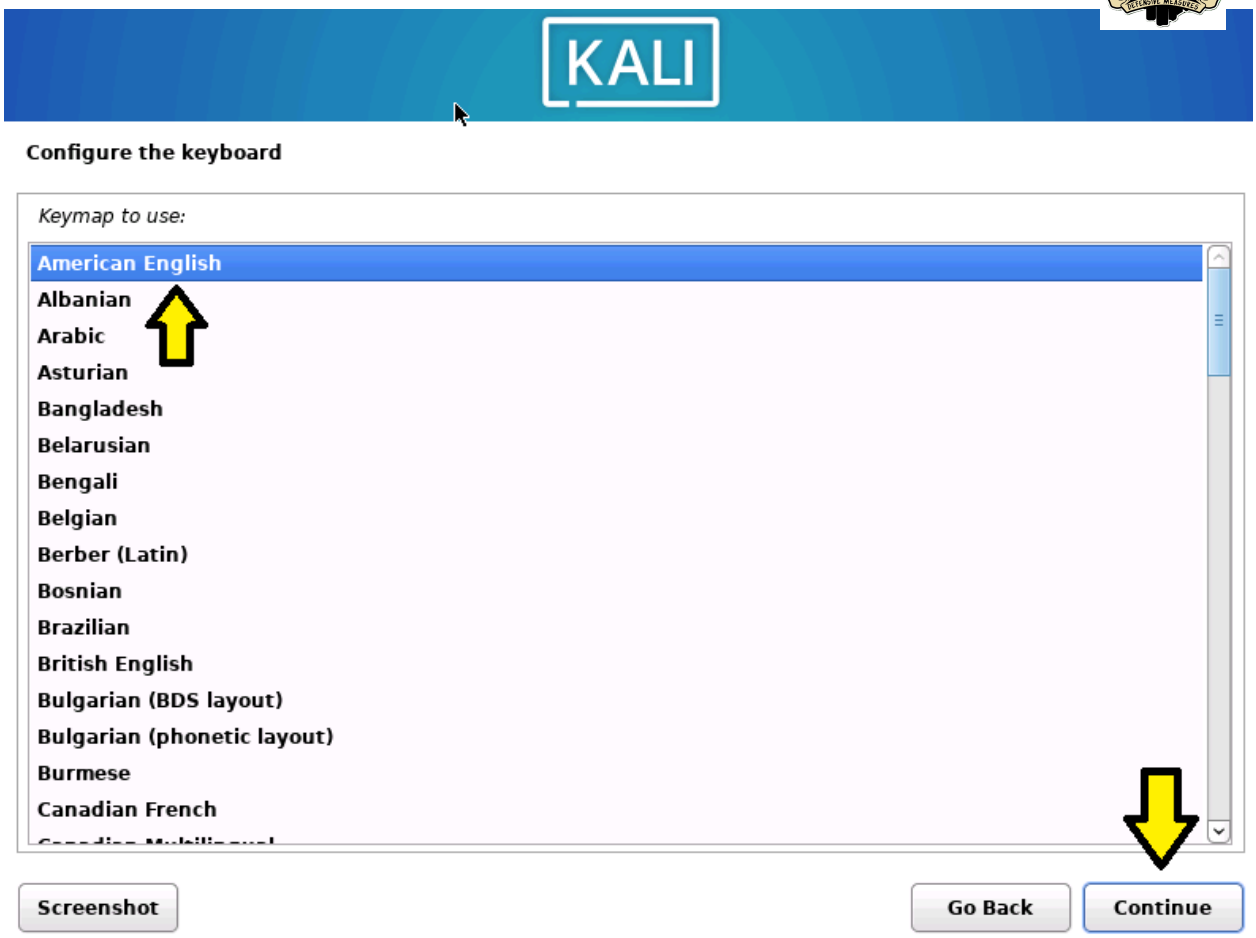
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

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

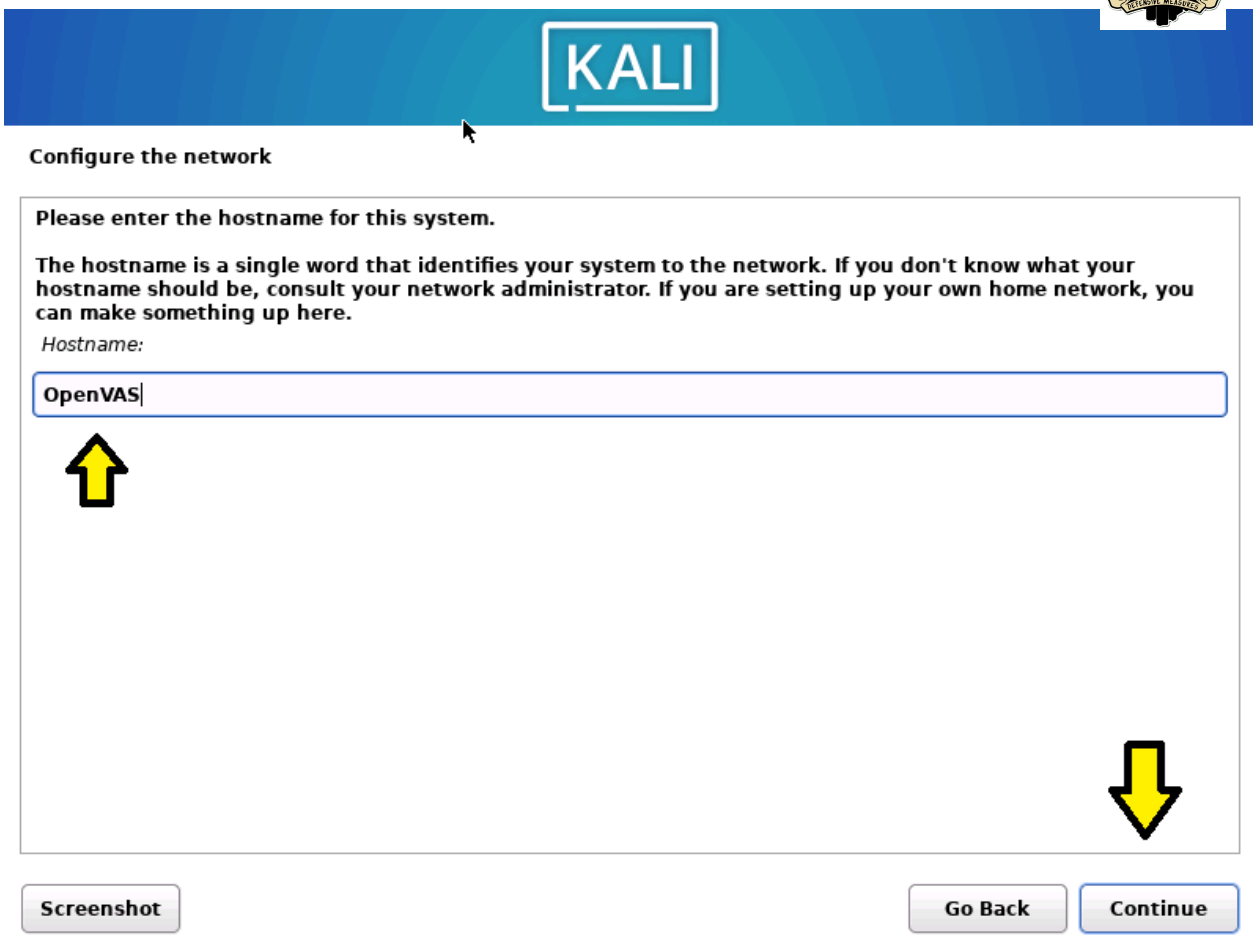
Country, territory or area:

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

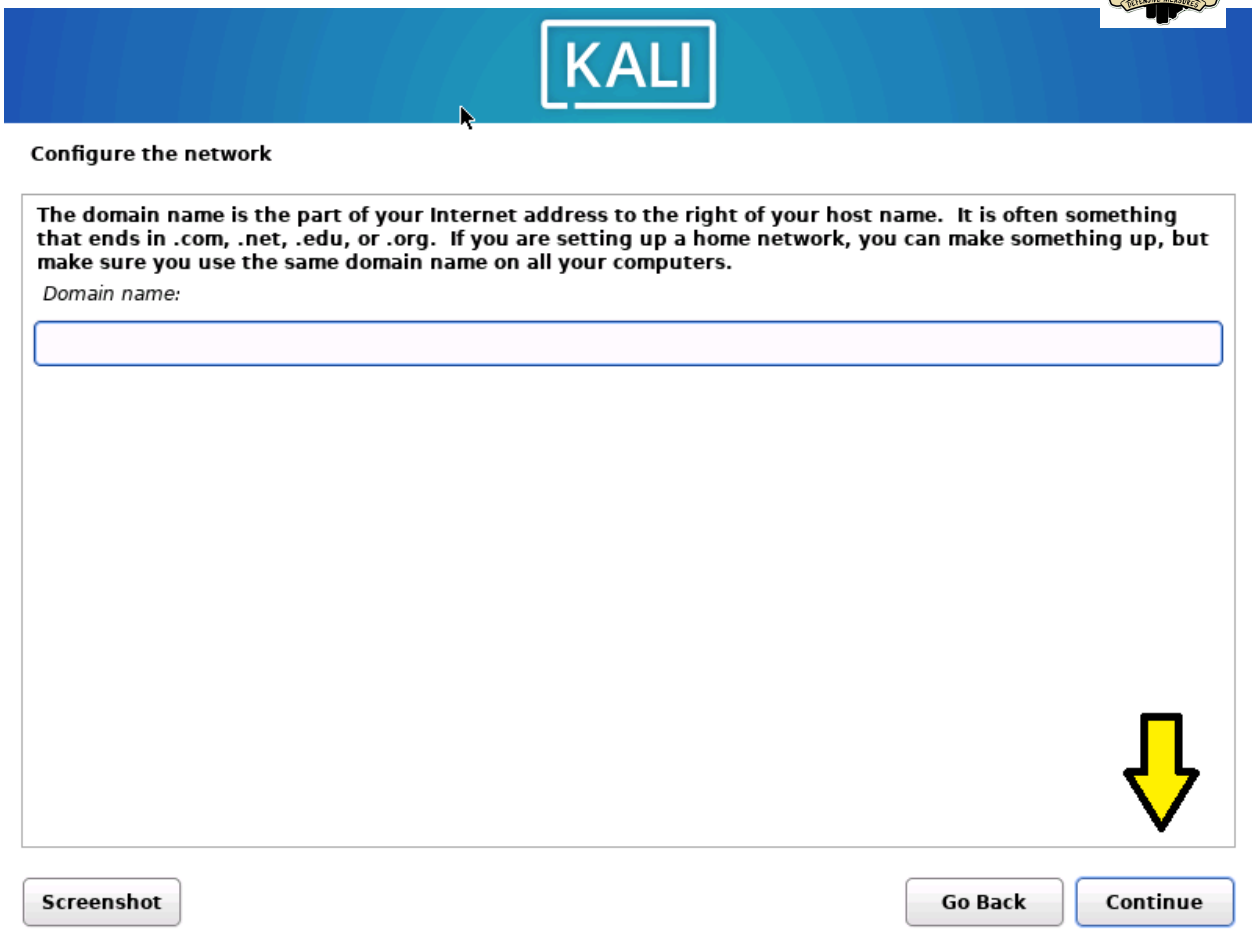
Screenshot **Go Back** **Continue**



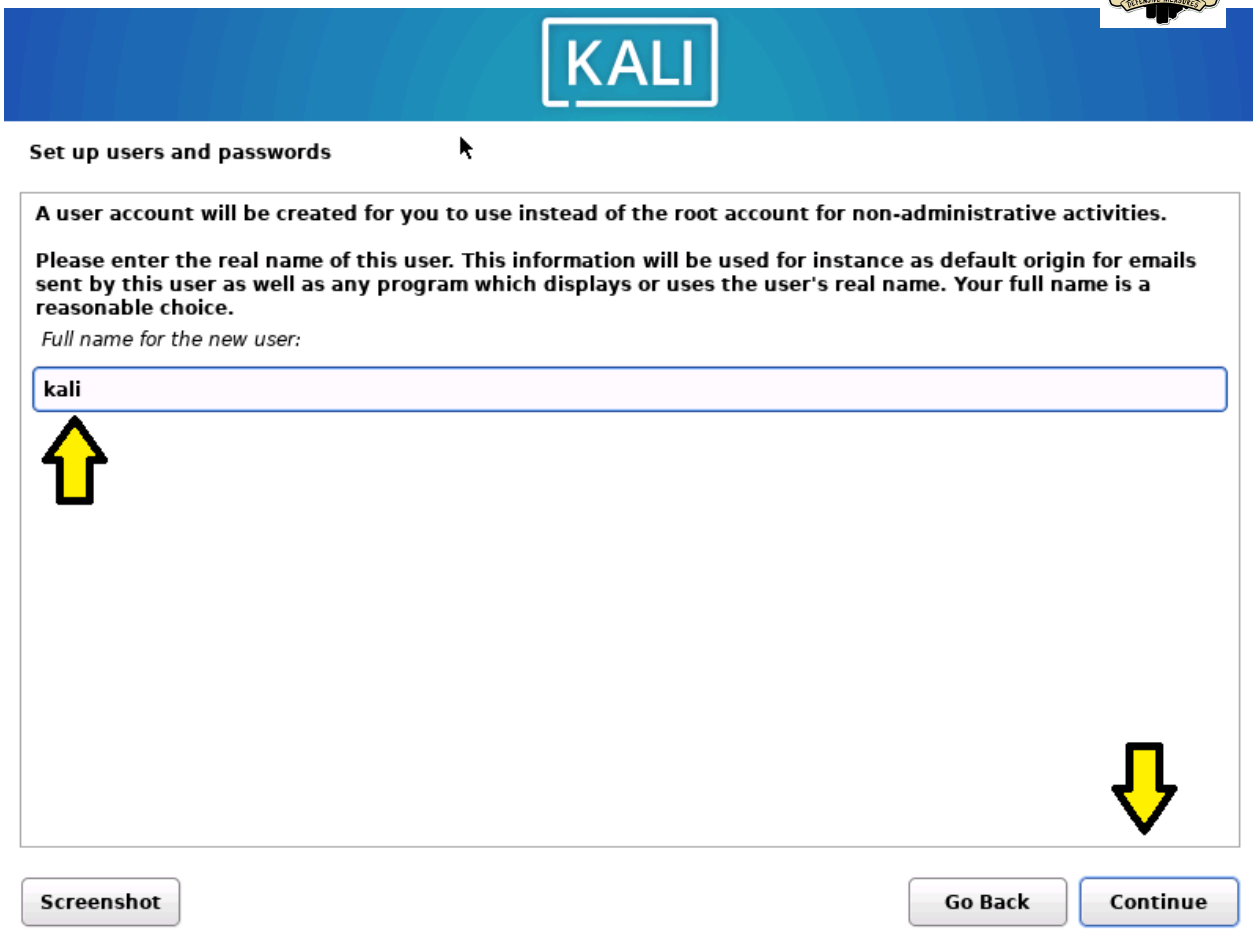
- Create a hostname for the machine



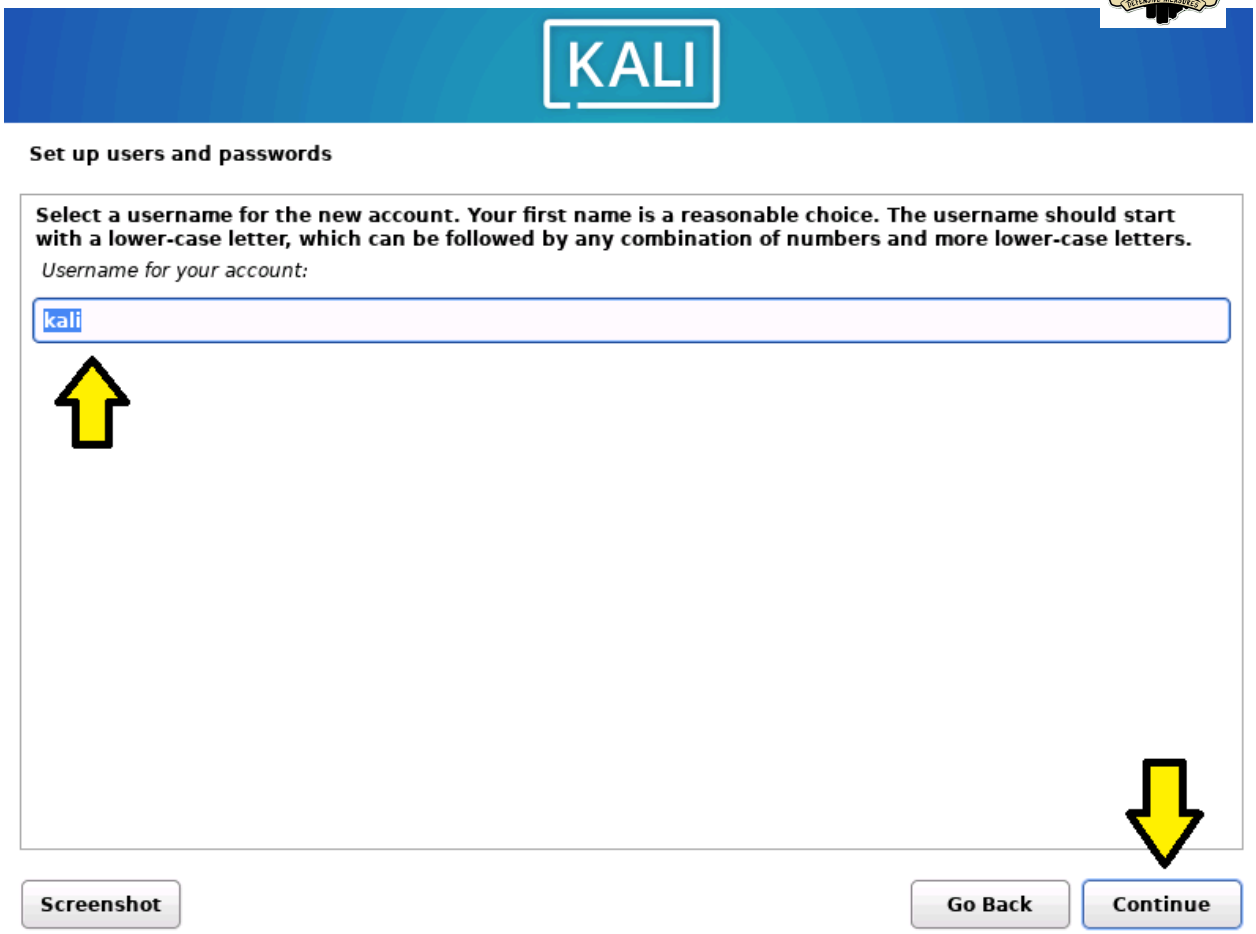
- Enter a domain if you wish. You can also leave it blank.



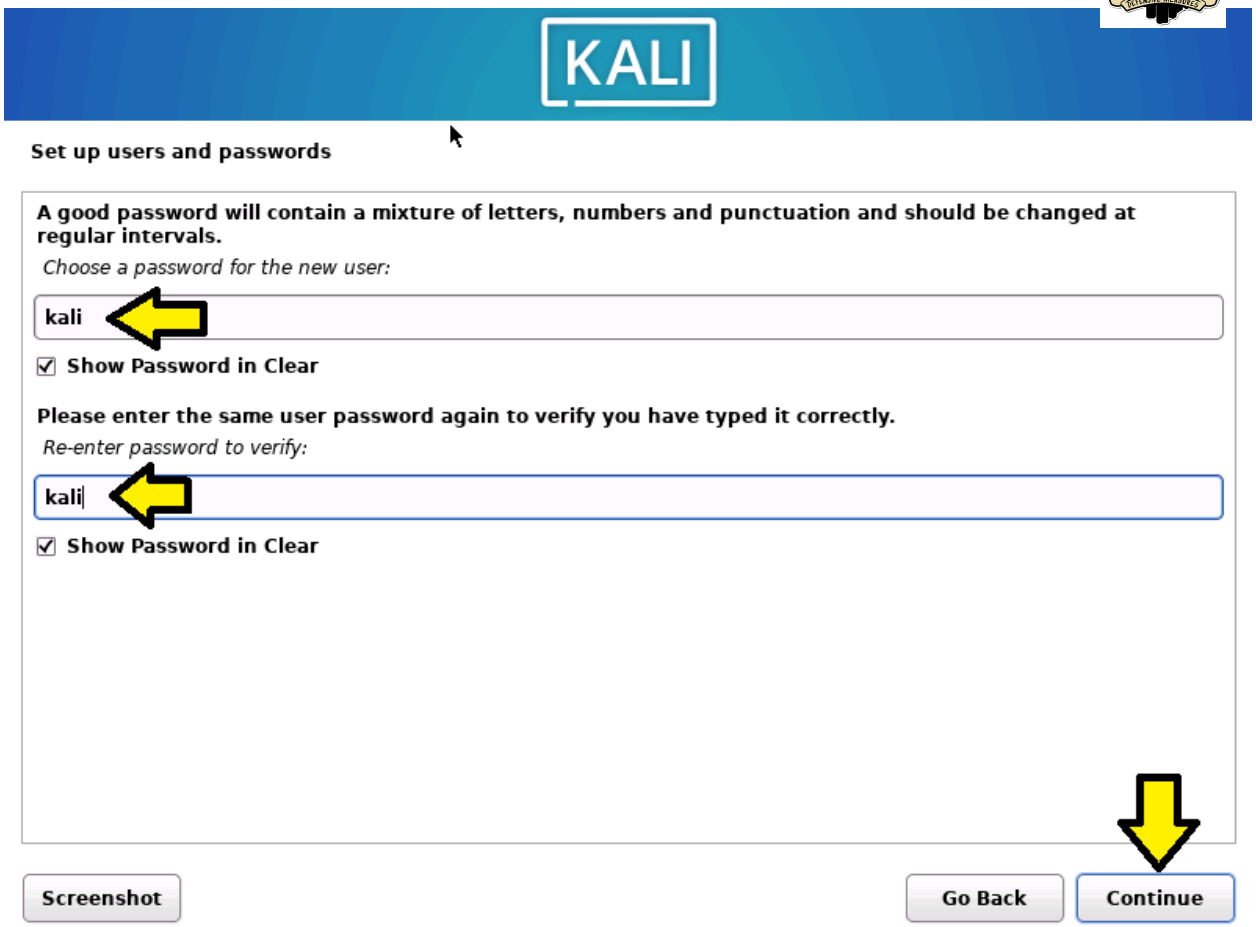
-
- Enter the full name of the primary user



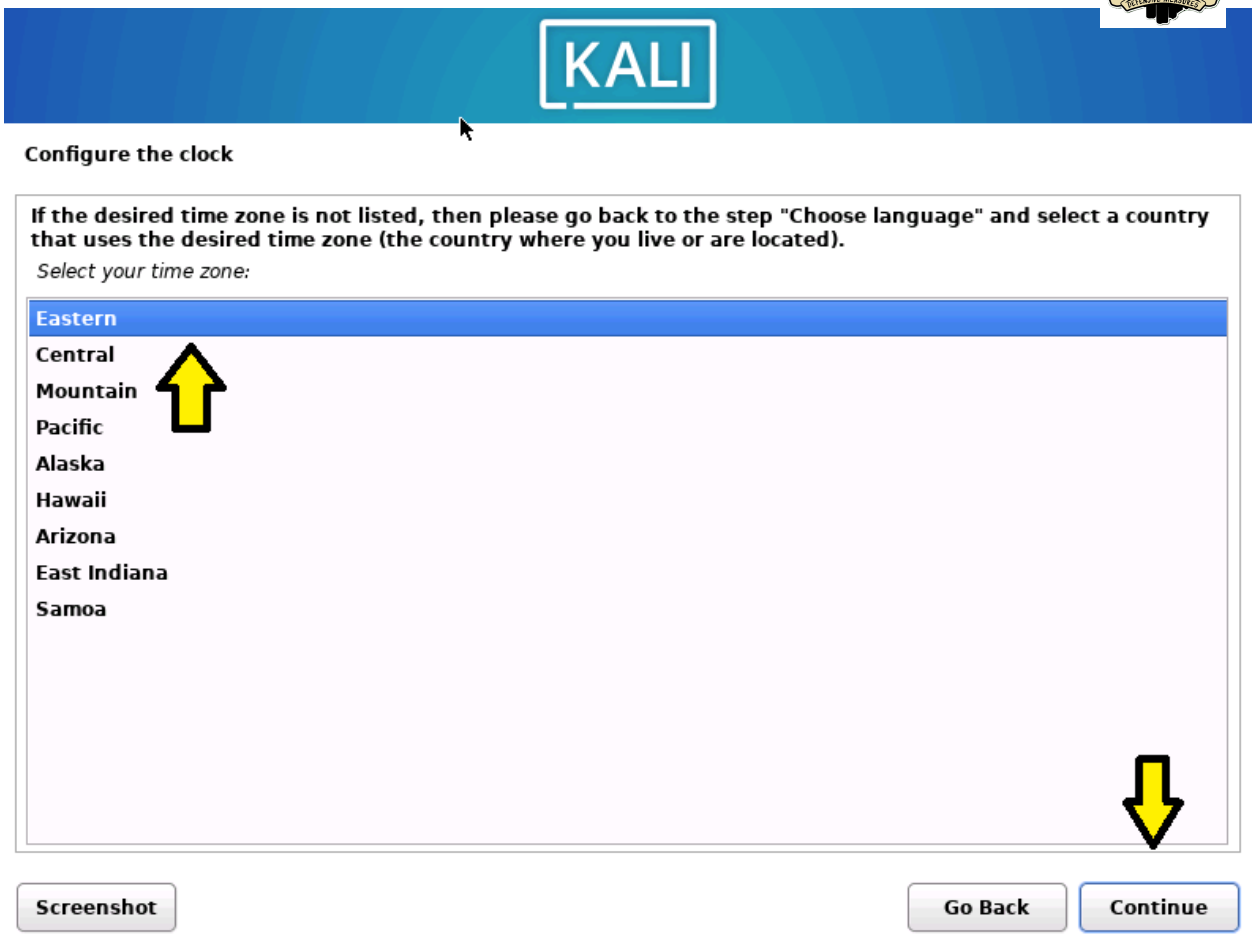
- Create a username for the machine



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



-
- Set up the system clock



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

KALI

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**

KALI

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**

KALI

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.

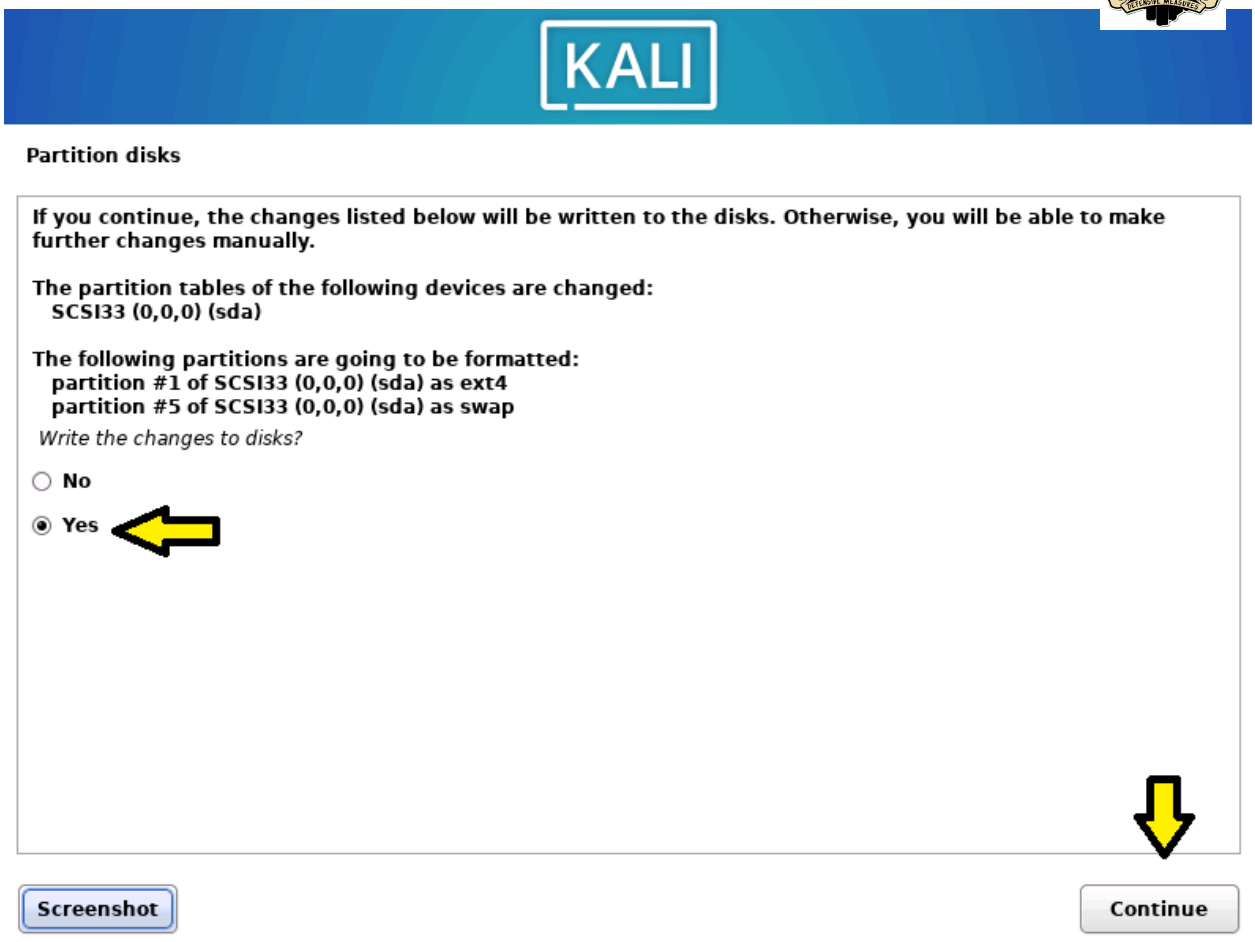
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

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

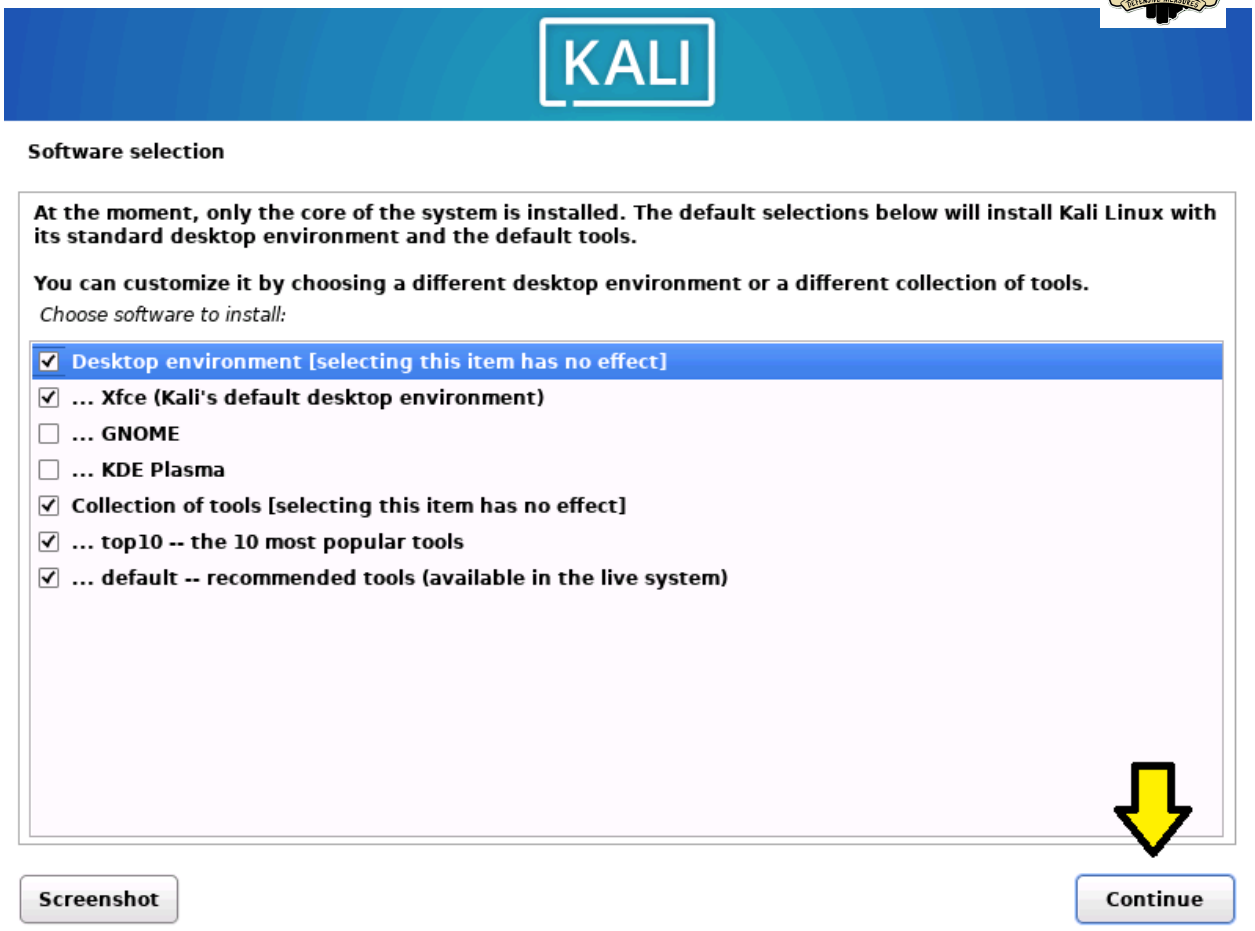
>	#1	primary	106.3 GB	f	ext4	/
>	#5	logical	1.0 GB	f	swap	swap

Undo changes to partitions
Finish partitioning and write changes to disk

Screenshot **Help** **Go Back** **Continue**



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



-
- Install the GRUB bootloader

KALI

Install the GRUB boot loader

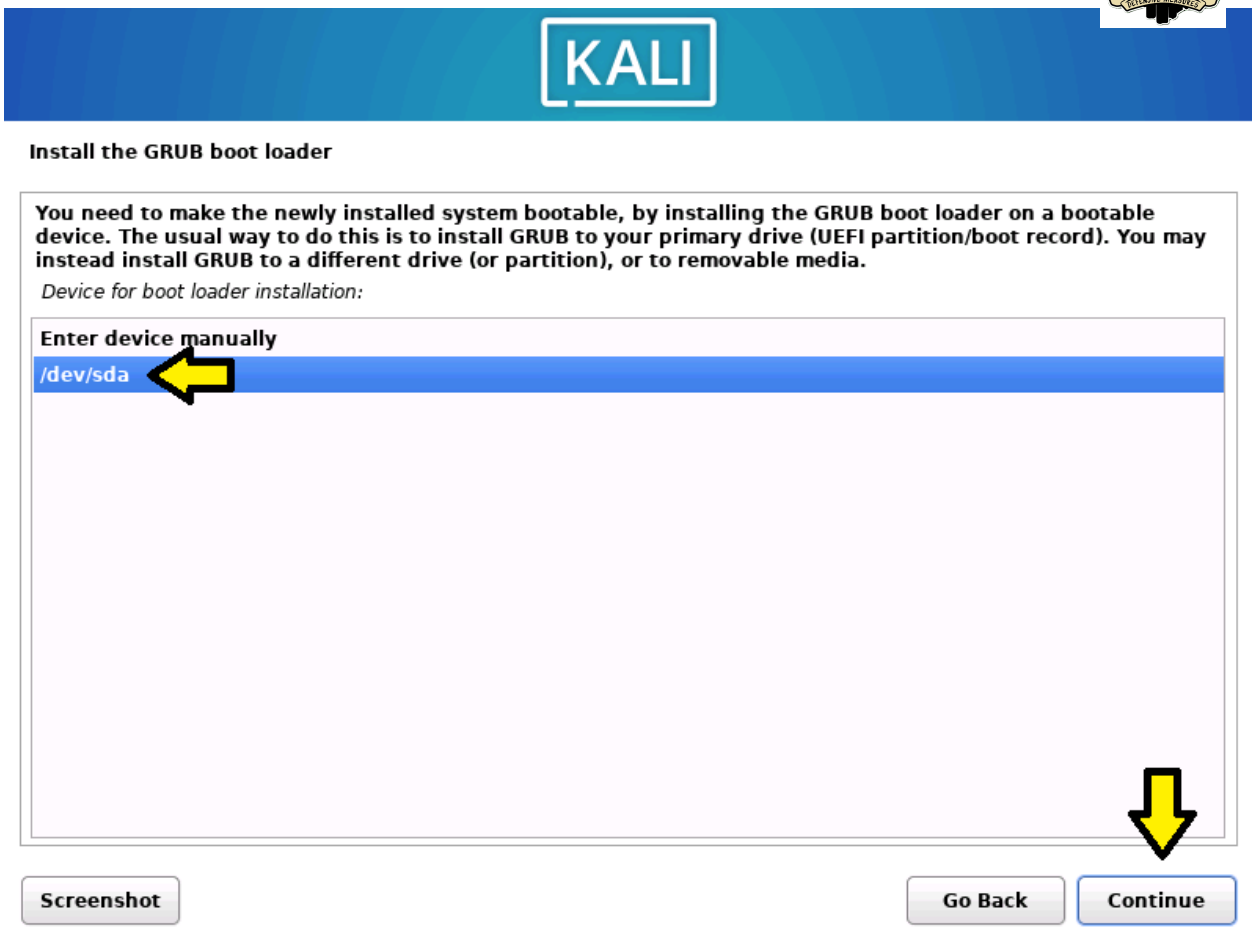
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

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.

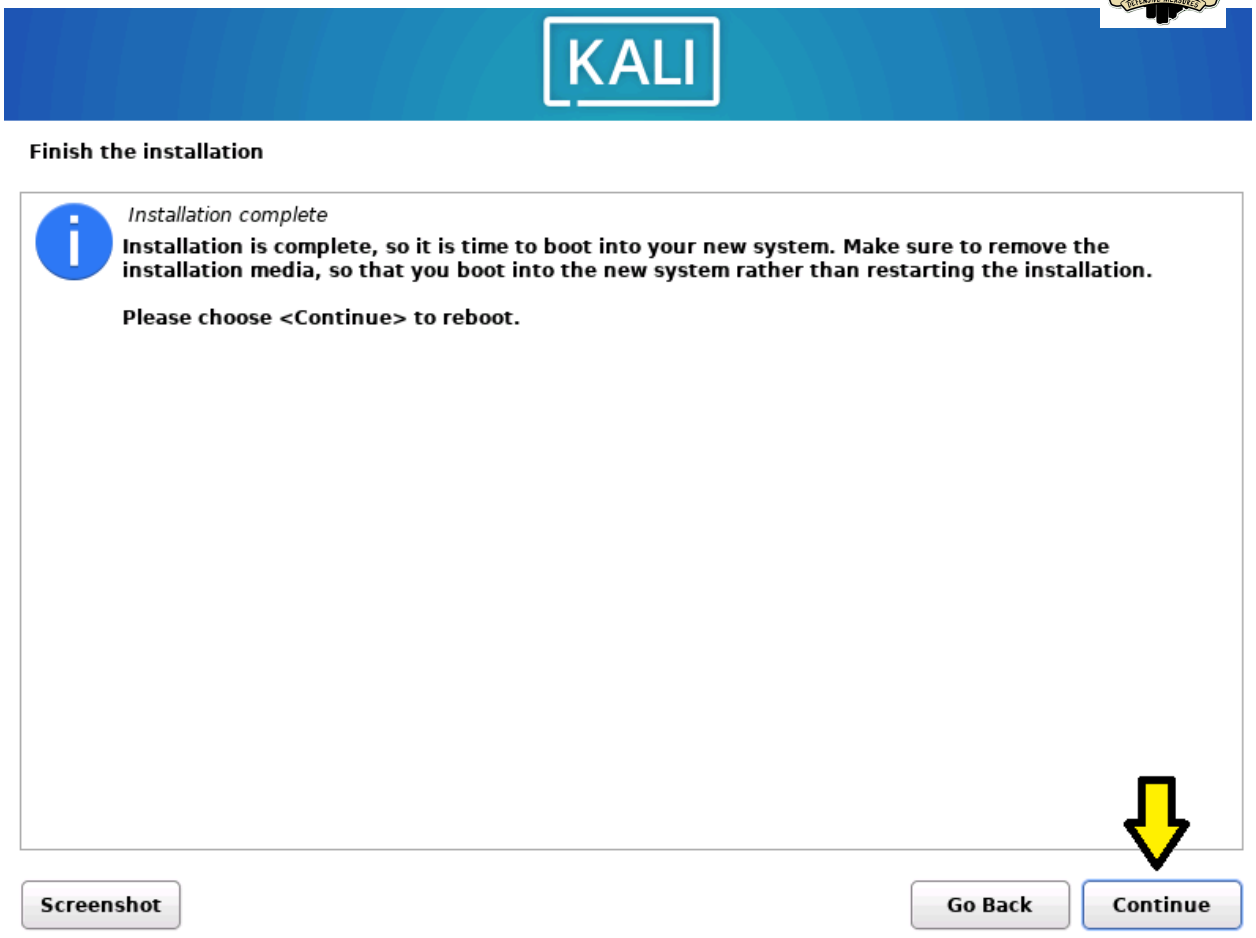
Install the GRUB boot loader to your primary drive?

- ○ **No**
- ◉ **Yes**

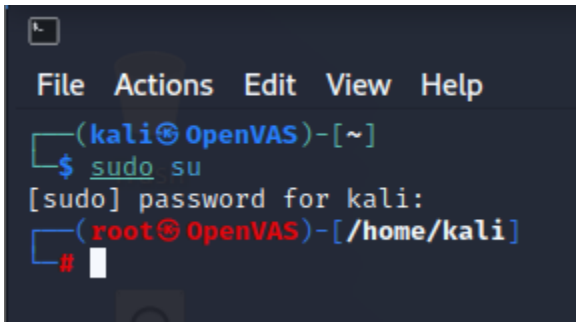
Screenshot **Go Back** **Continue**



- Press Continue to reboot and finish the Kali install



- 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'



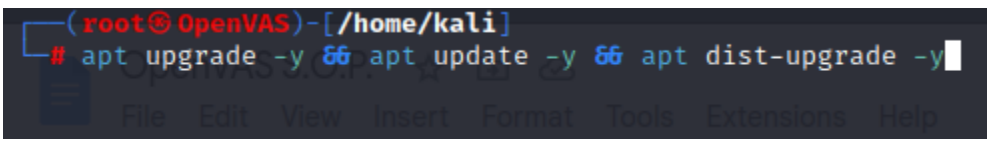
- Upgrade the OS, and install and upgrade packages with the following commands:
  - **sudo apt update -y**
  - **sudo apt upgrade -y**

- 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.

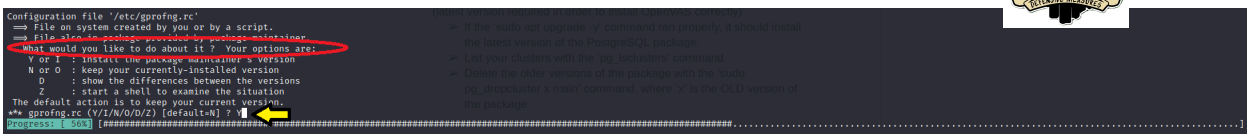
- You will also be alerted to an obsolete version of the PostgreSQL daemon. This will come into play later.

➢ **sudo apt dist-upgrade -y**

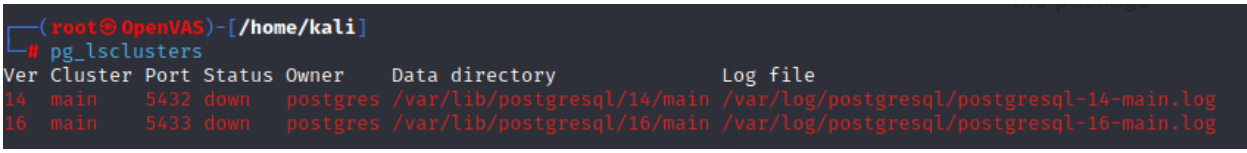
➢ You can chain these three command together using '**&&**' as pictured below

➢ 

➢ 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

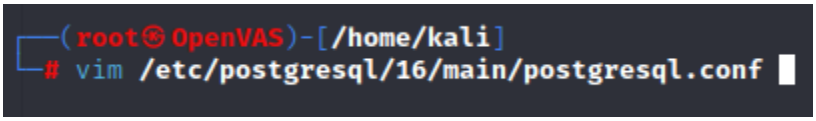


- ❖ Upgrade the PostgreSQL package and configure the correct listening port (latest version required in order to install OpenVAS correctly)
  - ➢ If the above commands ran properly, it should install the latest version of the PostgreSQL package.
  - ➢ List your clusters with the '**pg_lsclusters**' command. You can see here that both version 14 and version 16 are installed on the very left hand side of the picture



  - ➢ Delete the older versions of the package with the '**sudo pg_dropcluster x main**' command, where 'x' is the OLD version of the package. Run **pg_lsclusters** again to verify that the latest version is the only one installed

  - ➢ The PostgreSQL daemon needs to be listening on port 5432. In order to configure this, you need to edit the **postgresql.conf** file. It should be located in **/etc/postgresql/x/main/** where 'x' is the version number.

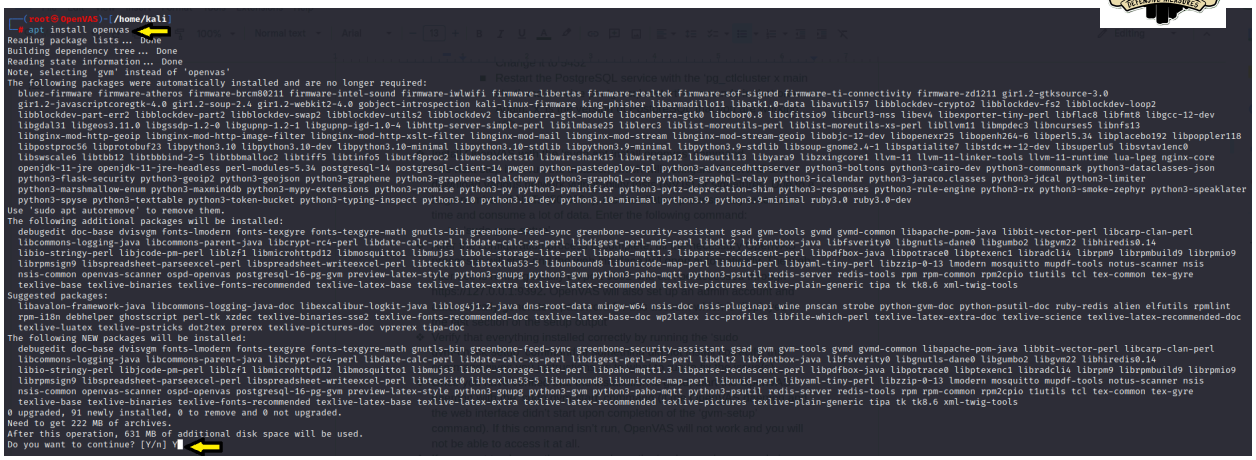


    - Scroll down a little bit until you see a line that says port = xxxx. Change it to **5432.**
    - Restart the PostgreSQL service with the '**pg_ctlcluster x main start**' and '**service postgresql restart**' commands in that order. Again, 'x' is the version of PostgreSQL that you are working with.

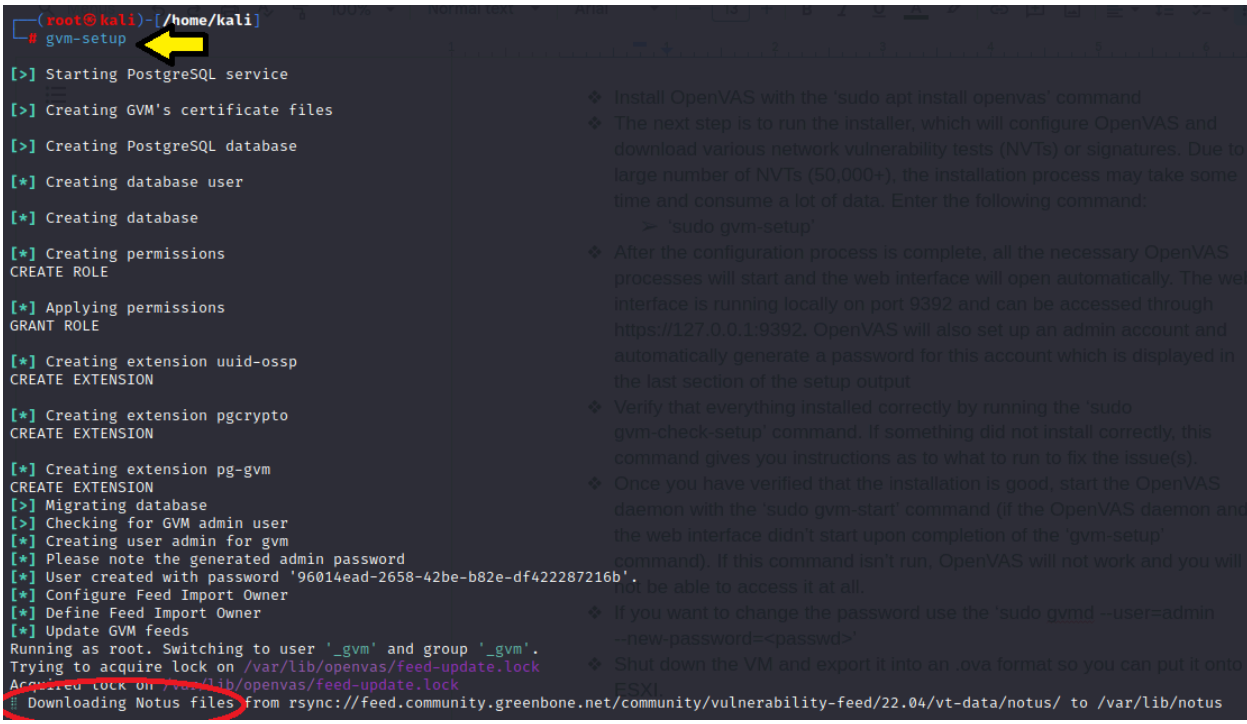
```
#------------------------------------------------------------------------------
# FILE LOCATIONS
#------------------------------------------------------------------------------

# 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



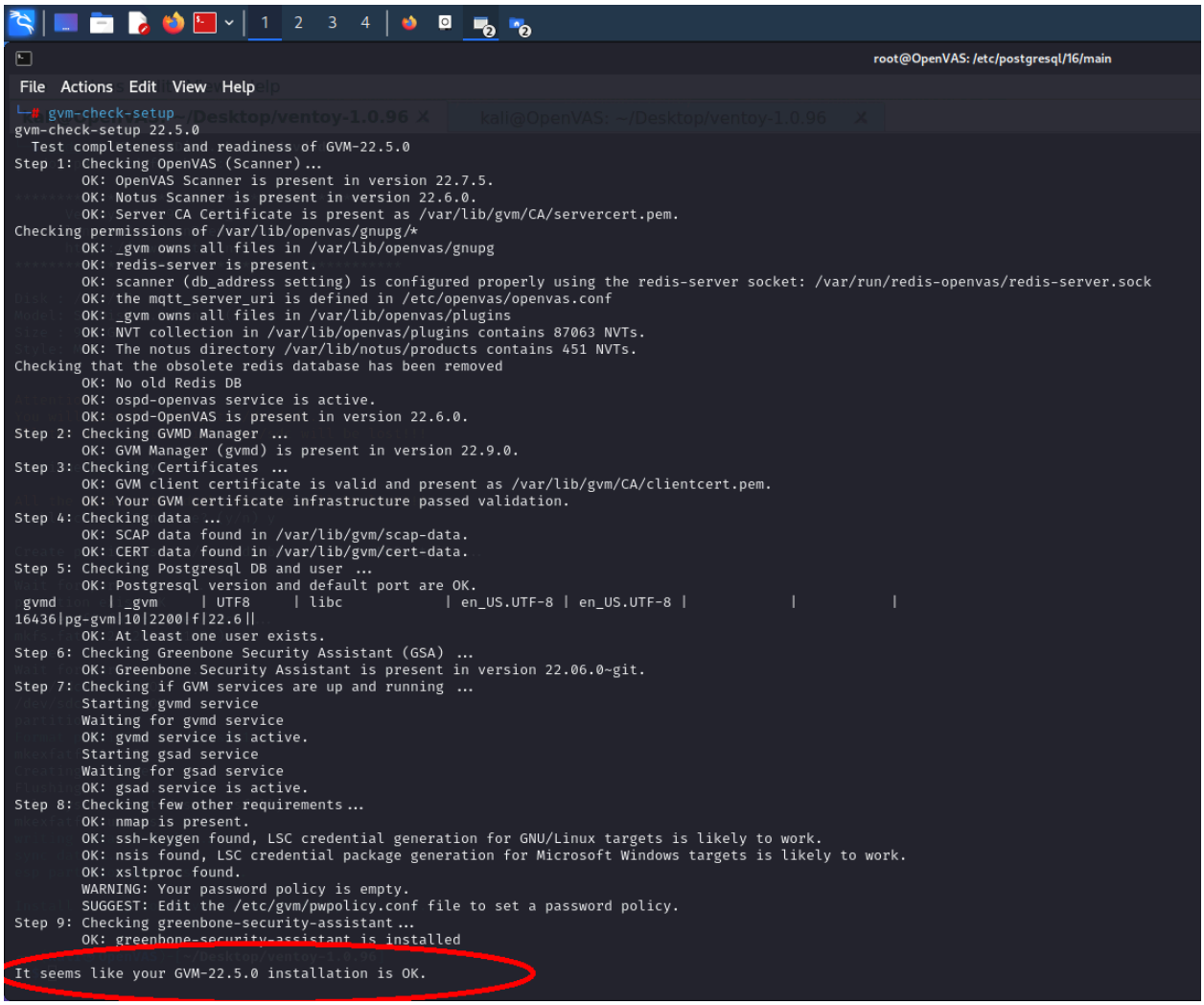
- The next step is to run the installer, which will configure OpenVAS and download various network vulnerability tests (NVTs) or signatures. Due to a large number of NVTs (50,000+), the installation process will take a lot of time and consume a lot of data. Keep in mind that if this step is done incorrectly, OpenVAS will not work at all because it will not have any virus definitions to work off of. Enter the following command:
  - ‘**sudo gvm-setup**’



- After the configuration process is complete, all the necessary OpenVAS processes will start and the web interface will open automatically. The web interface is running locally on port 9392 and can be accessed through **https://127.0.0.1:9392.** OpenVAS will also set up an admin account and

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).



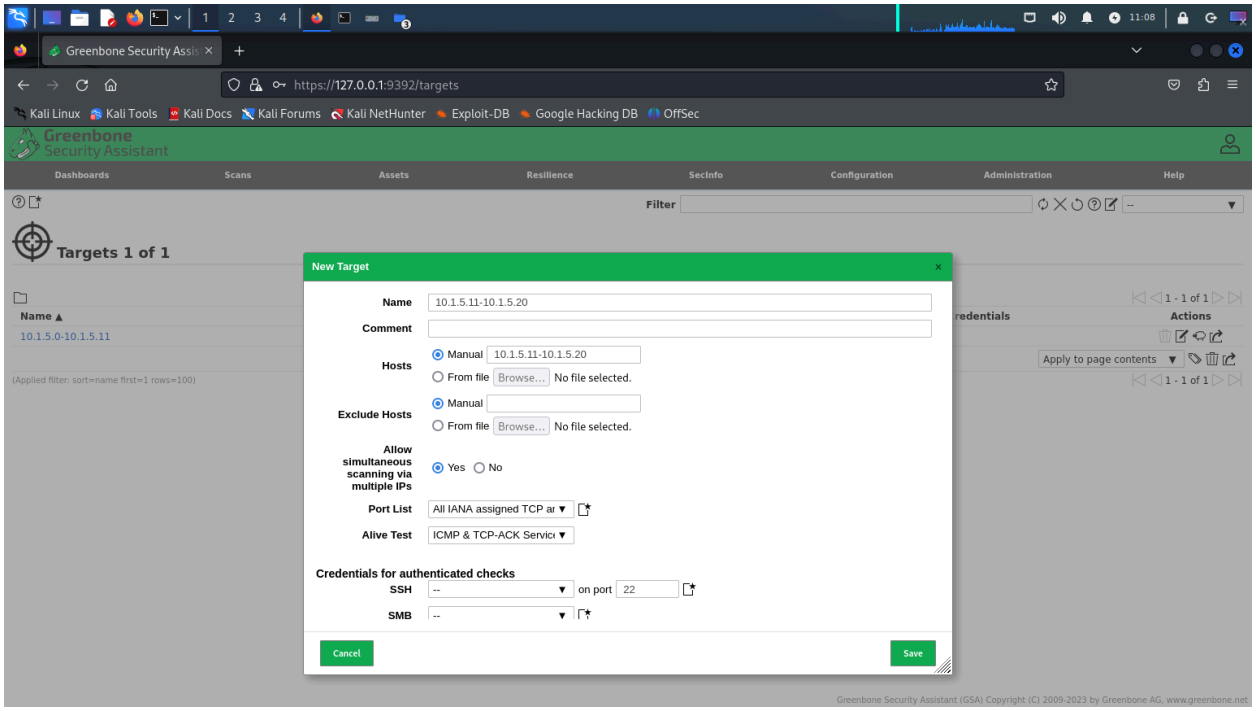
- Once you have verified that the installation is good, start the OpenVAS daemon with the '**sudo gvm-start**' command (if the OpenVAS daemon and the web interface didn't start upon completion of the 'gvm-setup' command). If this command isn't run, OpenVAS will not work and you will not be able to access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

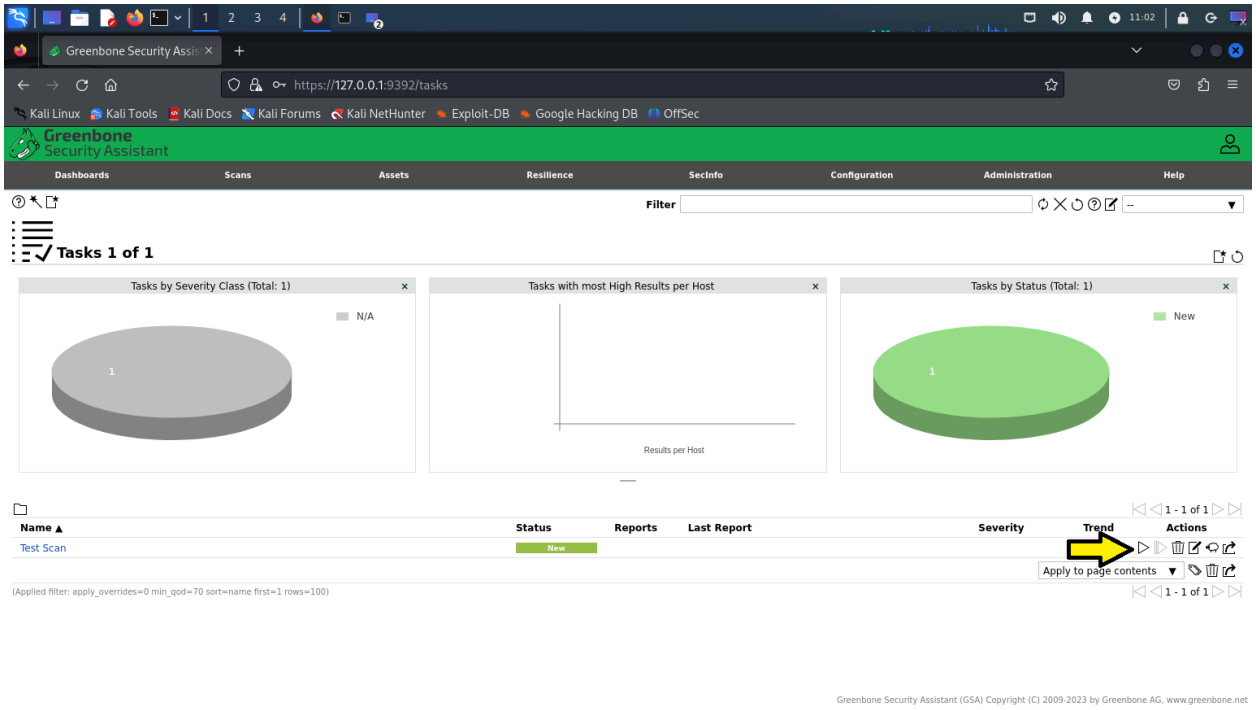
Before you start scanning, you need to make target profiles. You can do this either by going to Configuration -> Targets or by going to the Scans -> Tasks tab and creating a new task and then making the target profile from there. The below screenshot shows the easier option; Configuration -> Targets

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



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:

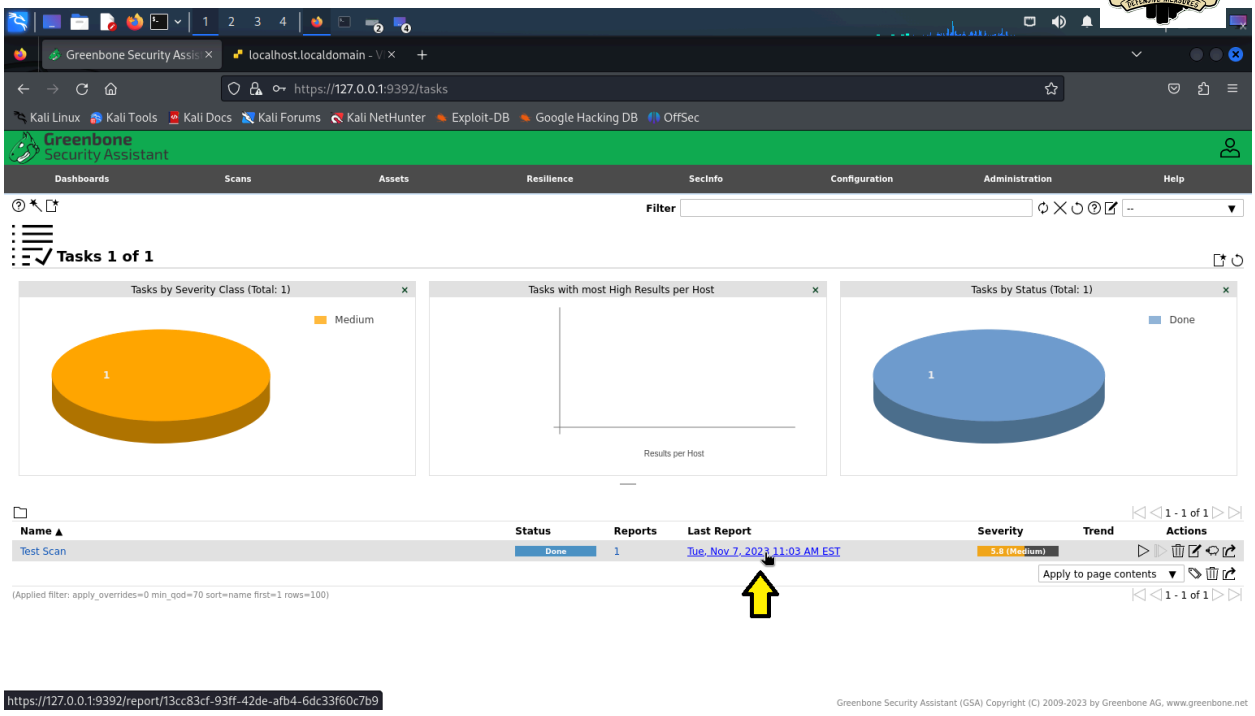


Once your scans are done, you can view the associated report by clicking on the date under the Last Report section.

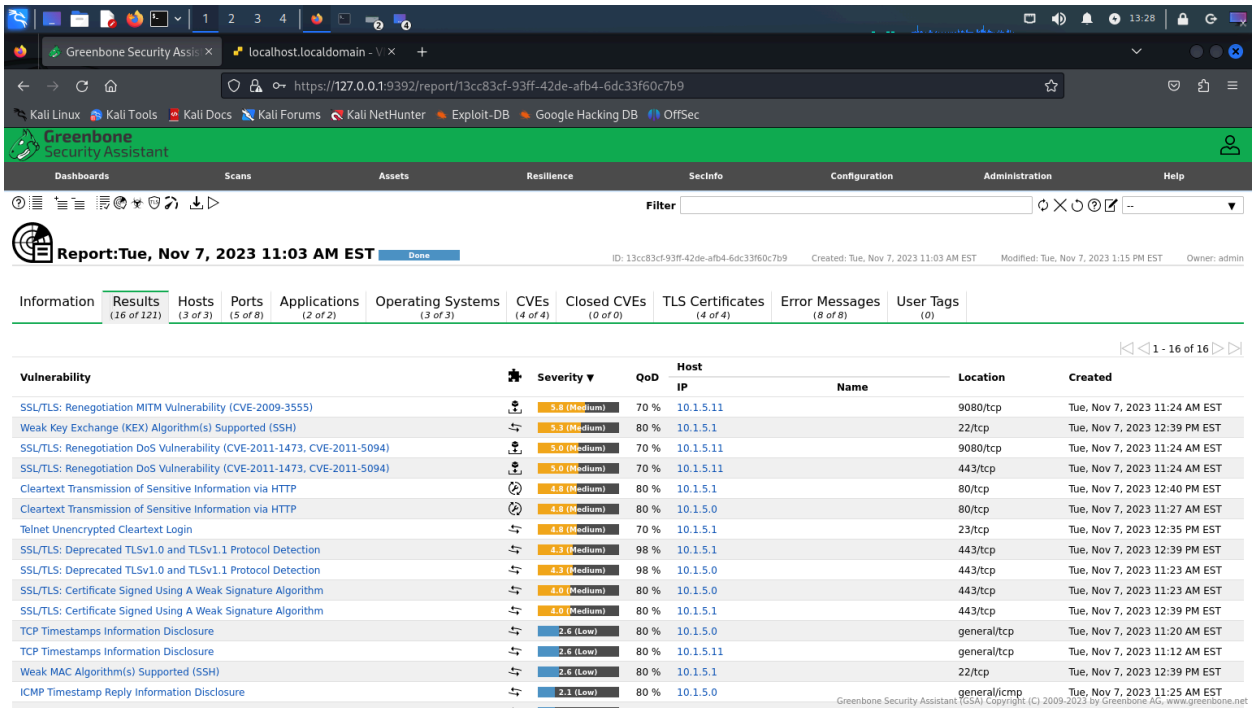
-Alternatively, if you want to view earlier reports, click on the number of reports, and then click on the report you wish to see.

-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:

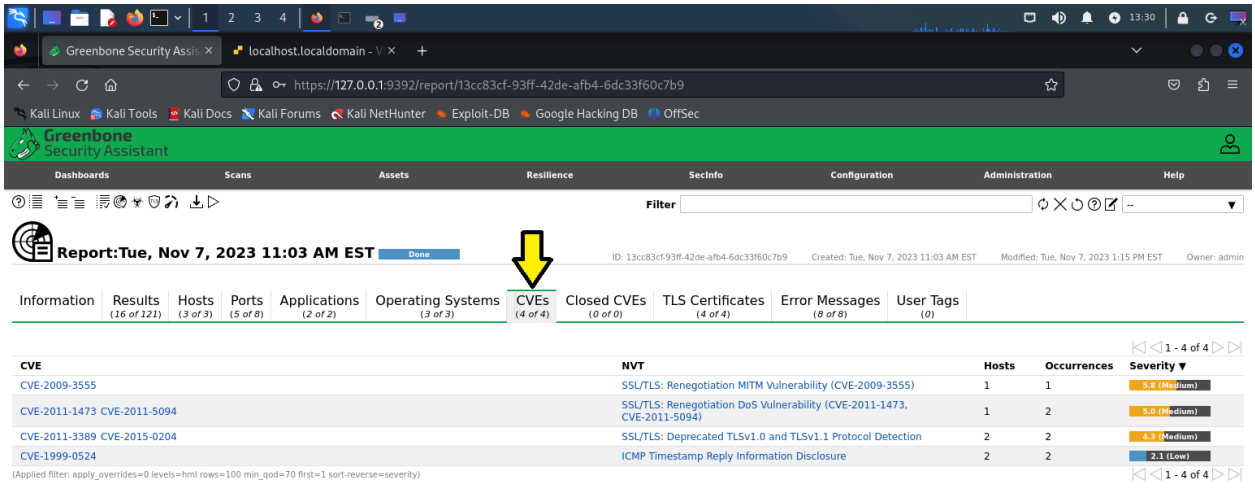


Screenshot depicting Results tab once the report has been pulled up:

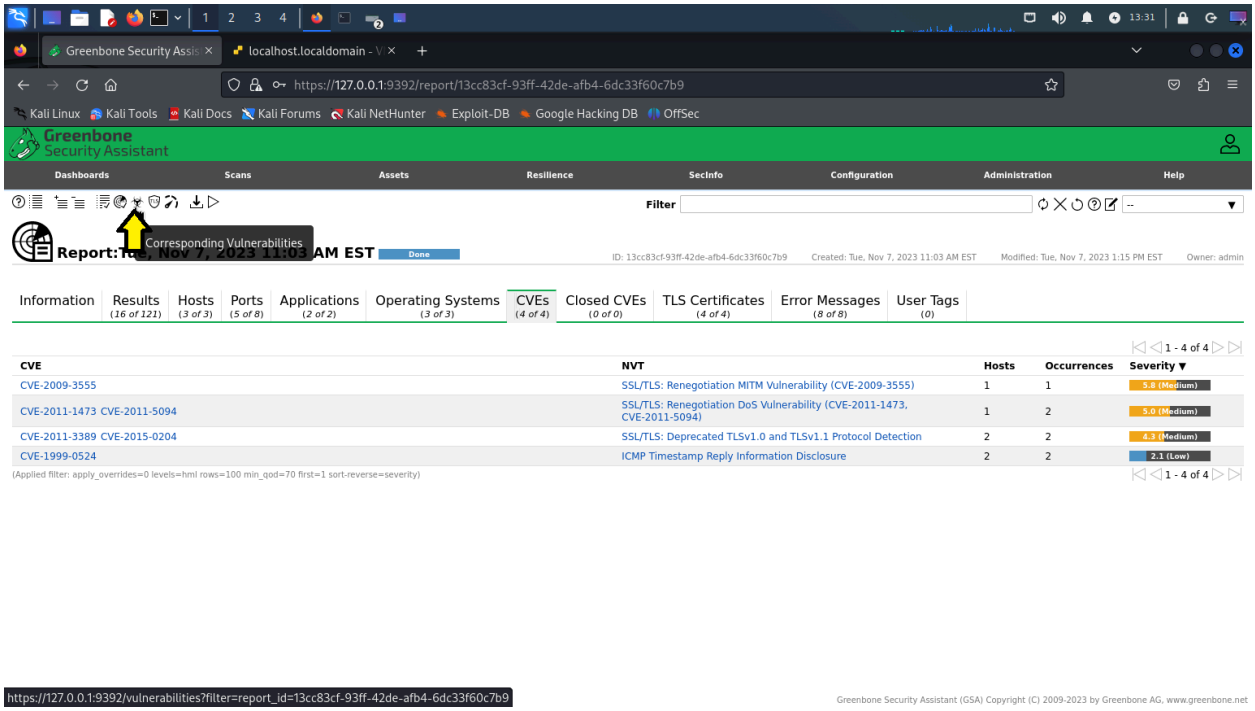


This is a screenshot of the associated CVEs pulled from a report. Notice

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:



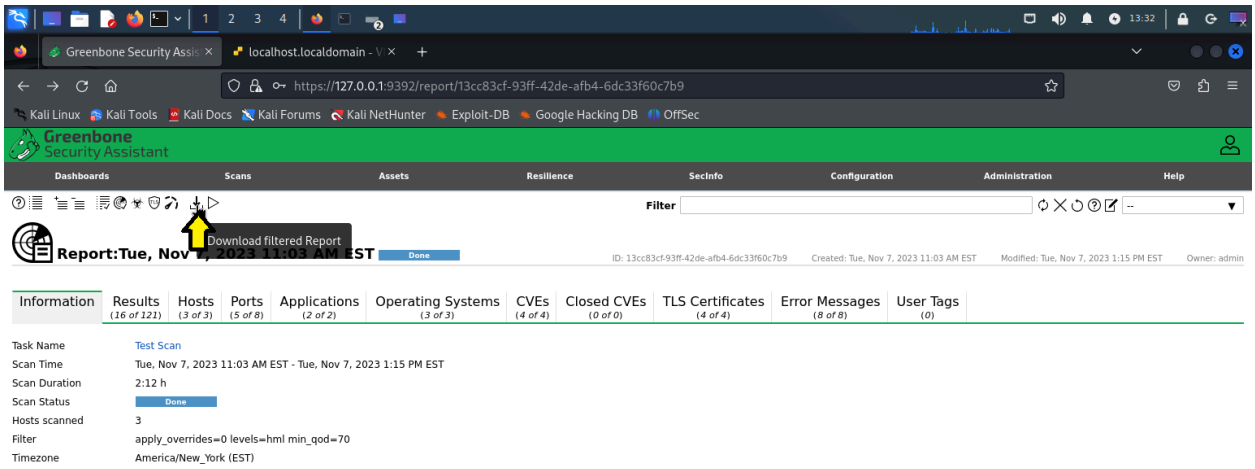
Click here to view the Corresponding Vulnerabilities

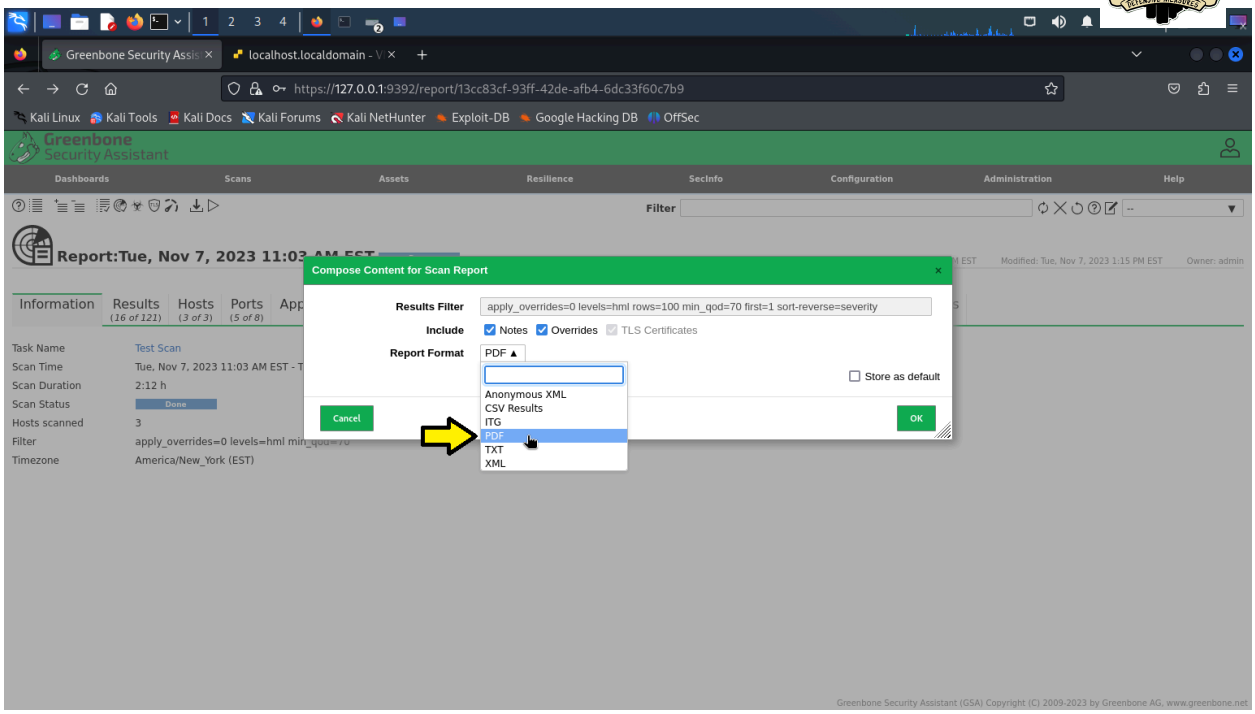


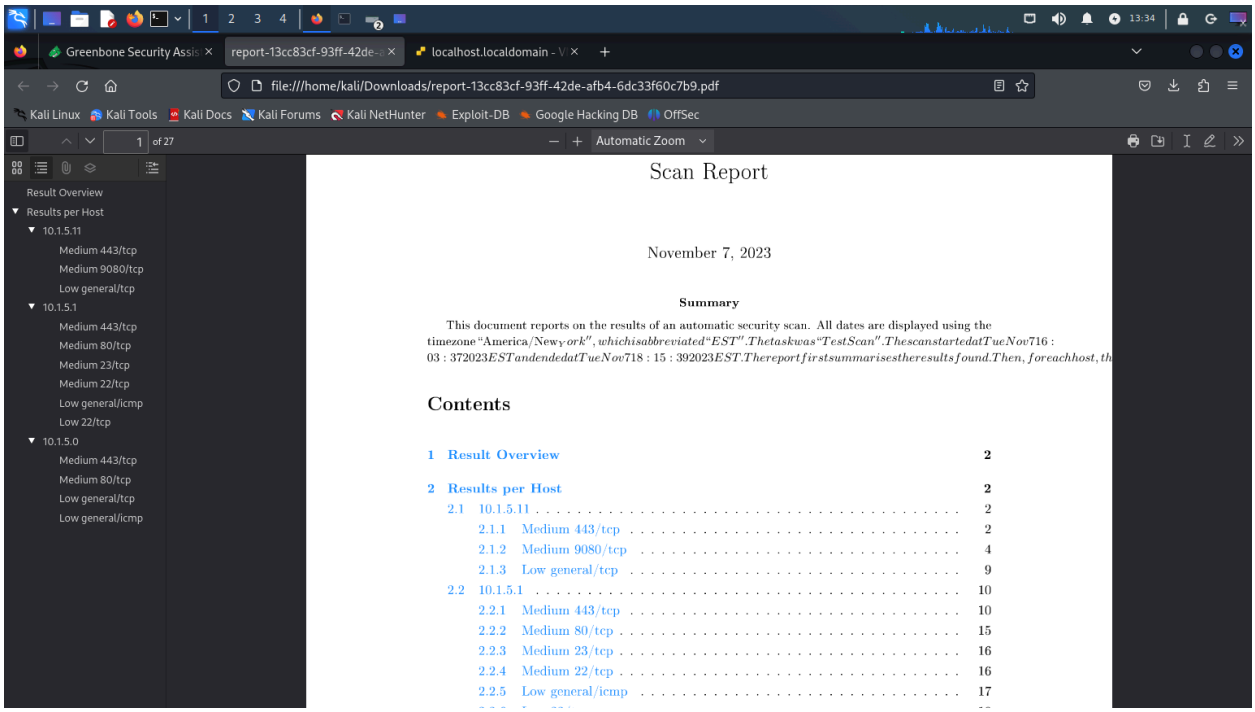
Another object of note is the 'Download Filtered Report' button, which looks like a downward facing arrow pointing into an open box.

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:



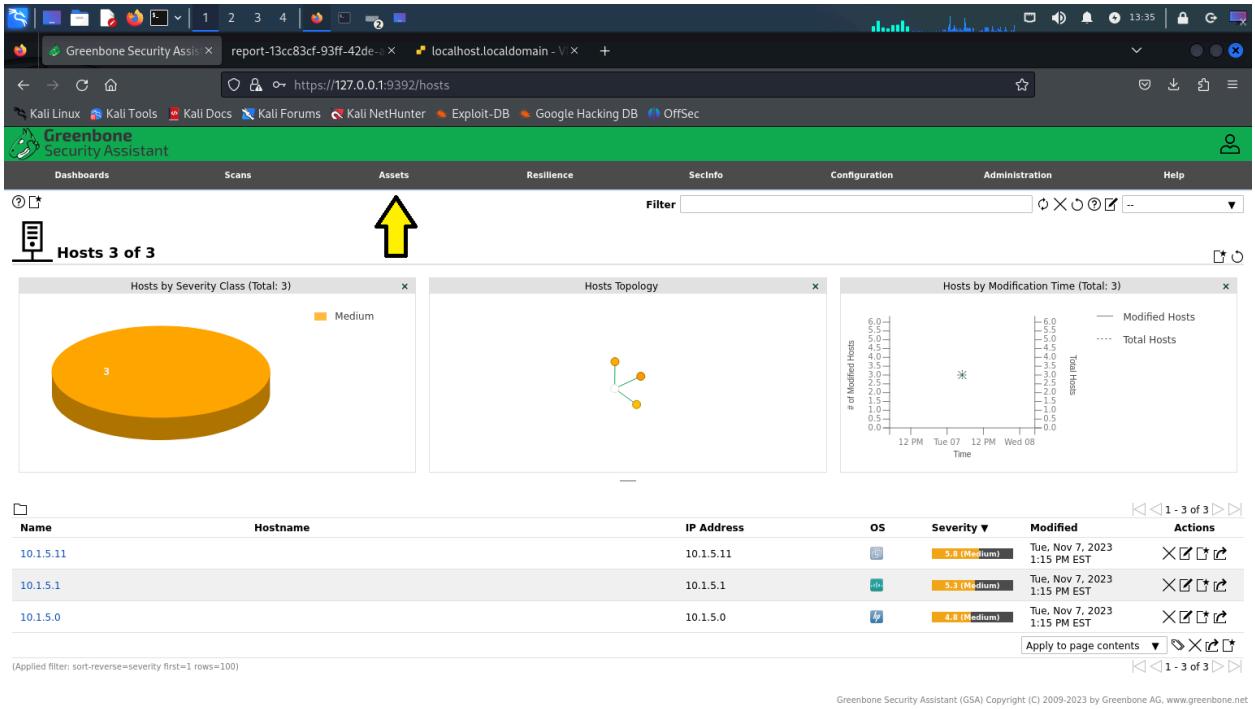




Another area of note is under the Assets tab under Hosts. This tab will show you a network map of your host topology which is color coded with their corresponding vulnerabilities' levels. Red is severe, orange is medium, blue is low, and gray is not vulnerable or not applicable. It will also

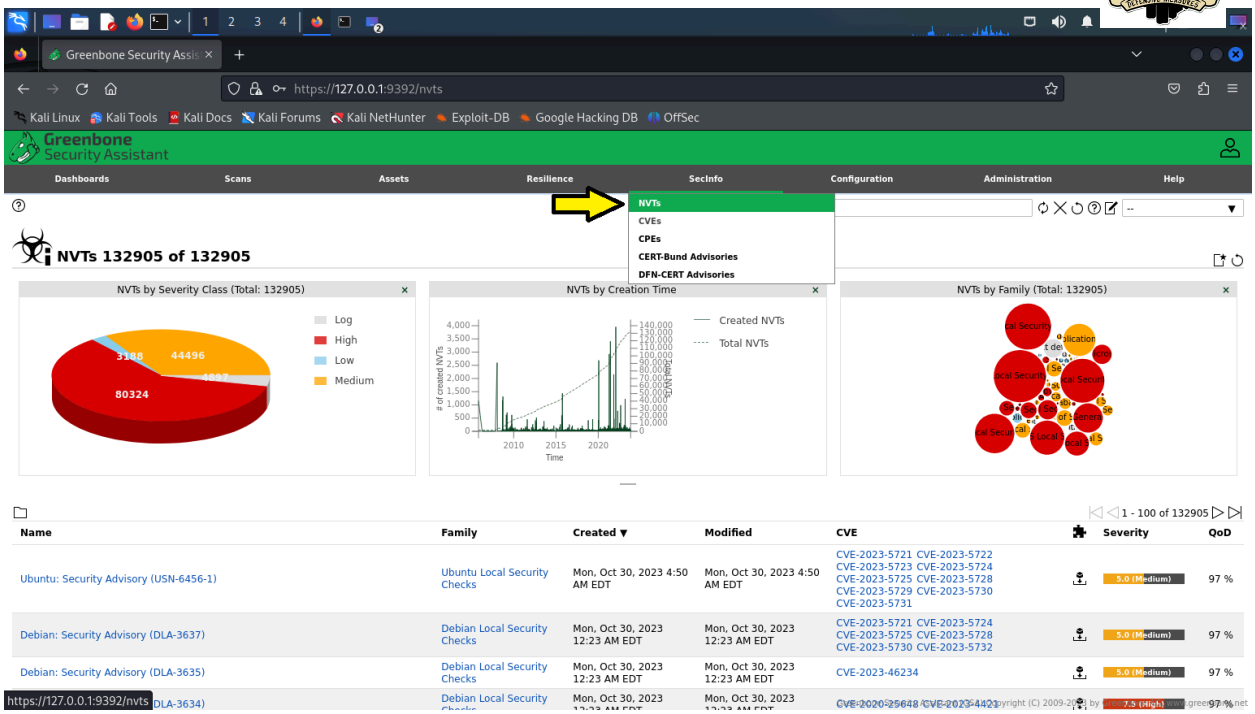
show you a list of scanned hosts, their IP address, their OS and the CVE severity level.

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

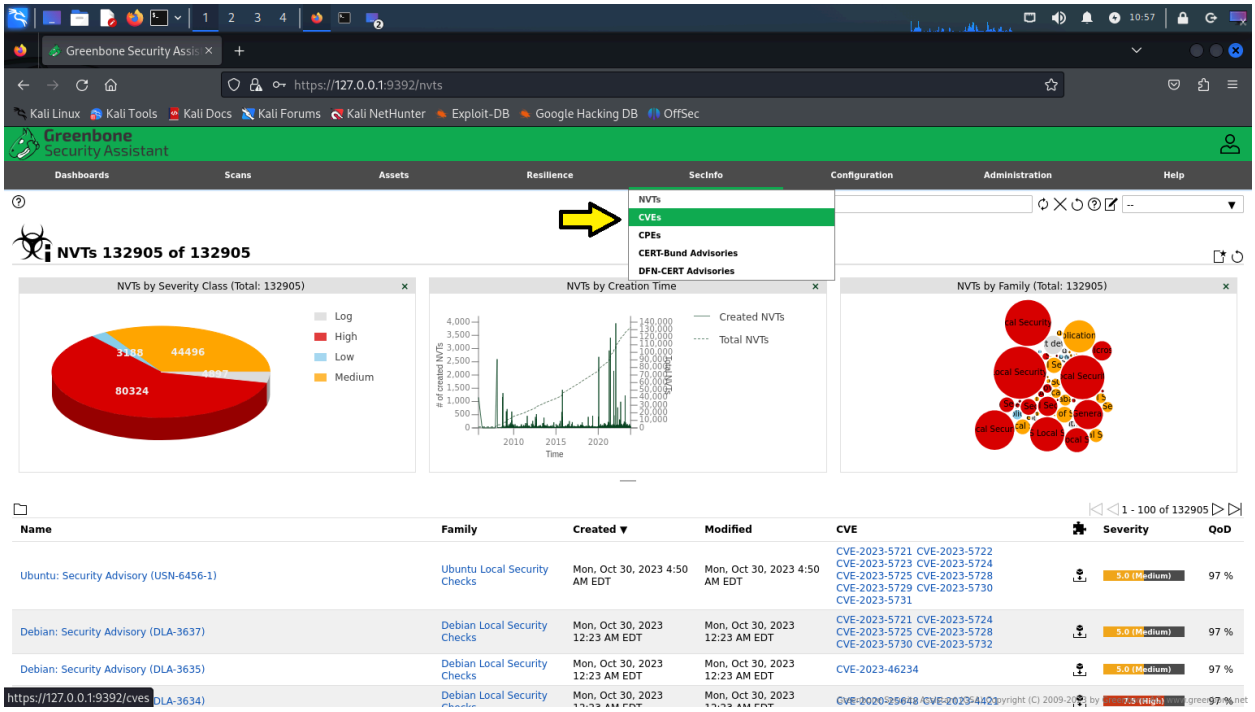


Further areas of interest are under SecInfo->NVTs, SecInfo->CVEs, Scans->Reports, Scans->Results and Scans->Vulnerabilities.

A picture of SecInfo -> NVTs

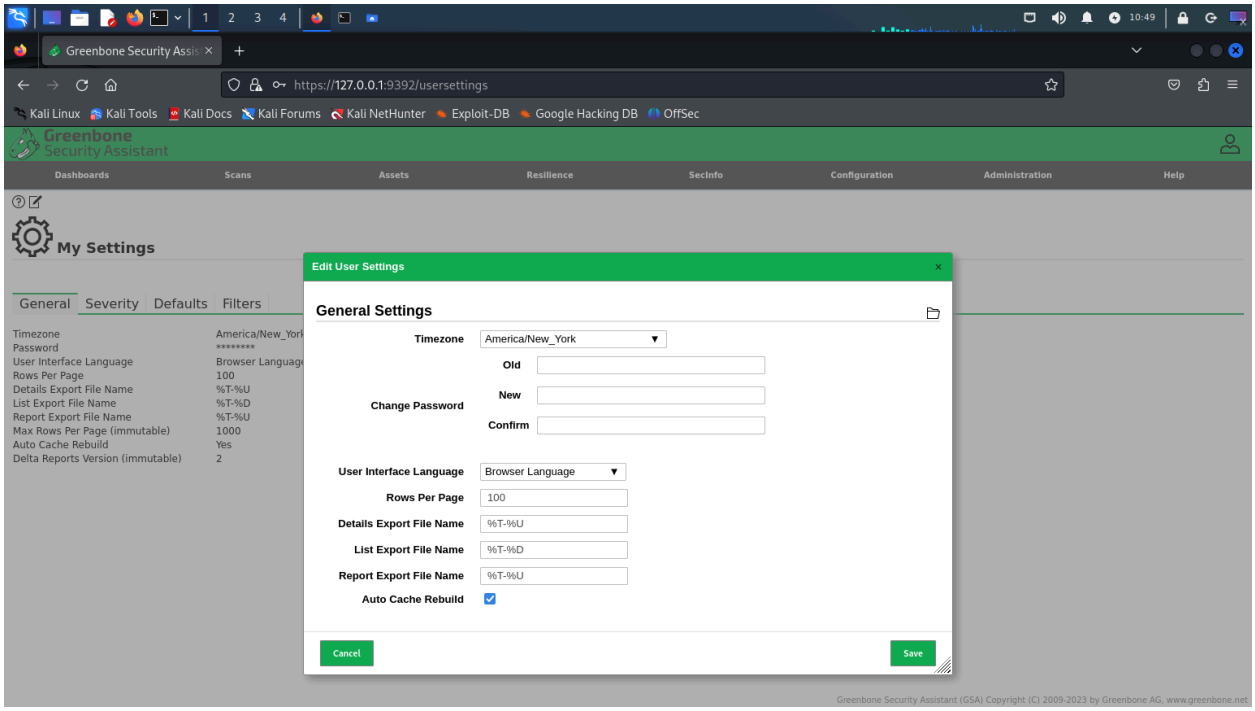


A picture of SecInfo -> CVEs



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.



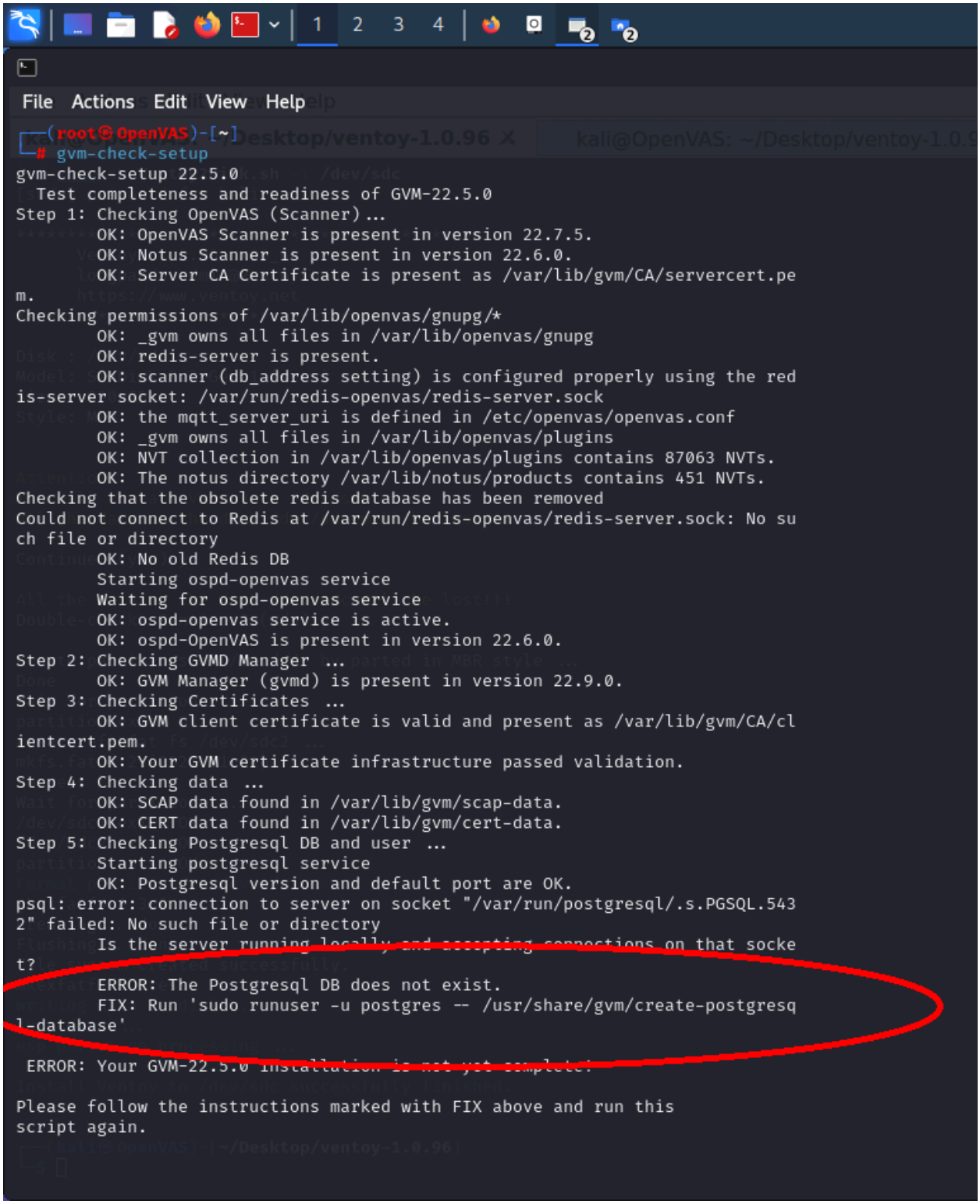
OpenVAS Baselining

- 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 ru... as sudo.



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