

Before anything, this documentation pertains to a WINDOWS machine only.

Computer Specs: 16GB RAM 1.5TB Storage AMD Ryzen 7 CPU

We will be using a virtual box with 5 virtual machines running. We will download and use Ubuntu Desktop as a general machine to use our other software that has a web gui. We will use Kali Linux Desktop as our attacker. Wazuh as our SIEM tool. OPNsense will be our main firewall. And finally, metasploitable2 will be our vulnerable machine.

I already have Ubuntu Desktop so I will be powering that up to have in the background until I need it. I have it set up to my bridged adapter. 2 CPU 2GB ram and 30GB storage for this machine.

Also create a notepad to have all the ip addresses and main gateway address in one place, which is what I did.

Using ifconfig, our first address to write down is 10.0.0.40.

With that being said, go to cmd on windows and type ipconfig.

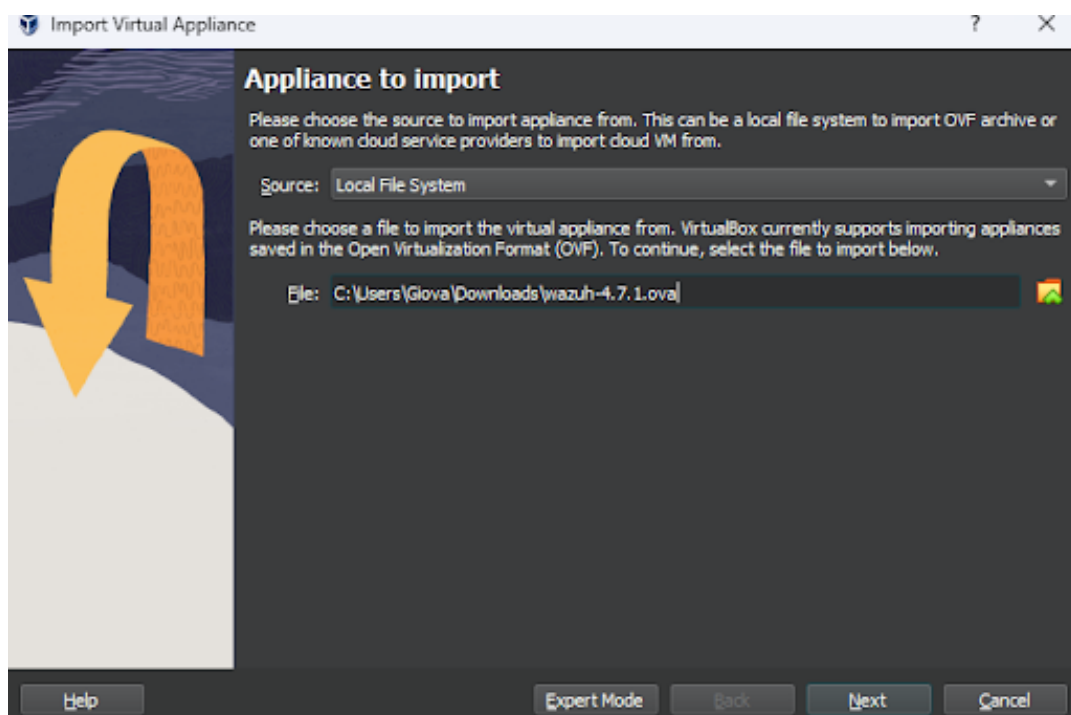
Write down the gateway address on the notepad, in which mine is 10.0.0.1

Next, we will be installing Wazuh.

I used this video for help. [Wazuh SIEM & XDR Agent Installation - Virtual Lab Building Series: Ep9](#)

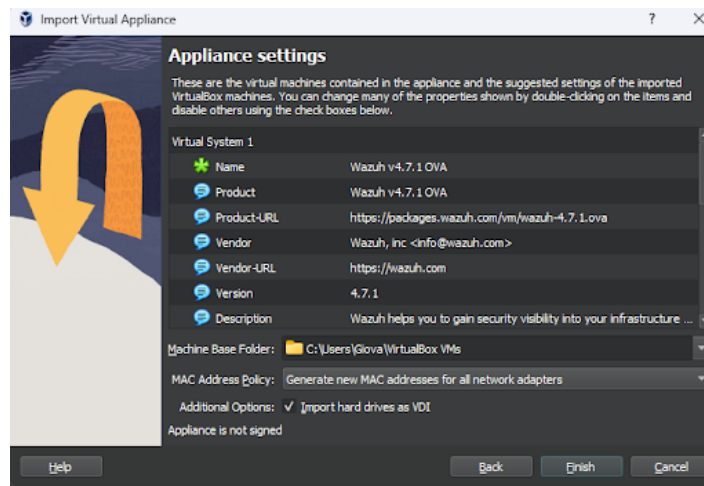
We will be using a ova file so the machine is already pre-built.

Simply use the import option in virtualbox to bring it in.

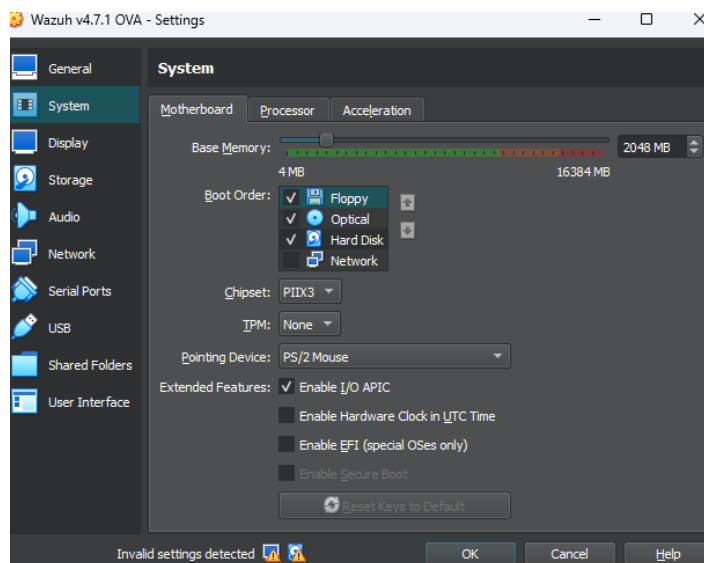
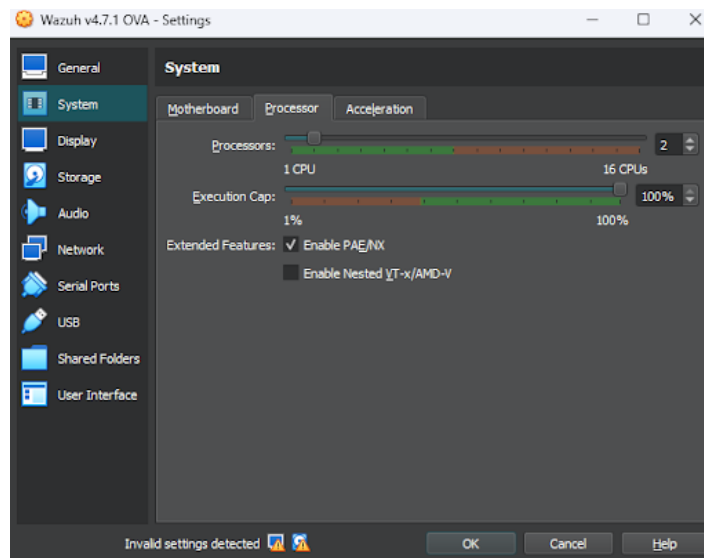


Click next

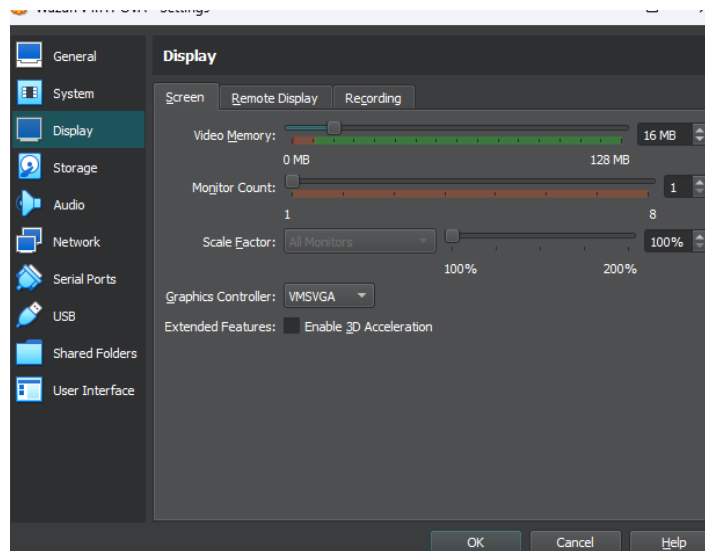
Make sure to give it new MAC addresses



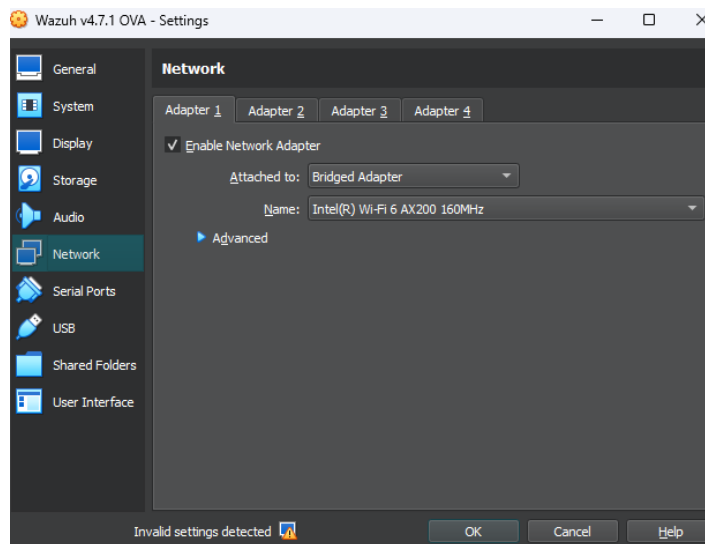
And click finish



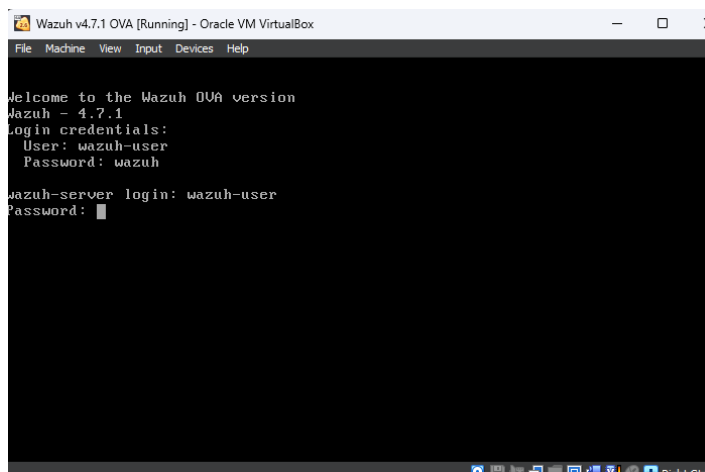
We will change its settings. Wazuh takes too much resources, so we will reduce that by making the machine have 2GB ram and only 2 processors.



Change the graphic controller so Wazuh doesnt glitch.



Next we will change the network adapter to Bridged adapter and then finally start the machine.



Login in with wazuh-user as the user and the password is wazuh

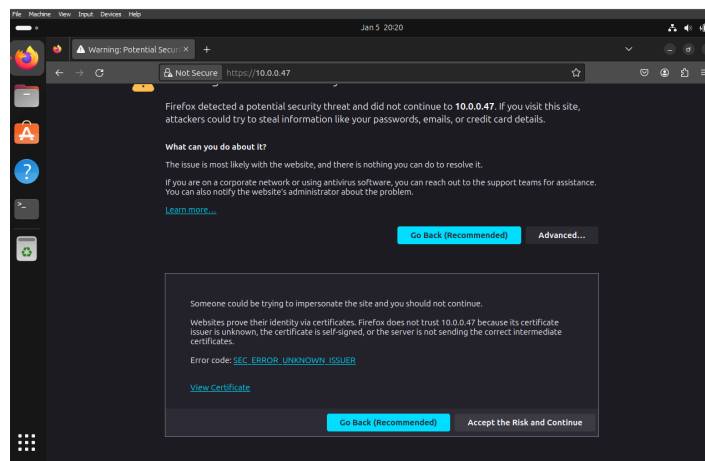
```
File Machine View Input Devices Help

No packages needed for security; 3 packages available
Run "sudo yum update" to apply all updates.
wazuh-user@wazuh-server ~]$ ifconfig
bash: ifconfig: command not found
wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.47 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::a00:27ff:feaa:7357 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:aa:73:57 txqueuelen 1000 (Ethernet)
    RX packets 53450 bytes 79730399 (76.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10463 bytes 788611 (770.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 49 bytes 2920 (2.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 49 bytes 2920 (2.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wazuh-user@wazuh-server ~]$
```

Once logged into the terminal, immediately ifconfig to get the wazuh address and write it in the notepad.



Now we are going to see if we can access wazuh webui

Head to the Ubuntu desktop and type in the ipaddress for wazuh in the search bar. It should look like this.

Click accept risk and continue, you should now have access to the webui. The username and password is Wazuh.

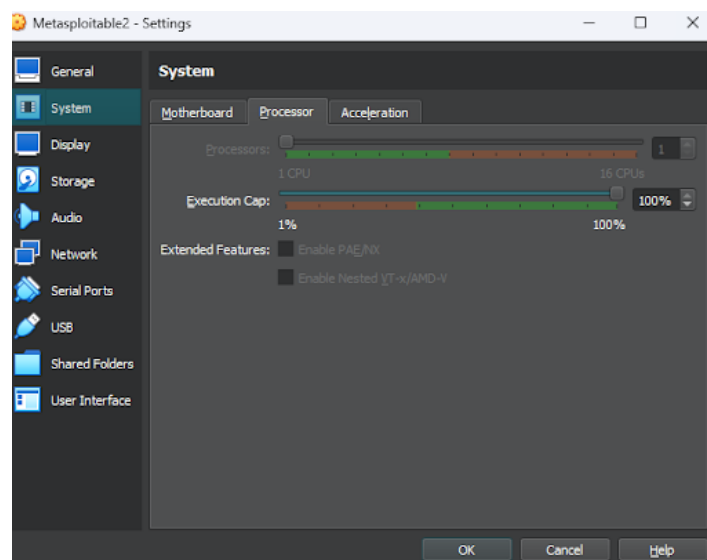
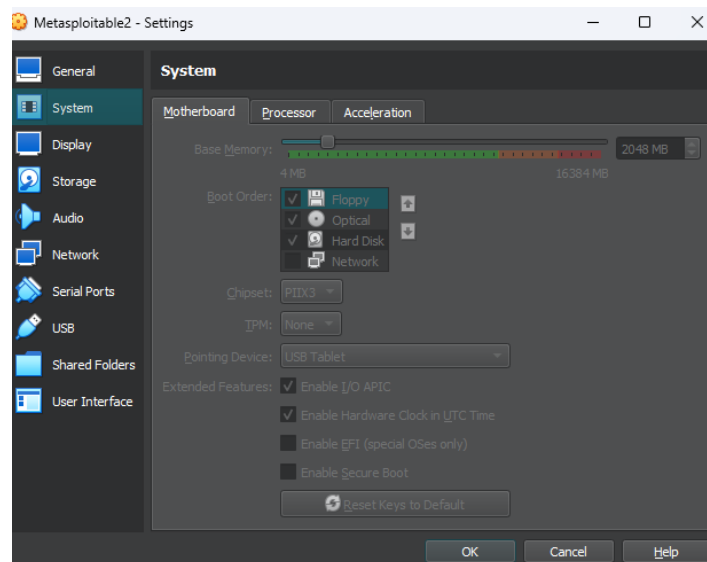
On to the next step.



Installing Metasploitable2 is a pretty straightforward process. Just download the iso and install it in virtual box.

This is a video that helped me install it, [How To Install Metasploitable 2 In VirtualBox - Home Hacking Lab Video 4](#)

I will show you how I have it configured though, so it belongs in the lab while not taking too many resources.



Really you just need it to be on the bridged network like all out other machines and give it 1 processor and 2GB ram.

```
Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

sfadmin@metasploitable:~$
sfadmin@metasploitable:~$
sfadmin@metasploitable:~$
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d3:51:83
          inet addr:10.0.0.35  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed3:5183/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1082 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:975190 (952.3 KB)  TX bytes:159036 (155.3 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1169 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:547533 (534.7 KB)  TX bytes:547533 (534.7 KB)

sfadmin@metasploitable:~$ _
```

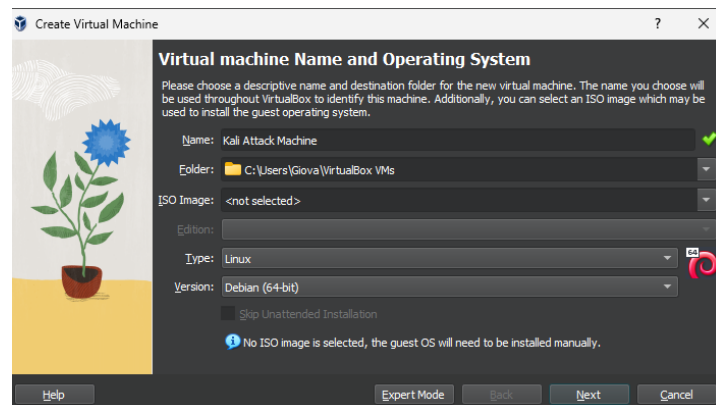
On the initial boot, you will have to login in which the user name and password are msfadmin.

Once again immediately go ifconfig and get the address for documentations sake and write it down.



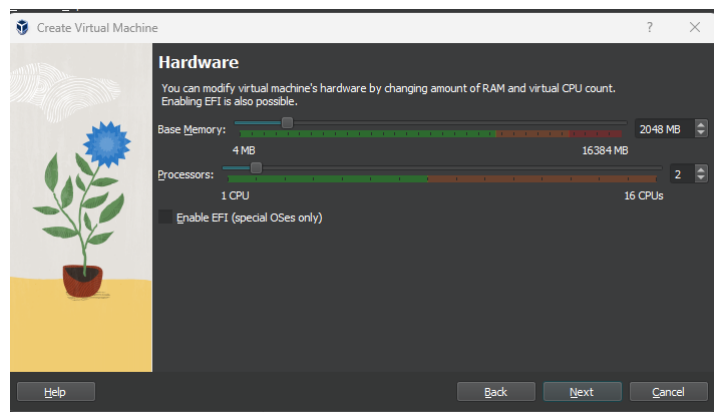
Up next is our attack machine, Kali Linux.

You can either download the prebuilt ova or the iso. In my example I am using the Virtual Hard Disk Drive.

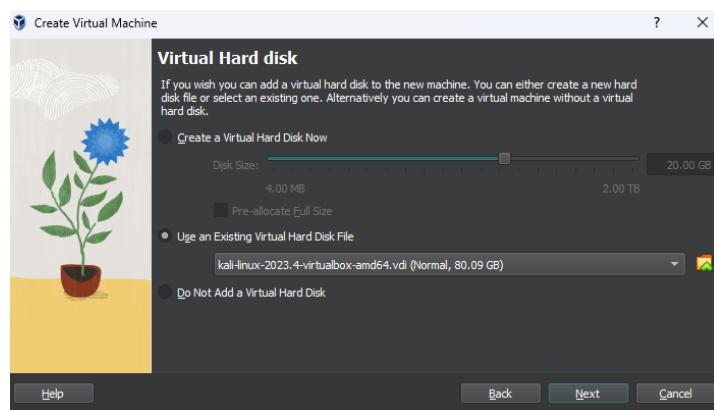


We will not be assigning an iso.

Click next

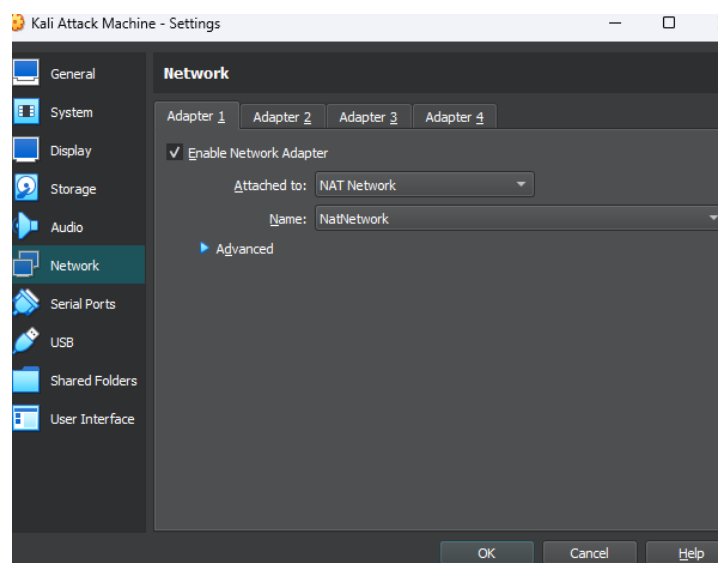


Give it 2 processors and 2GB ram. Click next

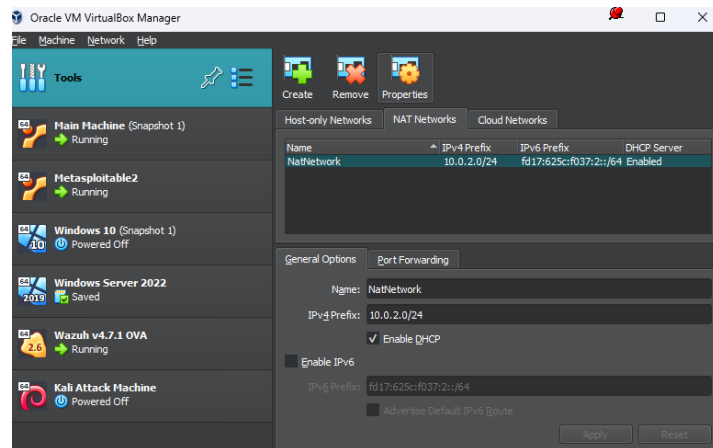


Click on use an existing virtual hard disk drive and look for the Kali vdi. It should have an orange cube icon.

Click next and finish.

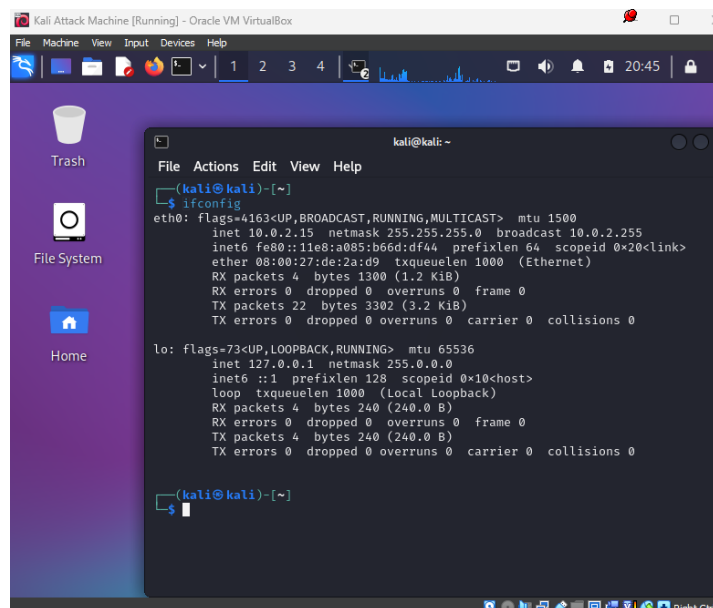


Before starting it up, make sure it is set up to the Nat Network.



If you dont have a nat network to work with, simply go to the Virtual Box tools and go to network.

Click on create within the Nat Networks tab to create one, which will be used for our Kali Machine.



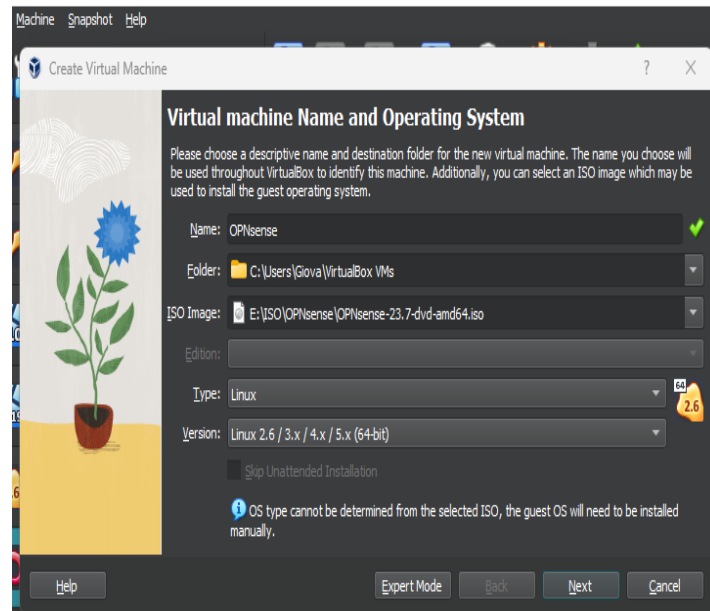
Lastly start up kali to see if it works.

The password and username will be both Kali.

Ifconfig and you will see it is on a different network!

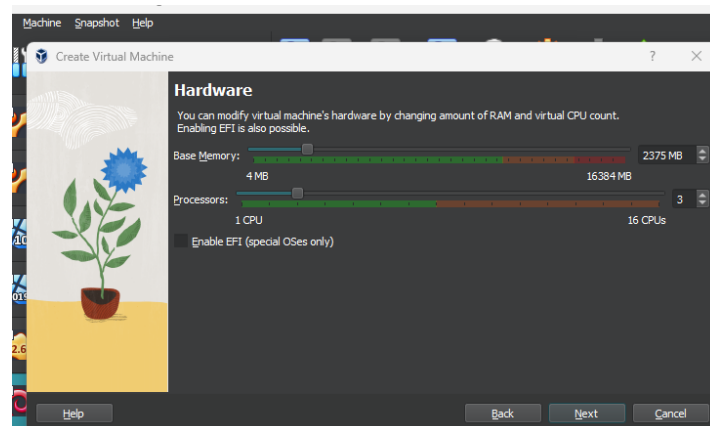


We will be finally installing our firewall, which will communicate with Wazuh. I chose this firewall specifically because it has a plugin for specifically connecting and sending logs to wazuh. Also it comes pre installed with suricata, a ids/ips tool.

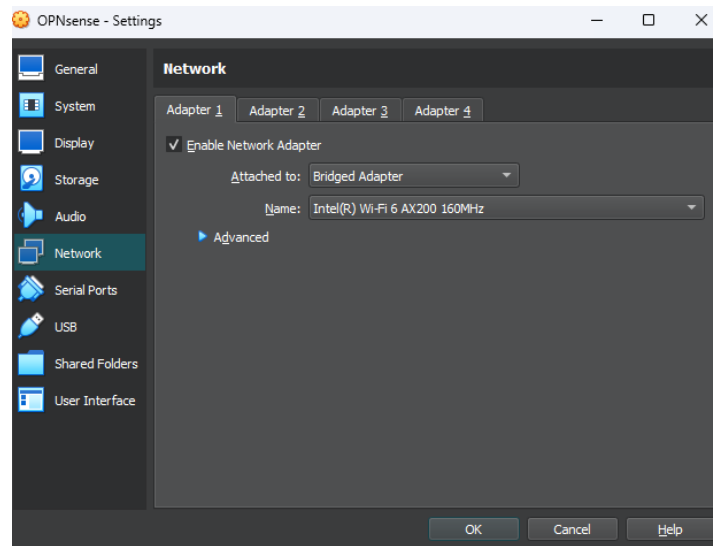


This installation will be through iso.

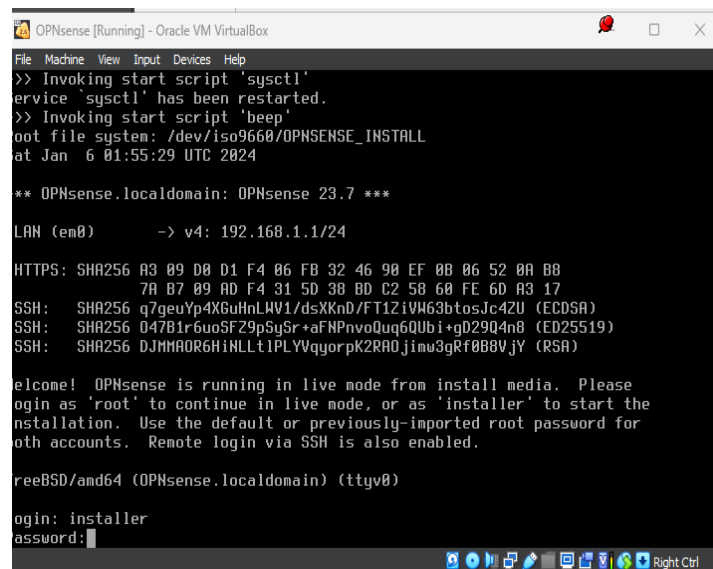
Click next



We will be giving this machine 2GB ram and 3 processors.

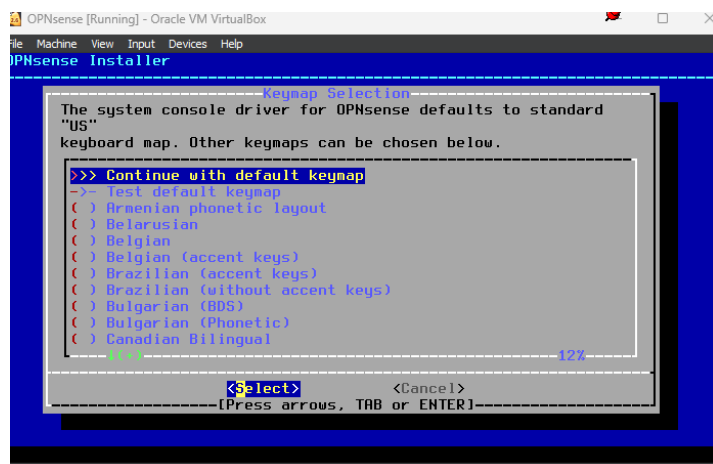


Make sure to check that this machine has bridged adapter.

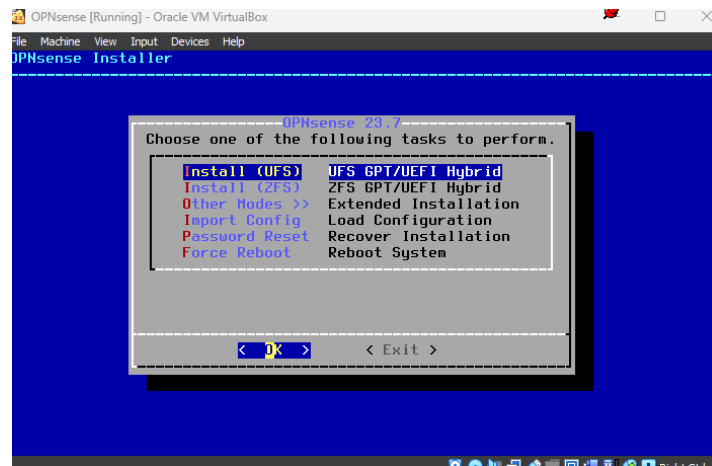


Now we can start it up.

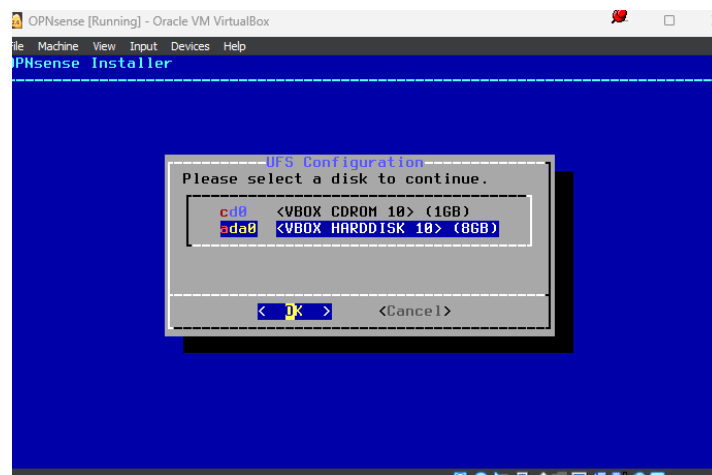
The login for the first boot is username root and password opnsense.



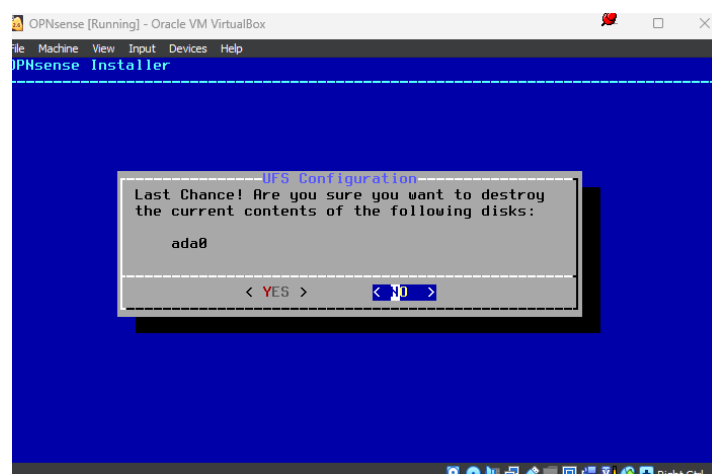
Press enter



Press enter again.

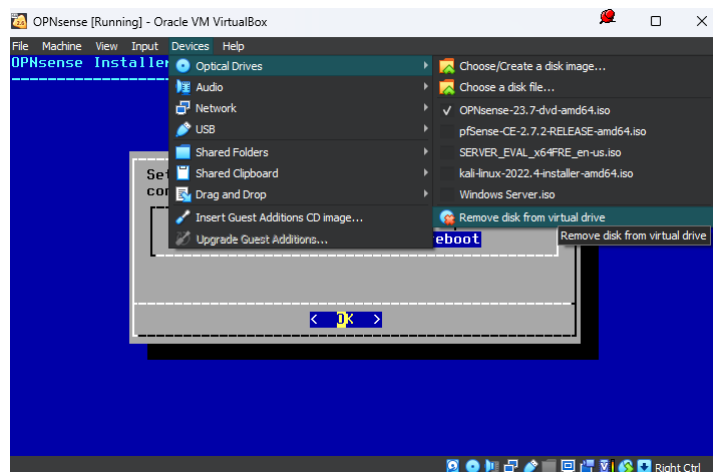


Press down arrow and then press enter.



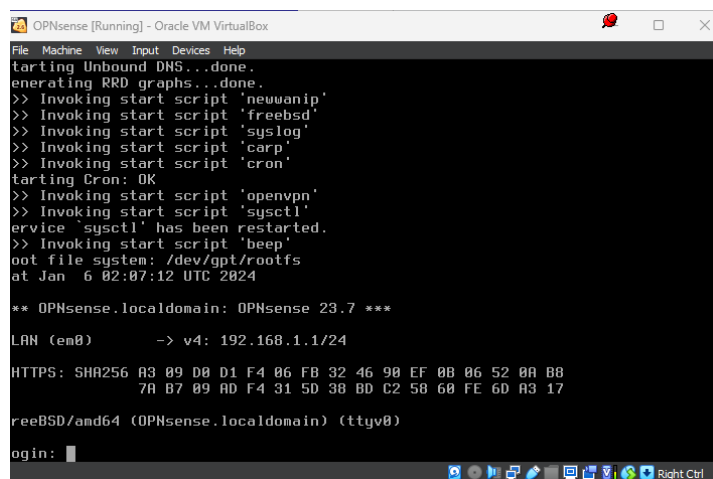
Right arrow and press enter

It should now be installing



This is a tricky part, when pressing down arrow to select exit and reboot, you hit enter.

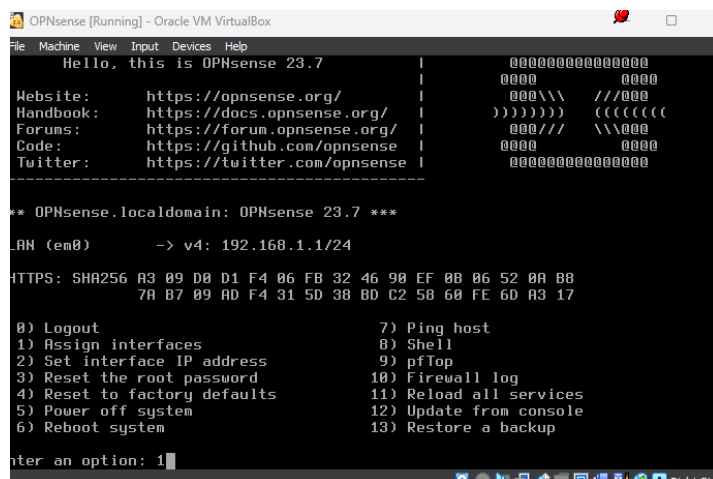
But while its shutting down, head to the devices tab > optical drives > remove disk from virtual drive.



Now you should be on this screen

The new username is root and the password is still opnsense. Login.

Now we are going to assign interfaces to have opnsense connect to our wan.



Press 1 to assign interfaces.

```
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Handbook: https://docs.opnsense.org/ | ))))))) (
Forums: https://forum.opnsense.org/ | @@@// \\
Code: https://github.com/opnsense | @@@@ @
Twitter: https://twitter.com/opnsense | @@@@@@@@@
-----
** OPNsense.localdomain: OPNsense 23.7 ***
LAN (em0) -> v4: 192.168.1.1/24
HTTPS: SHA256 A3 09 D0 D1 F4 06 FB 32 46 90 EF 0B 06 52 0A B8
7A B7 09 AD F4 31 5D 38 BD C2 58 60 FE 6D A3 17

0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 1
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

Type n on both of these options.

```
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HTTPS: SHA256 A3 09 D0 D1 F4 06 FB 32 46 90 EF 0B 06 52 0A B8
7A B7 09 AD F4 31 5D 38 BD C2 58 60 FE 6D A3 17

0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 1
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:
em0      08:00:27:fd:cf:9e Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
typing 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0
```

Here we will type em0 which is our bridged network.

```
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HTTPS: SHA256 A3 09 D0 D1 F4 06 FB 32 46 90 EF 0B 06 52 0A B8
7A B7 09 AD F4 31 5D 38 BD C2 58 60 FE 6D A3 17

0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 1
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:
em0      08:00:27:fd:cf:9e Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
typing 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0
```

After pressing enter you will be prompted to enter more options. Ignore them as we only need our WAN.

```
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

em0      08:00:27:fd:cf:9e Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished):
Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> em0
Do you want to proceed? [y/N]:
```

Press y for yes

```
OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Getting up routes...done.
Getting up gateway monitors...done.
Configuring firewall.....done.
Starting NTP service...done.
Starting Unbound DNS...done.
Starting web GUI...done.
Syncing OpenVPN settings...done.
Generating RRD graphs...done.

*** OPNsense.localdomain: OPNsense 23.7 ***

WAN (em0)      -> v4/DHCP4: 10.0.0.49/24

HTTPS: SHA256 A3 09 D0 D1 F4 06 FB 32 46 90 EF 0B 06 52 0A B8
              7A B7 09 AD F4 31 5D 38 BD C2 58 60 FE 6D A3 17

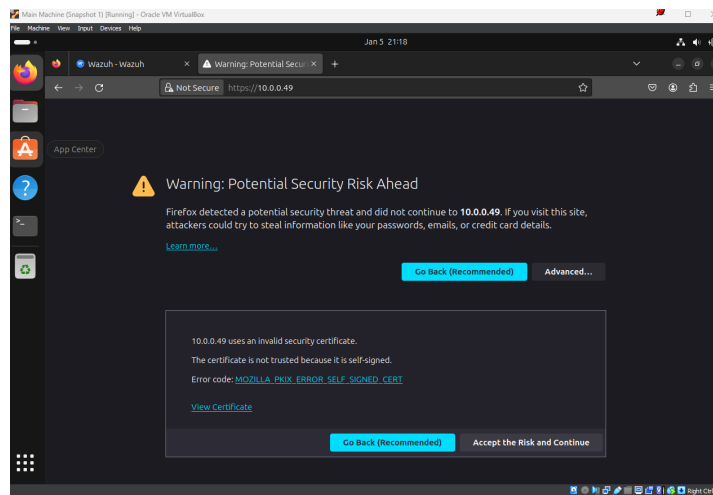
0) Logout              7) Ping host
1) Assign interfaces   8) Shell
2) Set interface IP address  9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system       12) Update from console
6) Reboot system          13) Restore a backup

Enter an option:
```

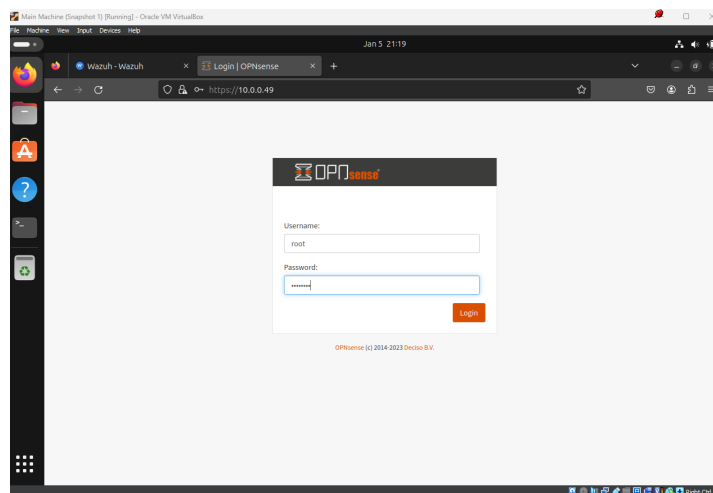
Take note of the new address, this will be the address we need to access the webui on our ubuntu desktop.

The next steps will now consist of having these machines interact with each other.

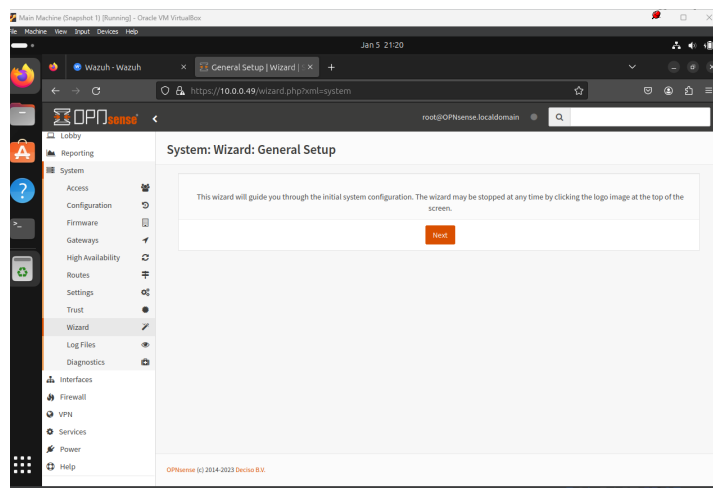




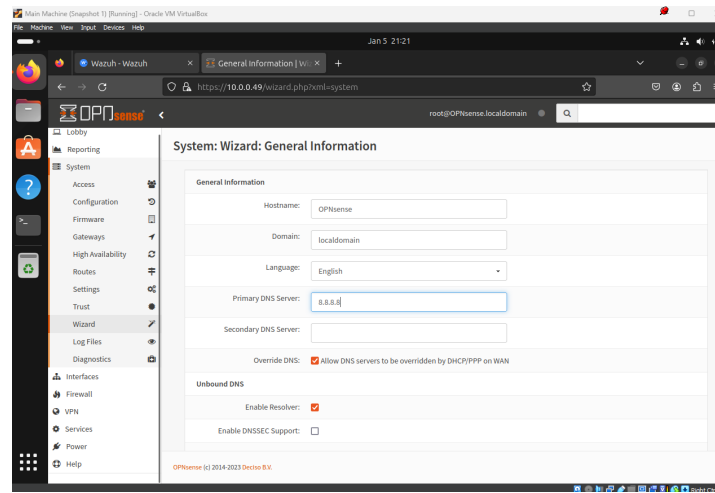
Lets go to our ubuntu desktop and type the opnsense address onto the search bar.  
Just like Wazuh, click accept the risks and continue.



It will use the same password and username as the opnsense server

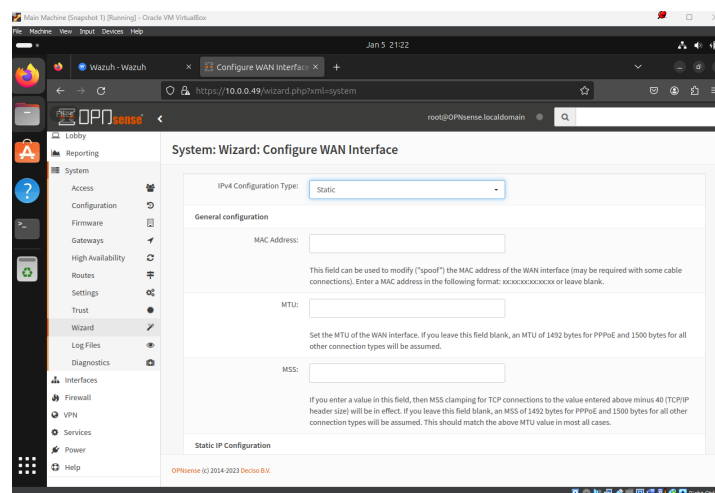


We'll now go through the wizard set up. Click next.



Follow these configurations. Then click next

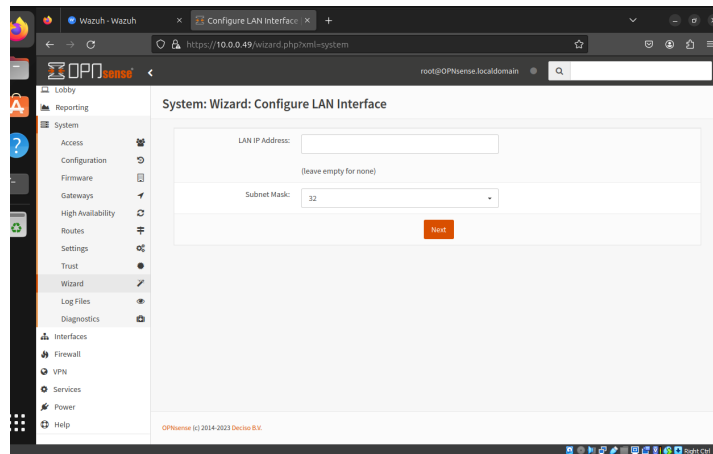
Click next again for time configuration.



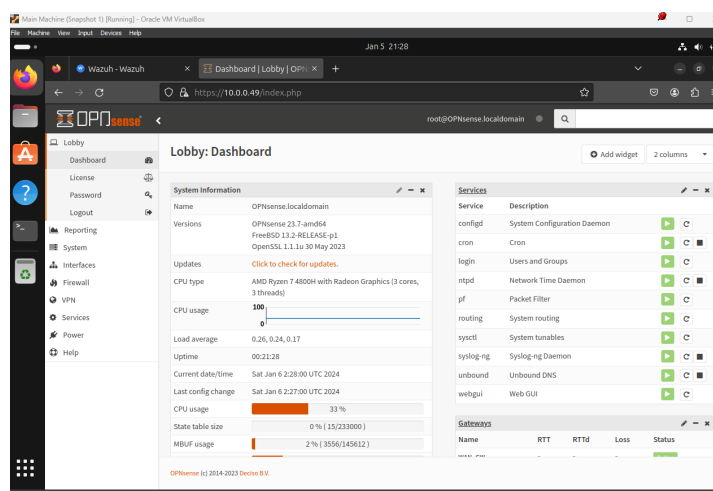
We want to change it to static.

Then enter the same address you are using to access opnsense web gui with a subnet of 24. To look for your gateway, use cmd on your host windows and type ipconfig. You should see you IPv4 address along with the default gateway. That is what I am using here. Click next after this part.

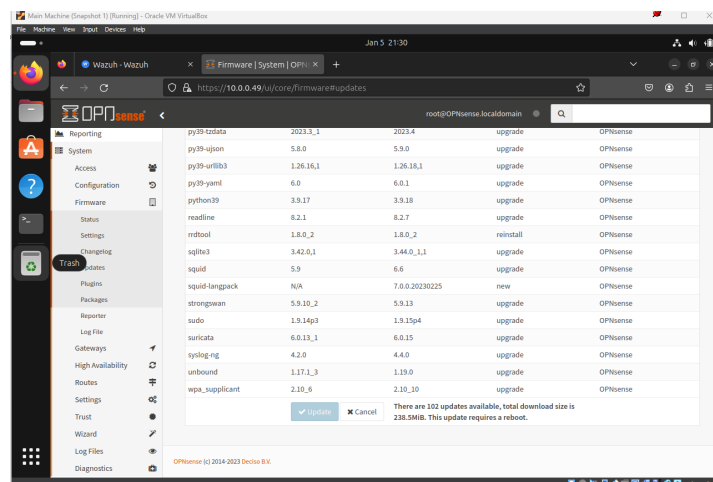




Leave this blank

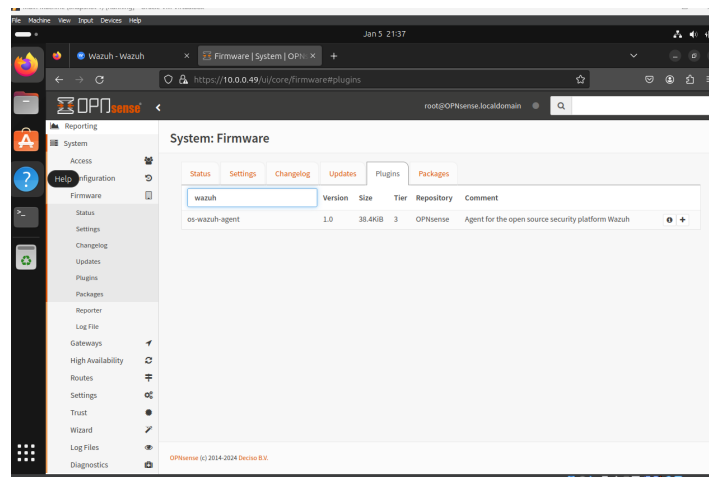


You will be prompted to change your password, that is up to you. I will leave it as is. Then you finally click reload and once it finishes setting up, it should look like this.



We are immediately going to go to look for updates. Go to System > Firmware > Updates

If there are updates needed go ahead and download them. I seem to have some so I went ahead and updated the system.



Updating will be crucial since we need the latest version to allow our Wazuh connection.

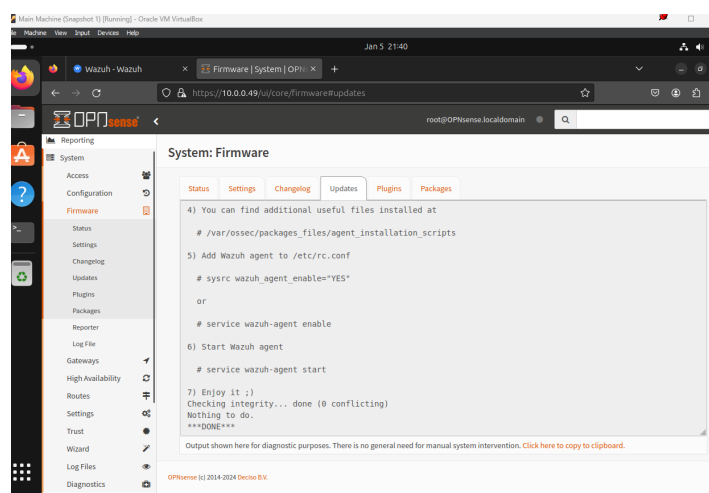
Now we are going to install a wazuh agent to allow syslogs from opnsense to be shown on the wazuh dashboard.

Will start by going to System>Firmware>Plugins

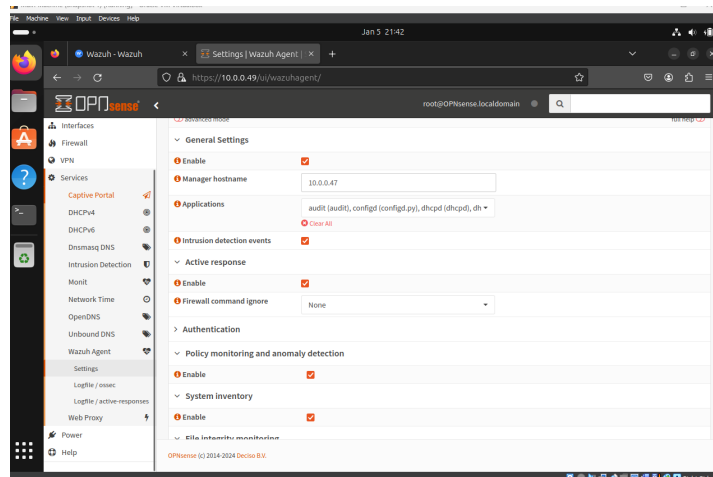
Then search for wazuh like shown above.

Also you should have the Wazuh dashboard open just to make sure we are connected.

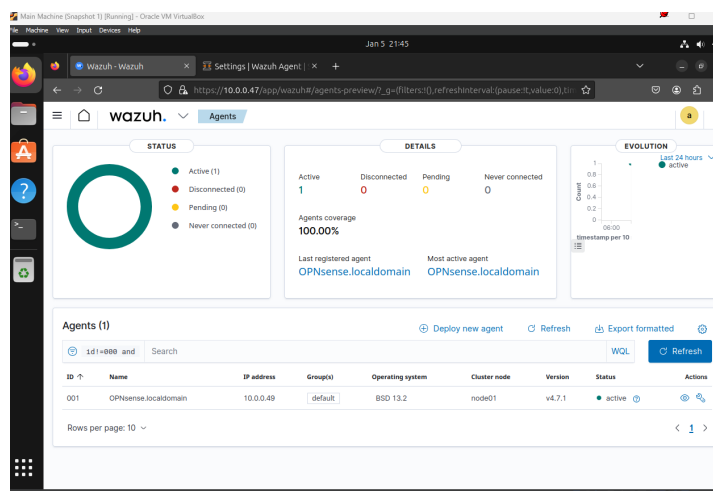
But now click the plus icon on the right and install.



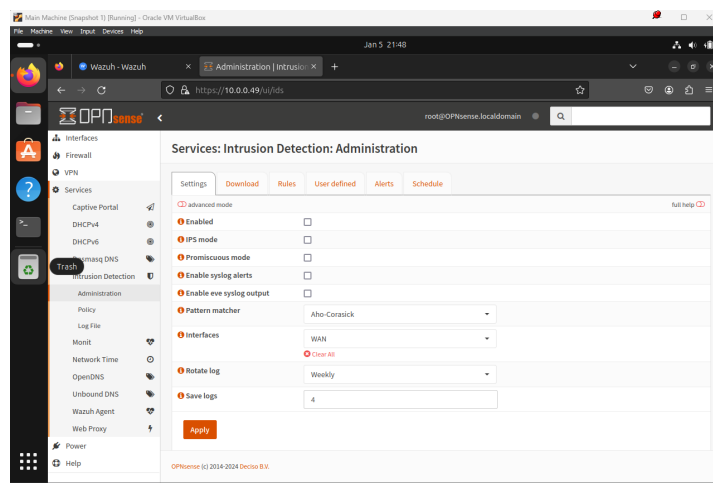
You should be met with this



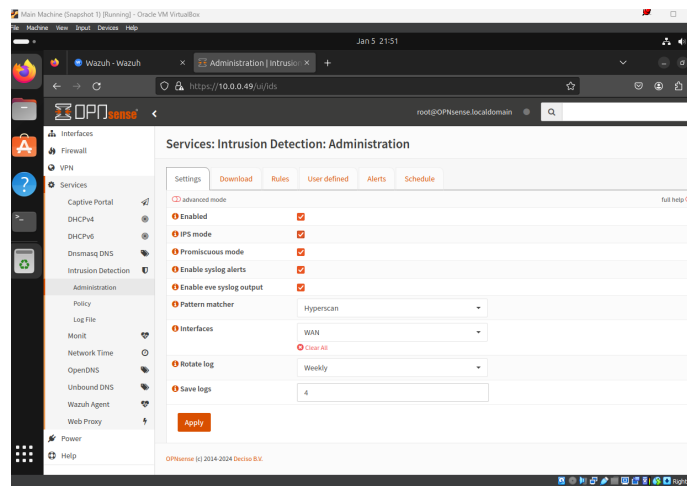
Now reload the page and then head to Services> Wazuh Agent> Settings Follow my  
Follow my configurations. Your wazuh ip address will be different than mine.  
Finally click apply.



Check back on the wazuh dashboard and we should now have been connected!

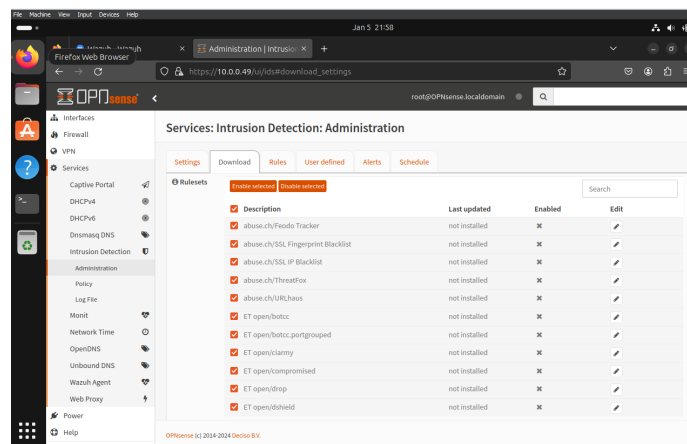


Head back to the opnsense dashboard and head to Services> Intrusion Detection > Administration.



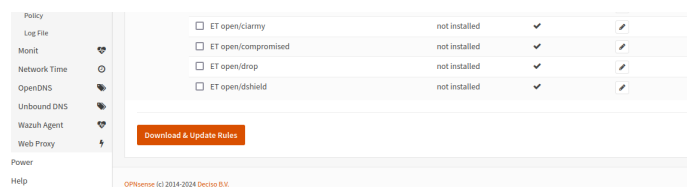
Now follow these configurations.

Then click apply.



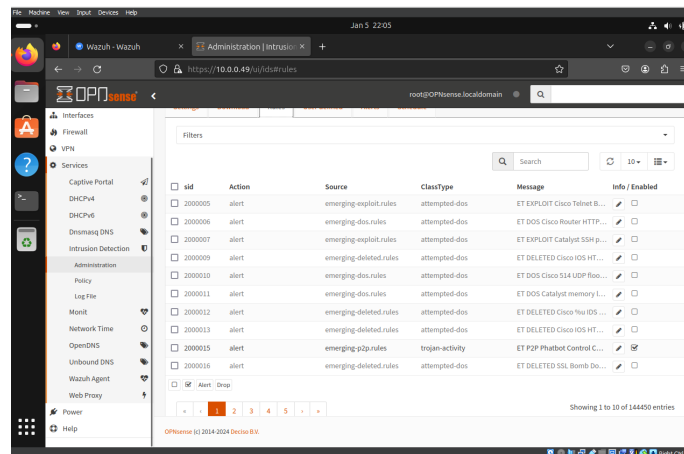
Next we will download rules for suricata. On the same page navigate to the download tab.

Tick the descriptions box to select all items. Then click on enable selected.



Then click download and update rules

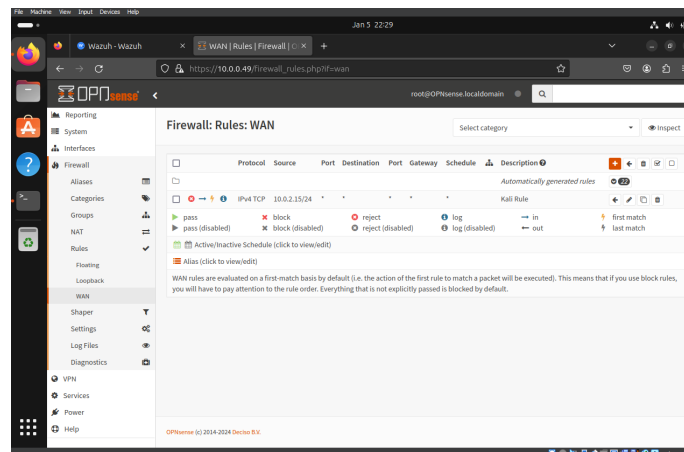
In the meantime, powerup the kali attack machine if you dont have it on yet. We will need it later.



After the download finishes, head to the rules tab and you should now have a ton of rules set for any attack!

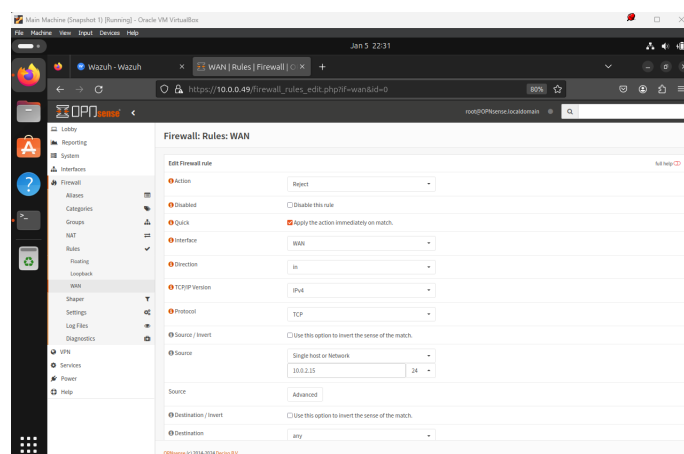
We will now try to make alerts for Suricata to pick up along with Wazuh.

First we will set up a firewall rule that has our attack machine ip address in mind.

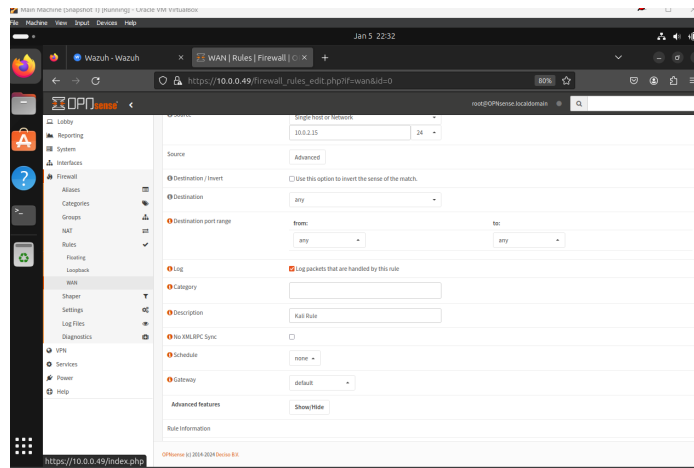


From the dashboard, we head to Firewall> Rules> Wan.

As you can see I already set up my firewall rule called Kali but I will show you what I set up.



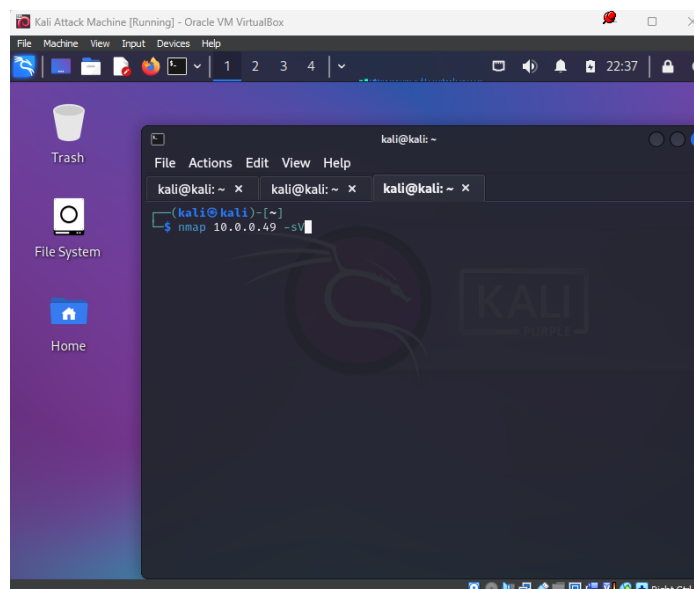
As you can see, I made it so the firewall rule will reject what's coming from the source address which is the same address that the Kali Attack Machine is using.



Scrolling a bit lower, we have to make sure to tick the box for collecting logs. After that, we can save and exit.

You will get a blue box telling you to apply changes, click apply and that should do it. Without applying changes the firewall will not take effect.

Now we will head to our kali machine and start our first attack, an nmap scan!



Lets try using this.



The screenshot shows the Wazuh Security Alerts page. The table lists several alerts, with the first five being Suricata alerts and the last four being pfSense firewall blocks events.

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 5, 2024 @ 22:28:58.693			Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed	3	86601
Jan 5, 2024 @ 22:28:58.651			Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed	3	86601
Jan 5, 2024 @ 22:28:58.649			Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed	3	86601
Jan 5, 2024 @ 22:28:58.647			Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed	3	86601
Jan 5, 2024 @ 22:24:06.635	T1110	Credential Access	Multiple pfSense firewall blocks events from same source.	10	87702
Jan 5, 2024 @ 22:20:06.432	T1110	Credential Access	Multiple pfSense firewall blocks events from same source.	10	87702
Jan 5, 2024 @ 22:18:05.341	T1110	Credential Access	Multiple pfSense firewall blocks events from same source.	10	87702
Jan 5, 2024 @ 22:06:38.592	T1110	Credential Access	Multiple pfSense firewall blocks events from same source.	10	87702

And through Wazuh...

The screenshot shows the Wazuh Security events page with a list of alert details.

@timestamp	2024-01-06T03:26:58.693Z
_id	sziP3wBdpd4vq3MVLB
agent.id	001
agent.ip	10.0.0.49
agent.name	OPNsense.localdomain
data.alert.action	allowed
data.alert.category	Web Application Attack
data.alert.cid	1
data.alert.metadata.affected_product	Any
data.alert.metadata.attack_target	Client_and_Server
data.alert.metadata.created_at	2017_06_08
data.alert.metadata.deployment	Perimeter
data.alert.metadata.former_category	SCAN
data.alert.metadata.performance_impact	Low
data.alert.metadata.signature_severity	Informational

The screenshot shows the Wazuh Security events page with a list of alert details.

data.http.length	0
data.http.protocol	HTTP/1.1
data.http.uri	/hmap1
data.in_face	em0
data.proto	TCP
data.src_ip	10.0.0.11
data.src_port	52969
data.timestamp	2024-01-06T03:26:58.498358+0000
data.tx_id	0
decoder.name	json
id	1704511618.26721
input.type	log
location	/var/log/suricata/eve.json
manager.name	wazuh-server
rule.description	Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed
rule.firedtimes	4
rule.groups	ids, suricata

As you can see, the attack was detected.