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 Linus Desktop as our attacker. Wazuh as our SIEM tool. OPNsense will be ou 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 iI 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.

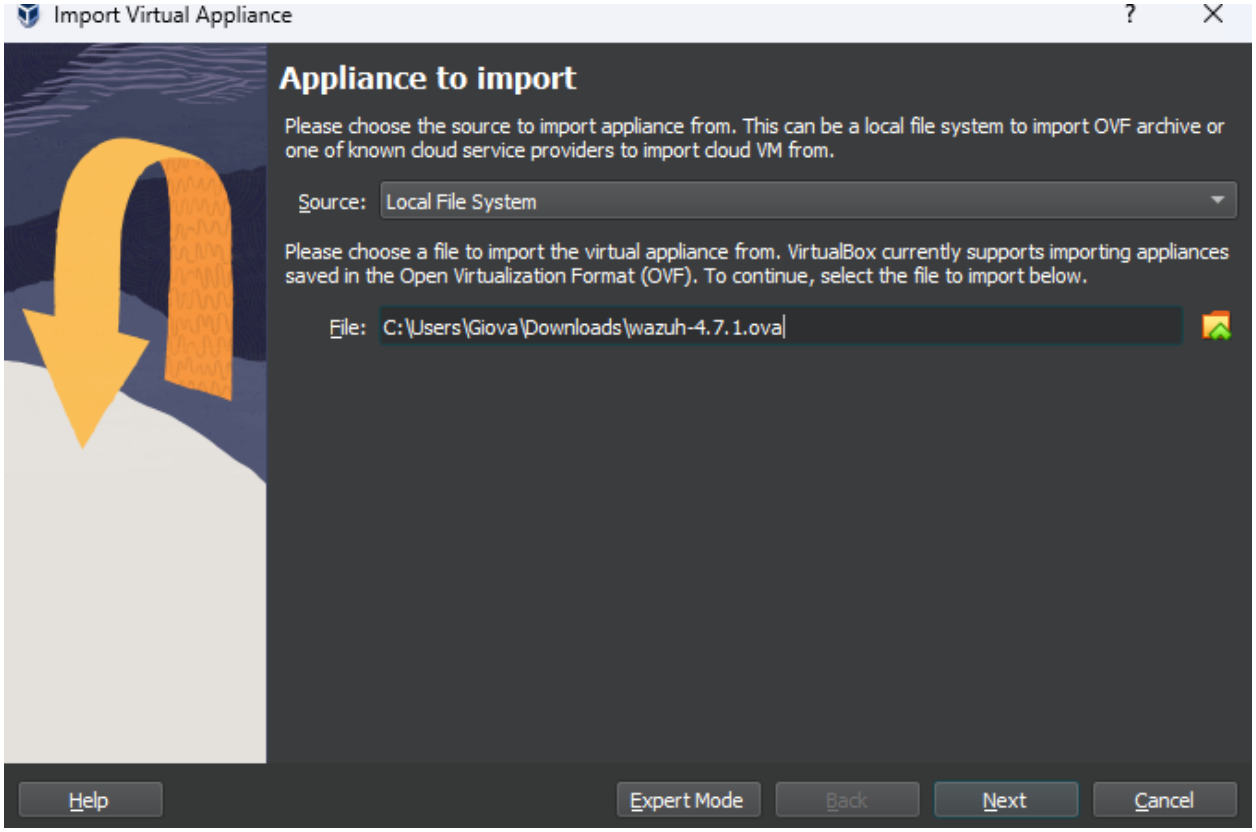
Write down the gateway address on the notepad, in which mine is 10.0.0.1

Next, we will be installing Wazuh.

I used this video for help. Wazuh SIEM & XDR Agent Installation - Virtual Lab Building Ser…

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.

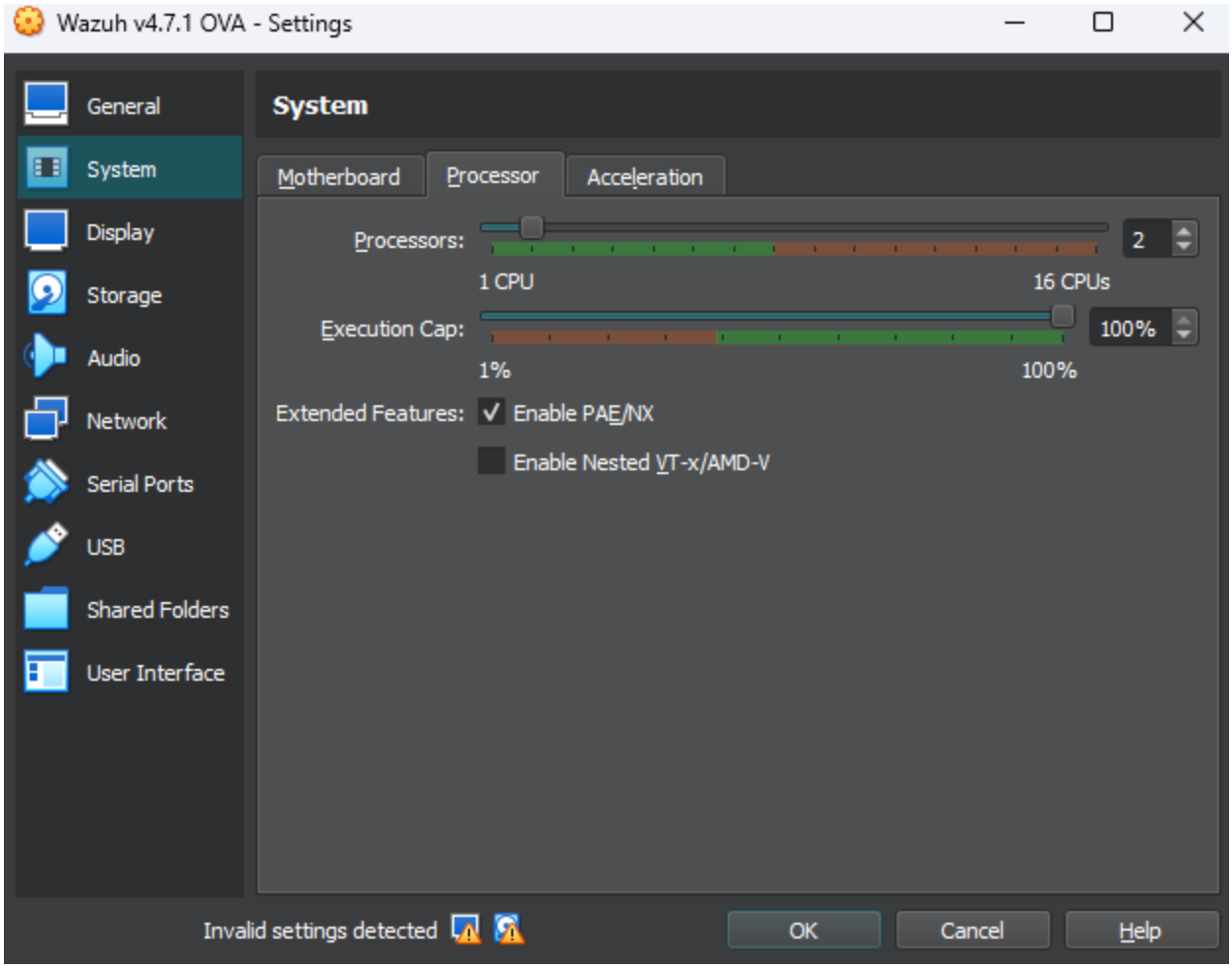


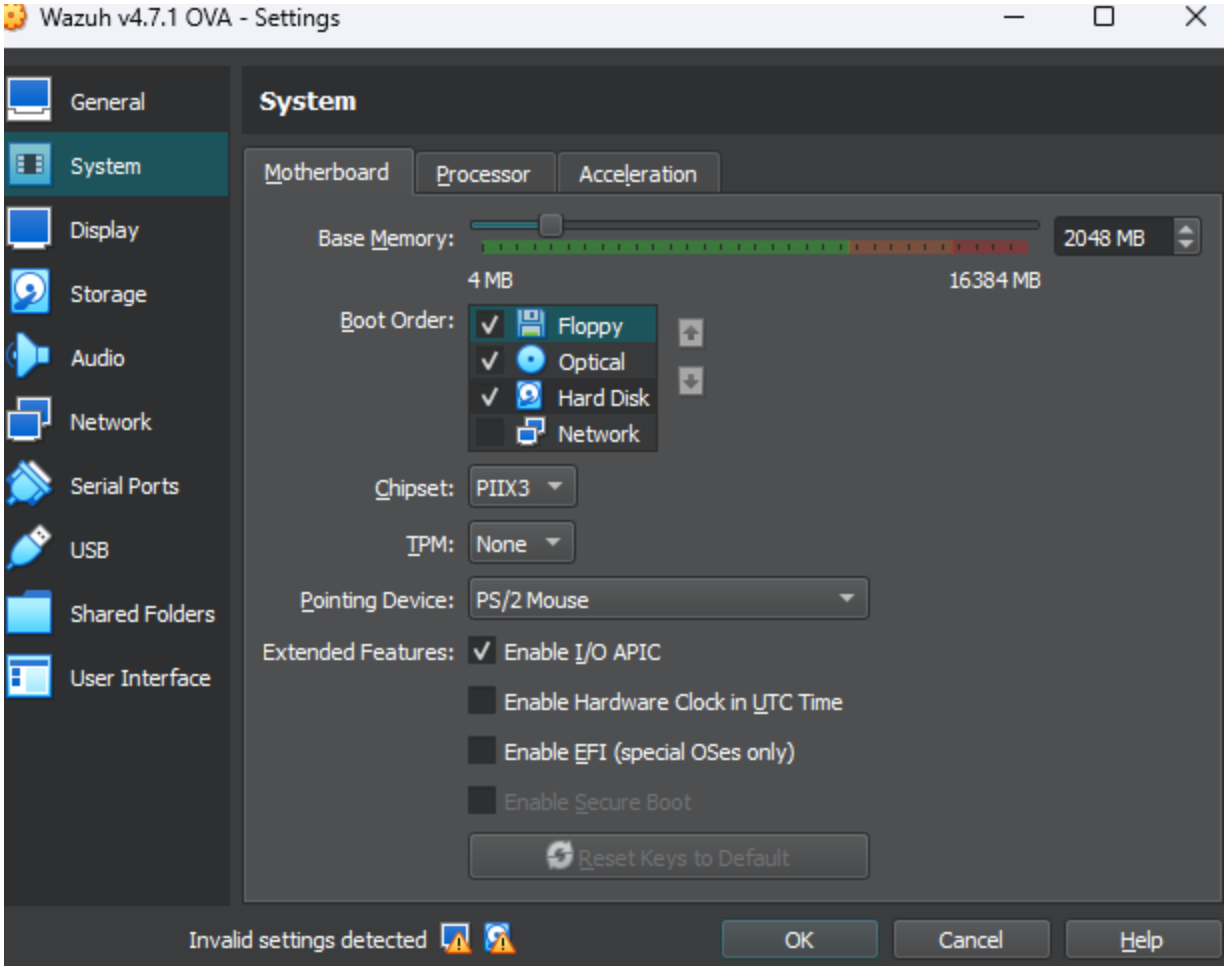
Click next

Make sure to give it new MAC addresses

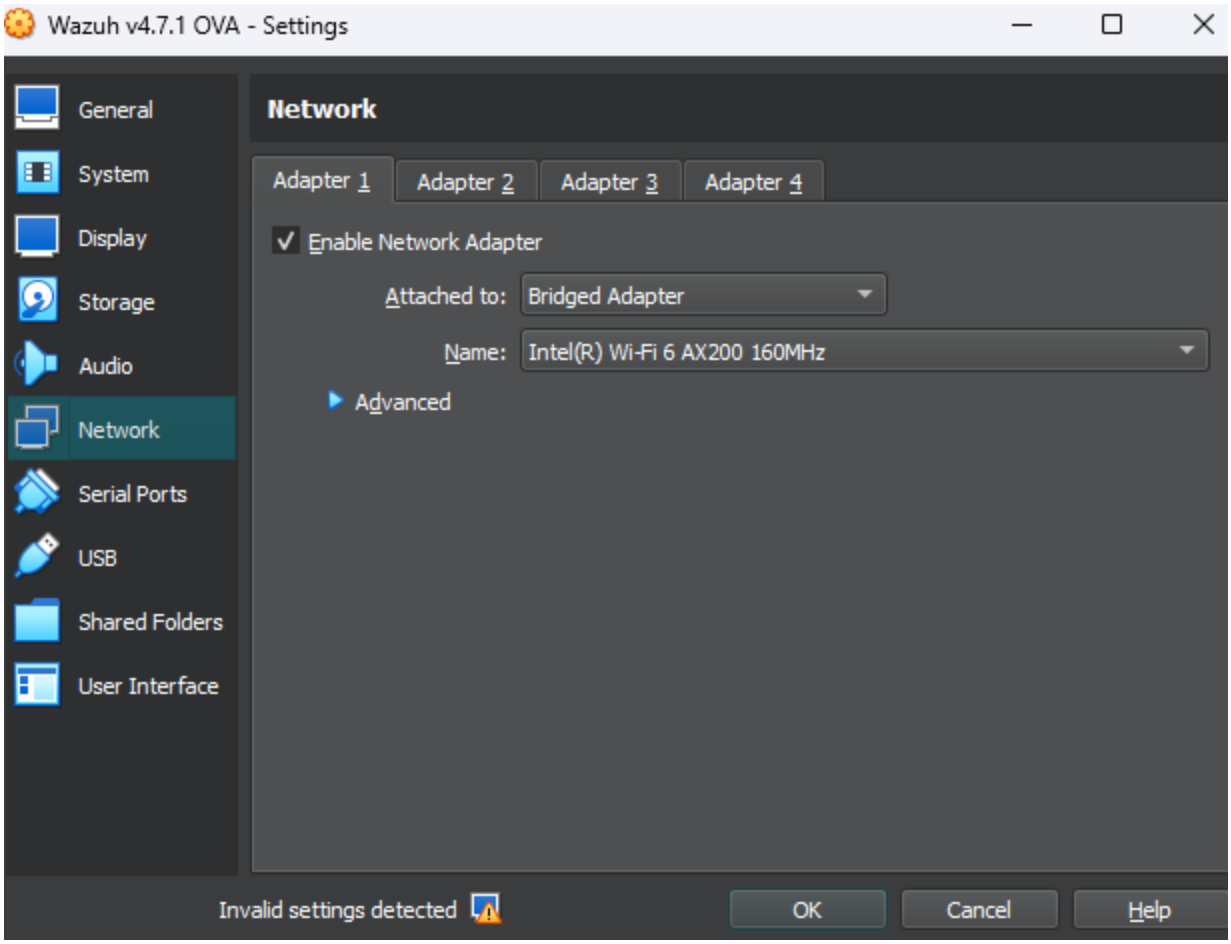
And click finish

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

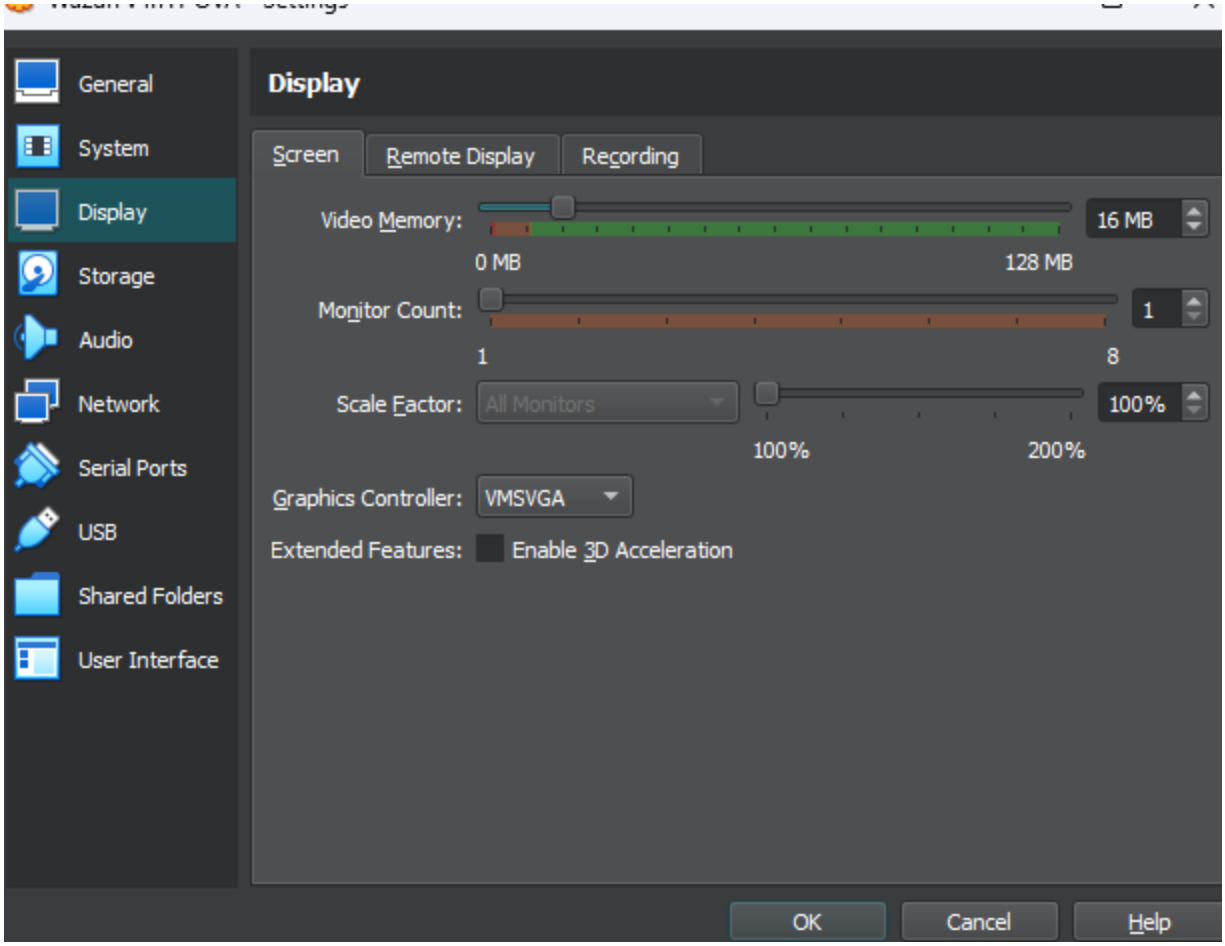

Wazuh v4.7.1 OVA - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Processors:
2
1 CPU
16 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Enable Nested VT-x/AMD-V
Invalid settings detected
OK
Cancel
Help



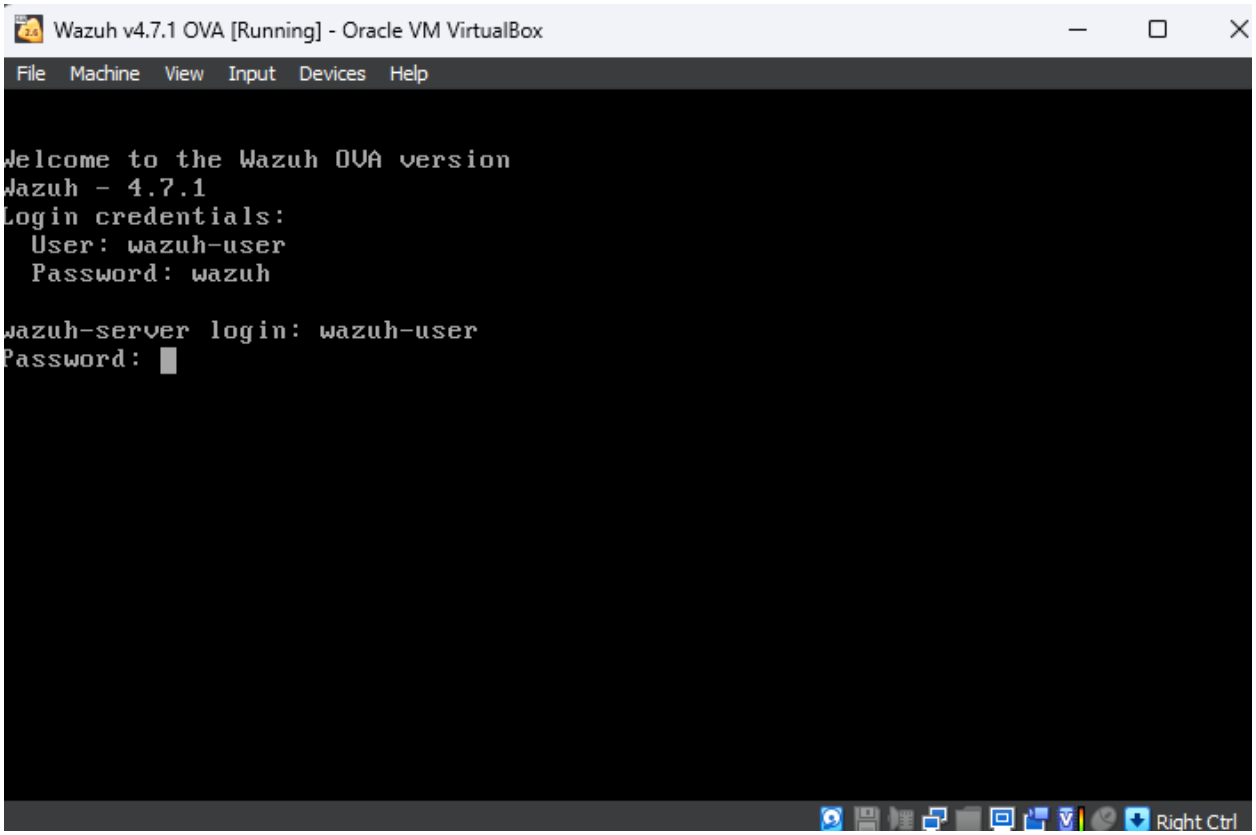
Next we will change the network adapter to Bridged adapter and then finally start the machine.



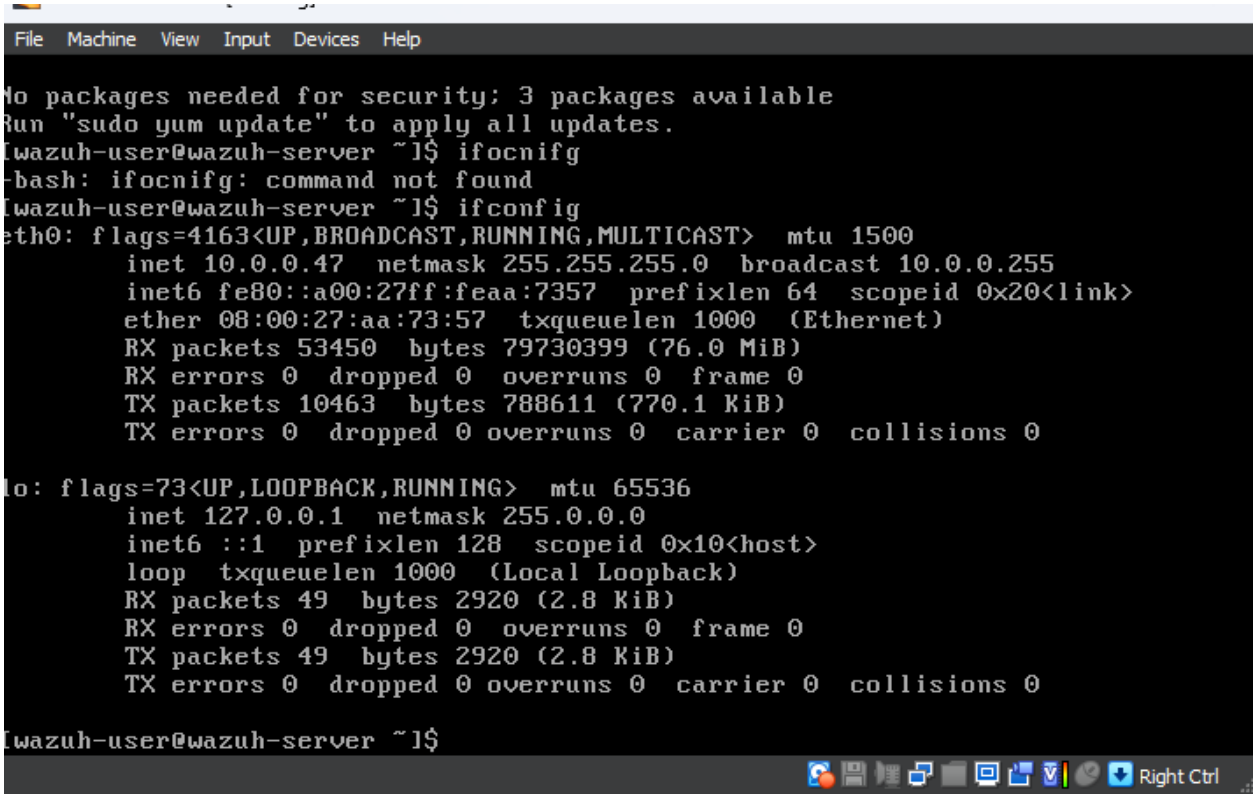
Change the graphic controller so Wazuh doesnt glitch.



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

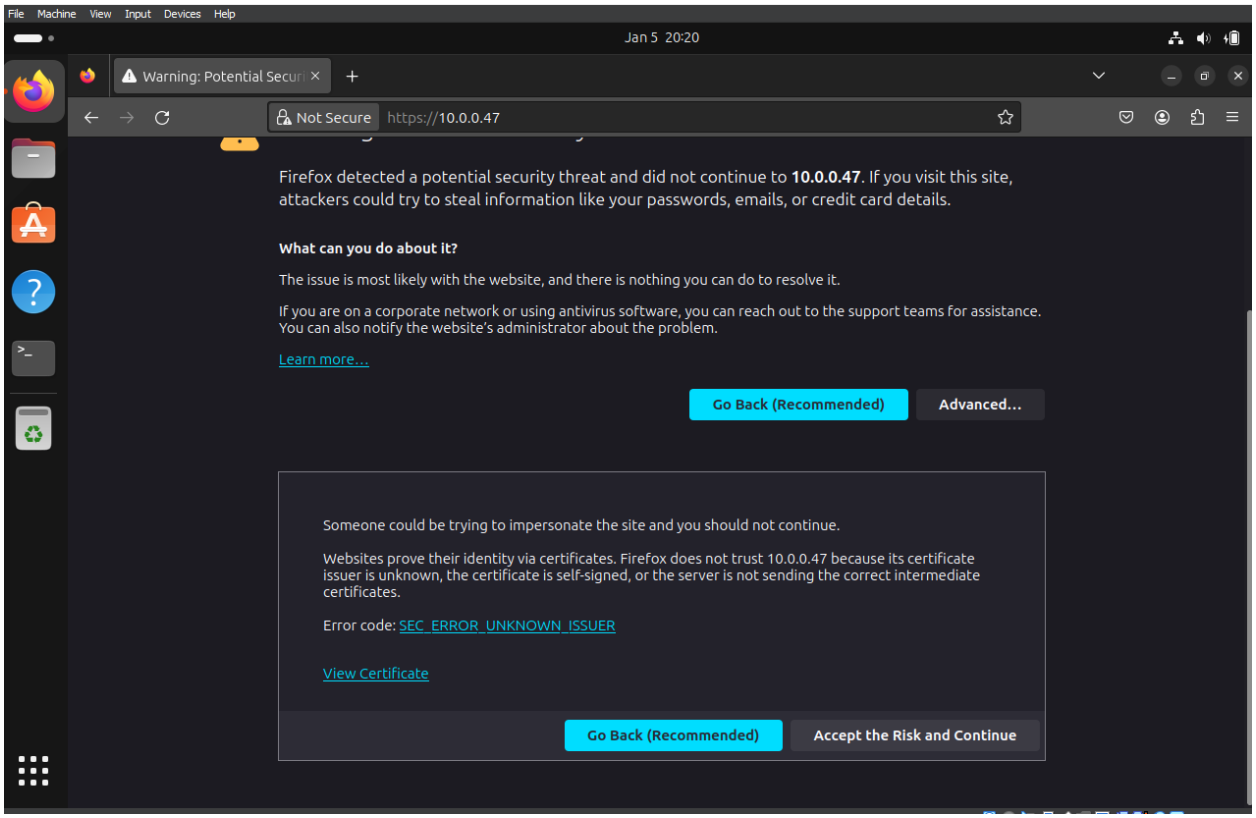


Once logged into the terminal, immediately ifconfig to get the wazuh address and write it in the notepad.



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.

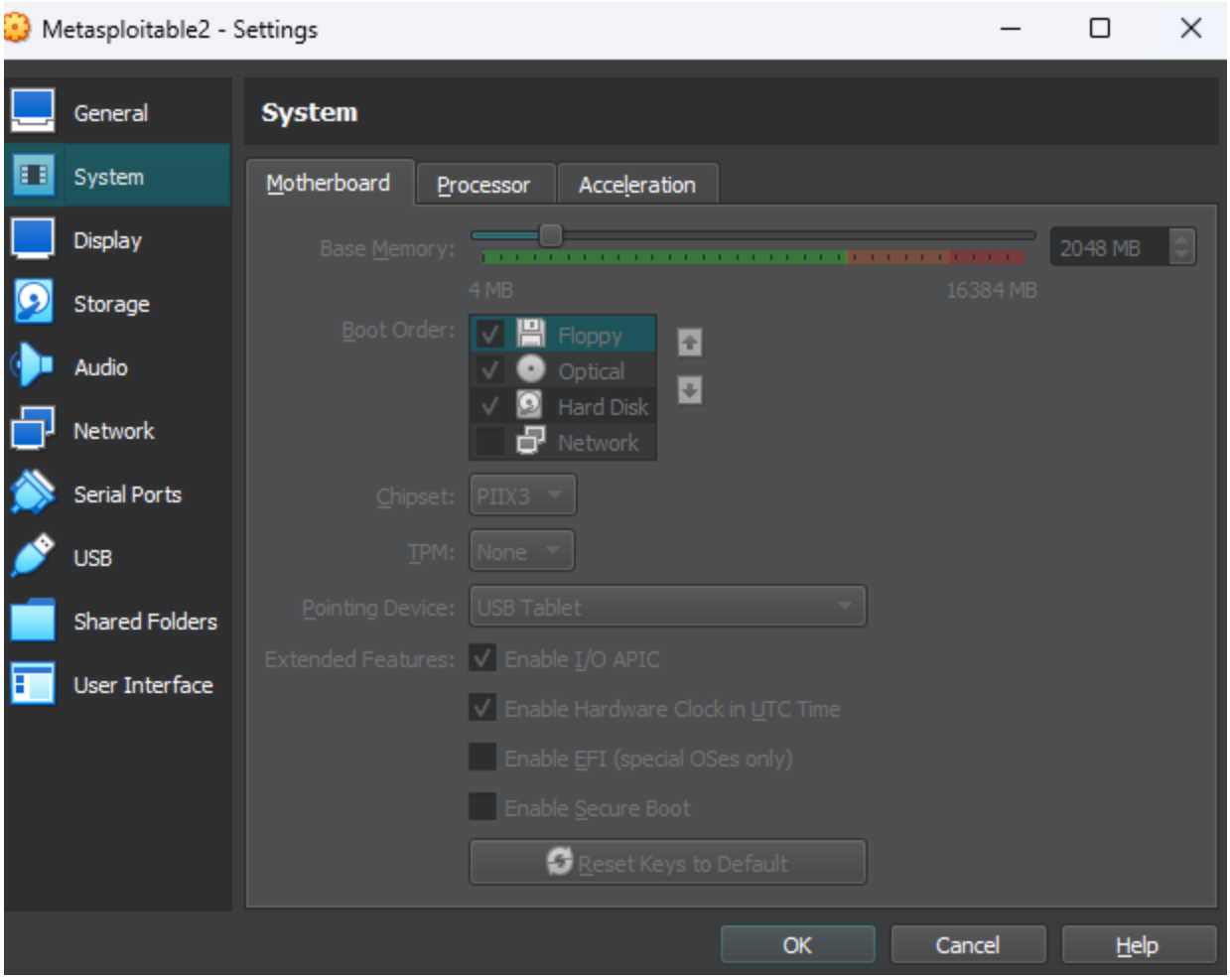
On to the next step.

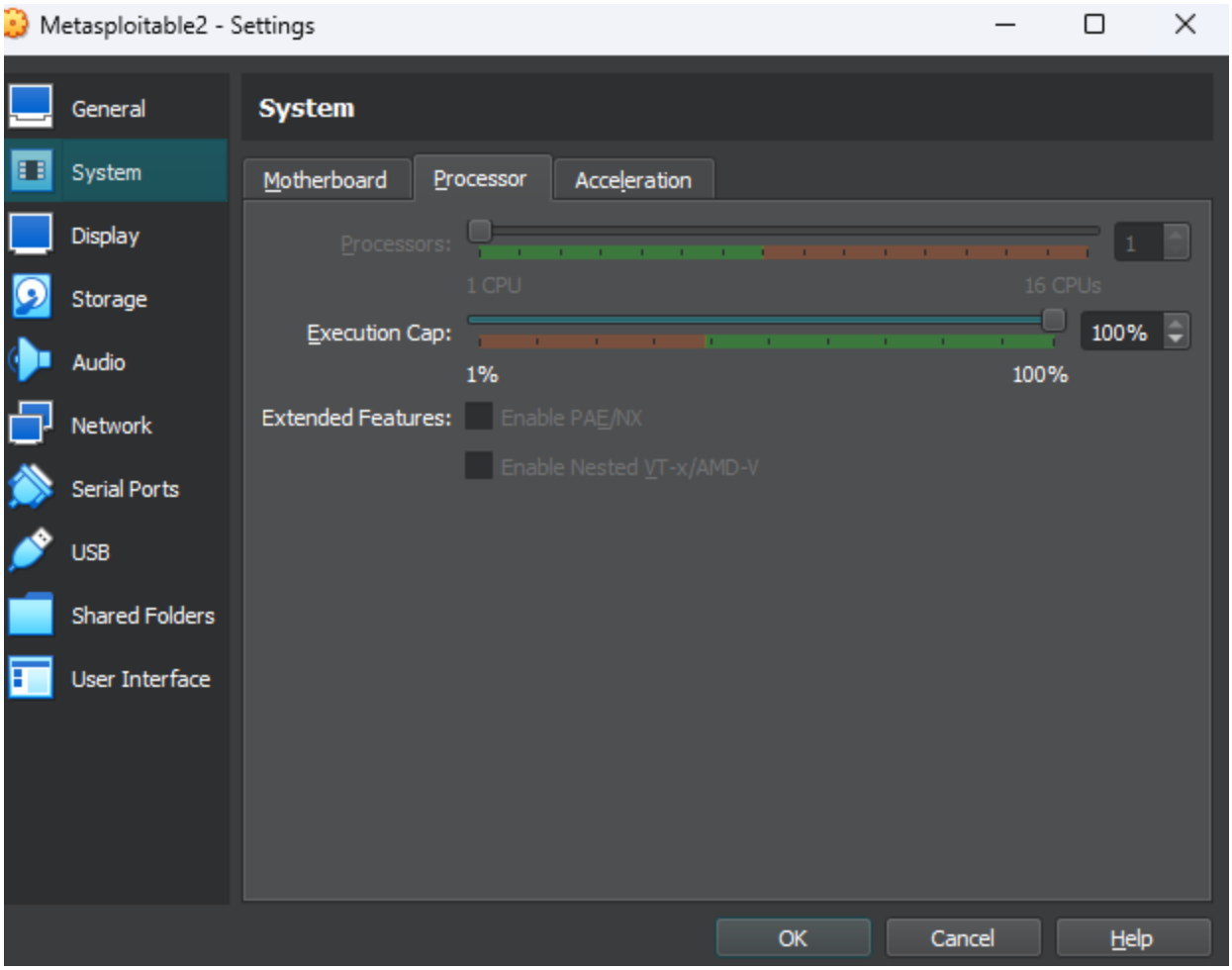
Installing Metasploitable2 is a pretty straightforward process. Just download the iso and install it in virtual box.

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 recourses.

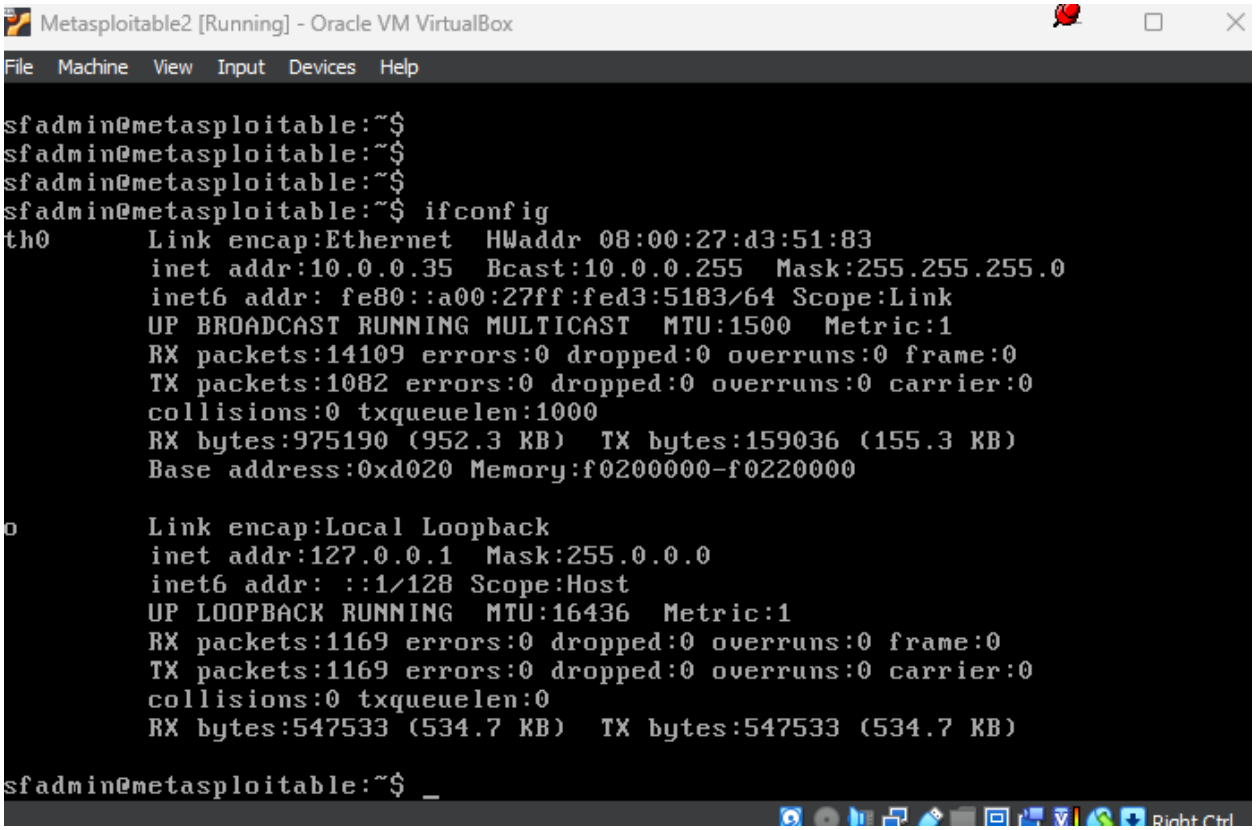
Really you just need it to be on the bridged network like all out other machines and give it 1 processor and 2GB ram.


Metasploitable2 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
2048 MB
4 MB
16384 MB
Boot Order:
Floppy
Optical
Hard Disk
Network
Chipset:
PIIX3
TPM:
None
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable Hardware Clock in UTC Time
Enable EFI (special OSes only)
Enable Secure Boot
Reset Keys to Default
OK
Cancel
Help



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.

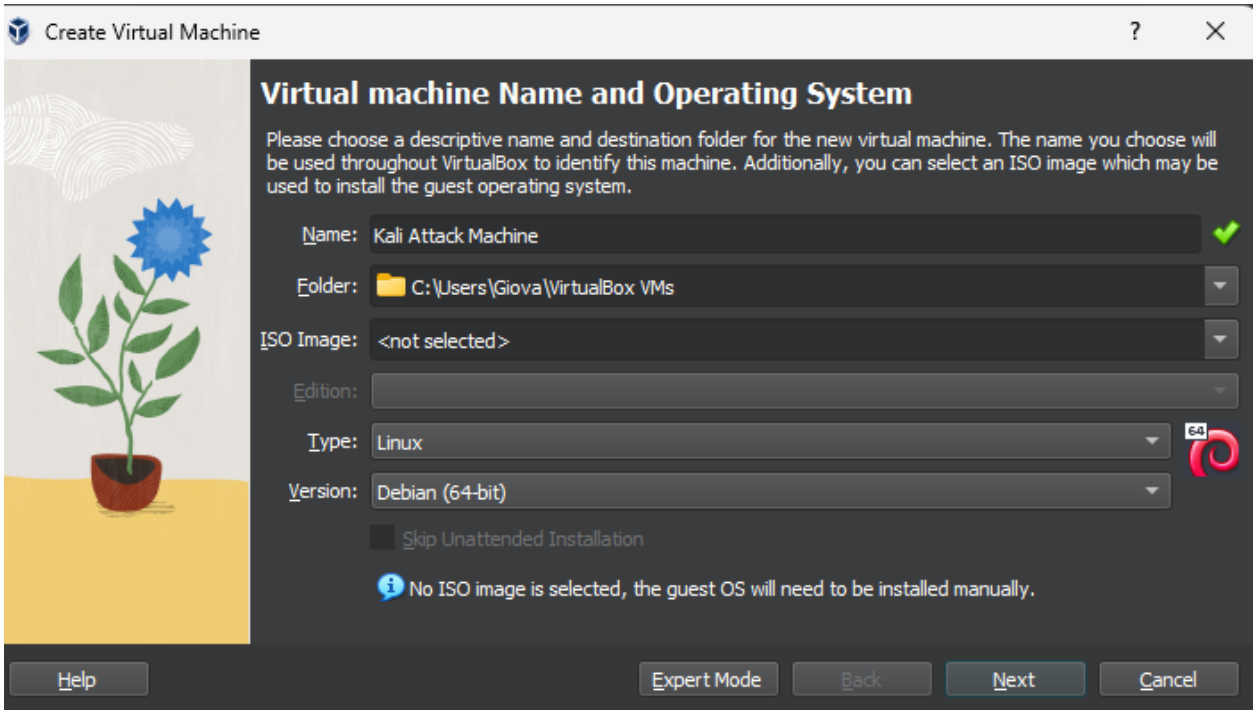


On to the next installation.

Up next is our attack machine, Kali Linux.

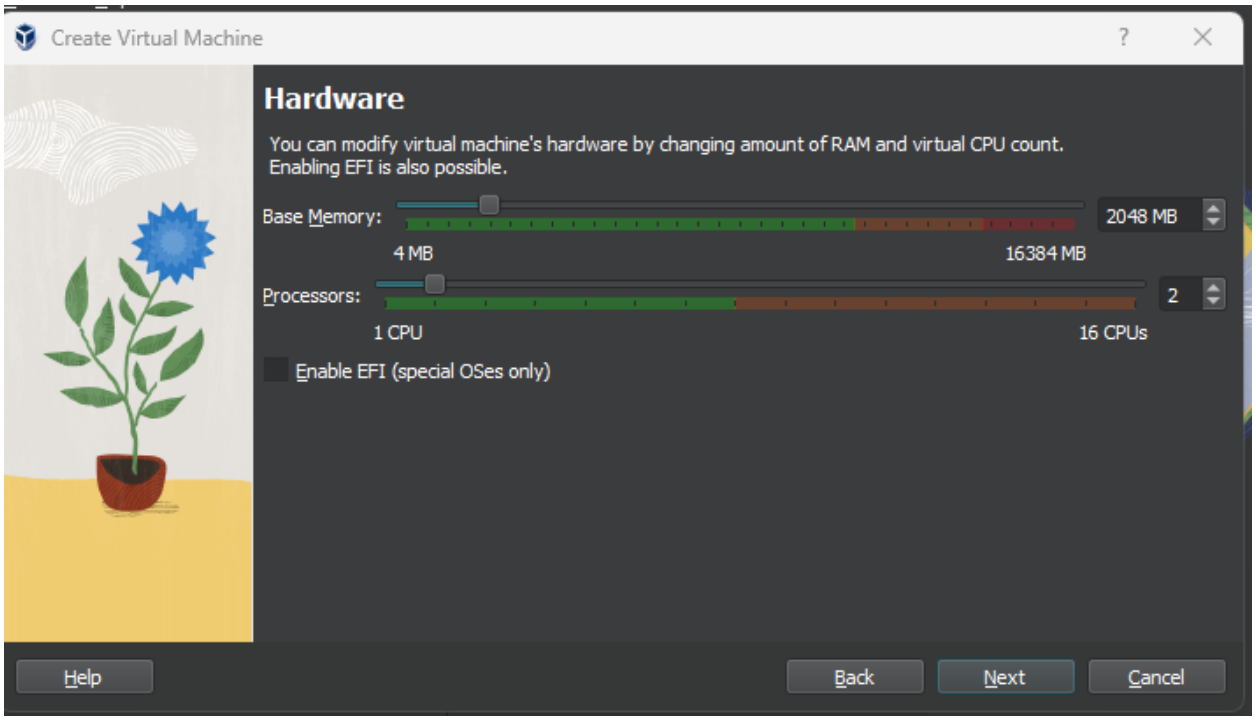
You can either download the prebuilt ova or the iso. In my example I am using the Virtual Hard Disk Drive.

We will not be assigning an iso.

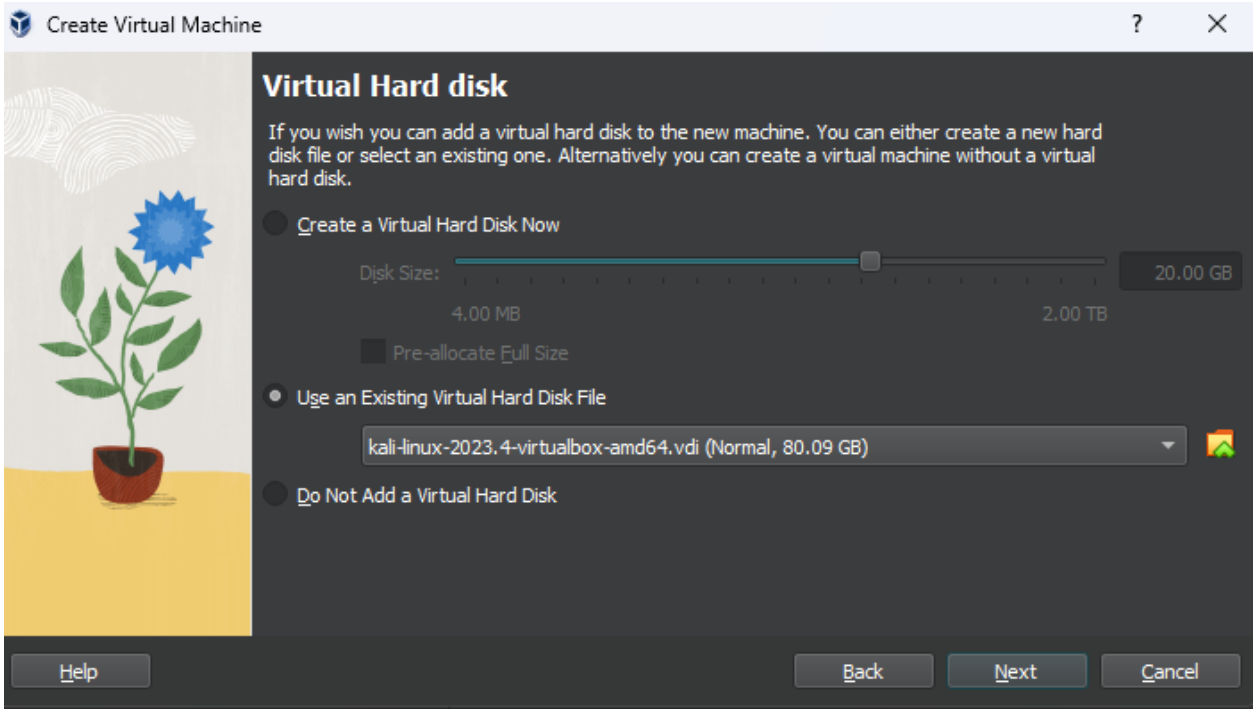


Click next

Give it 2 processors and 2GB ram. Click next

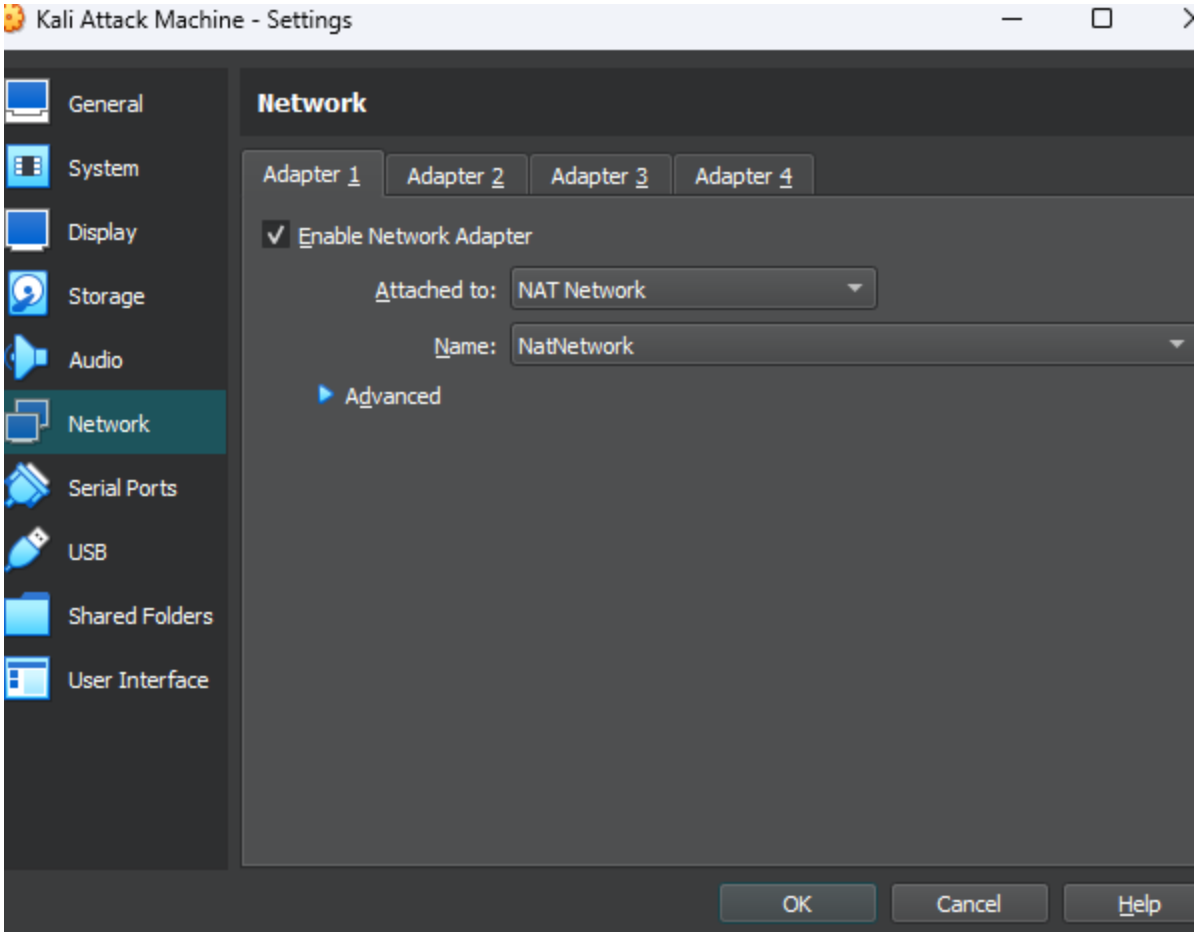


Click on use an existing virtual hard disk drive and look for the Kali vdi. It should have an orange cube icon.



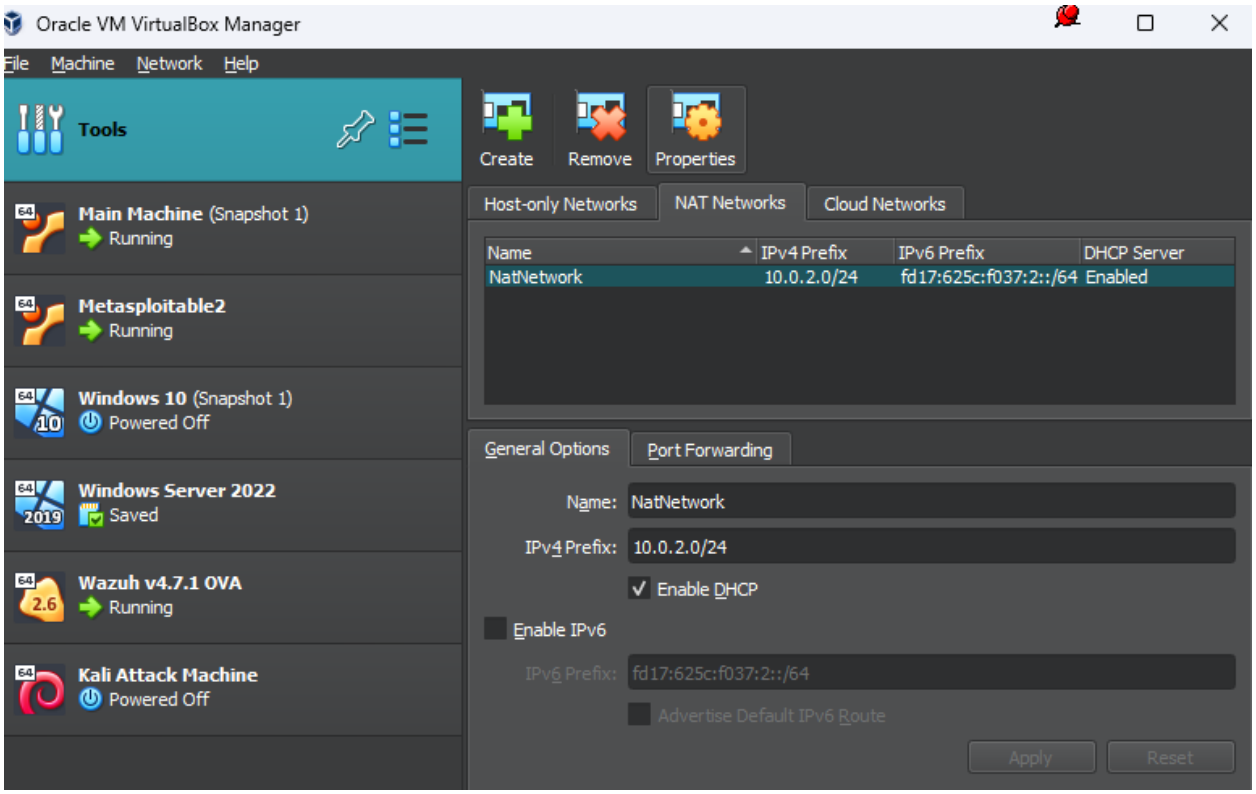
Click next and finish.

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.


Oracle VM VirtualBox Manager
File Machine Help
Tools
Main Machine (Snapshot 1)
Running
Metasploitable2
Running
Windows 10 (Snapshot 1)
Powered Off
Windows Server 2022
Saved
Wazuh v4.7.1 OVA
Running
Kali Attack Machine
Powered Off
Welcome
Extensions
Media
Network
Cloud
Activities
Export
New
Add

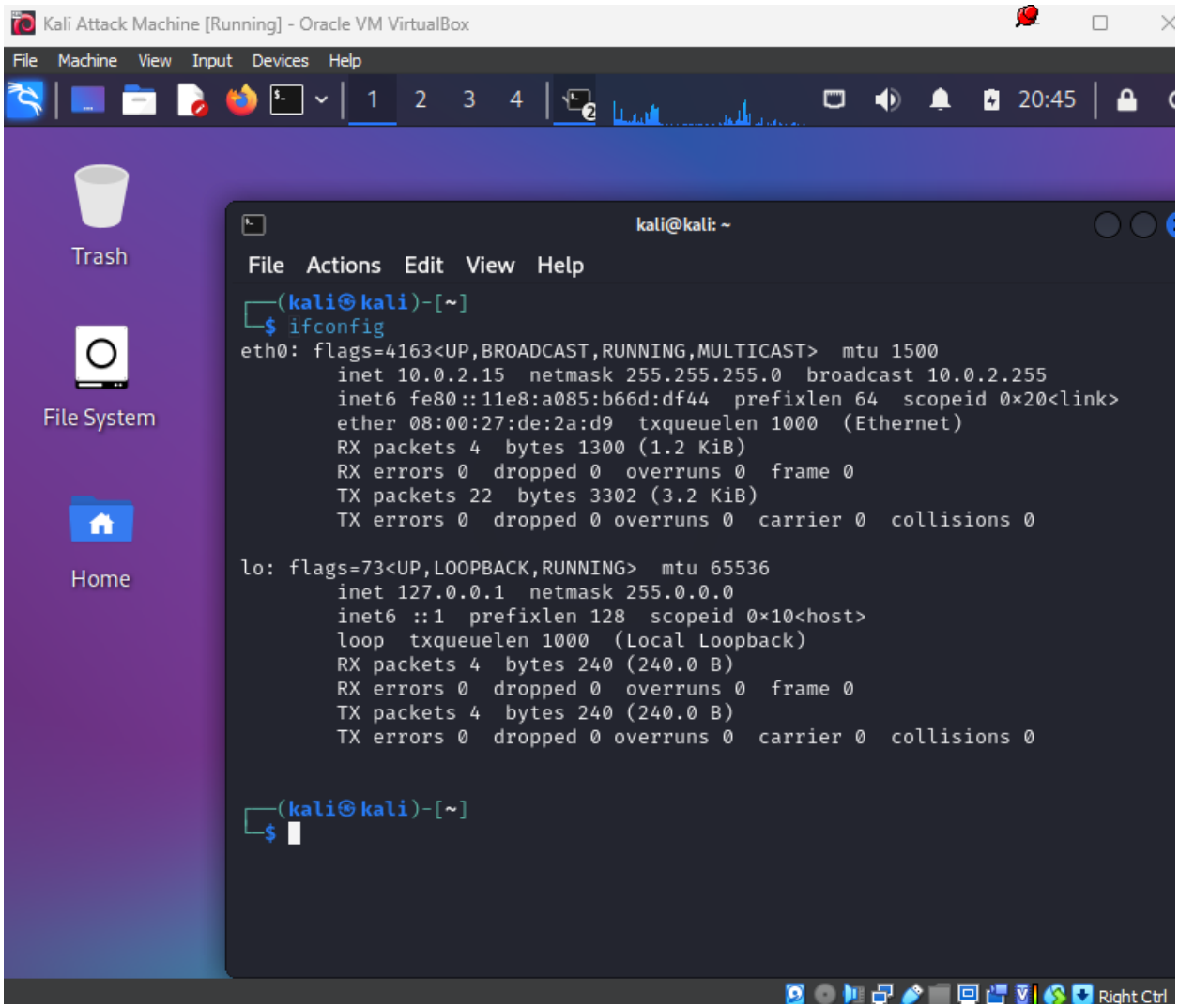

Oracle VM VirtualBox Manager
File Machine Network Help
Tools
Main Machine (Snapshot 1)
Running
Metasploitable2
Running
Windows 10 (Snapshot 1)
Powered Off
Windows Server 2022
Saved
Wazuh v4.7.1 OVA
Running
Kali Attack Machine
Powered Off
Create
Remove
Properties
Host-only Networks
NAT Networks
Cloud Networks
Name
IPv4 Prefix
IPv6 Prefix
DHCP Server
NatNetwork
10.0.2.0/24
fd17:625c:f037:2::/64
Enabled
General Options
Port Forwarding
Name: NatNetwork
IPv4 Prefix: 10.0.2.0/24
Enable DHCP
Enable IPv6
IPv6 Prefix: fd17:625c:f037:2::/64
Advertise Default IPv6 Route
Apply
Reset

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!



Thats it.

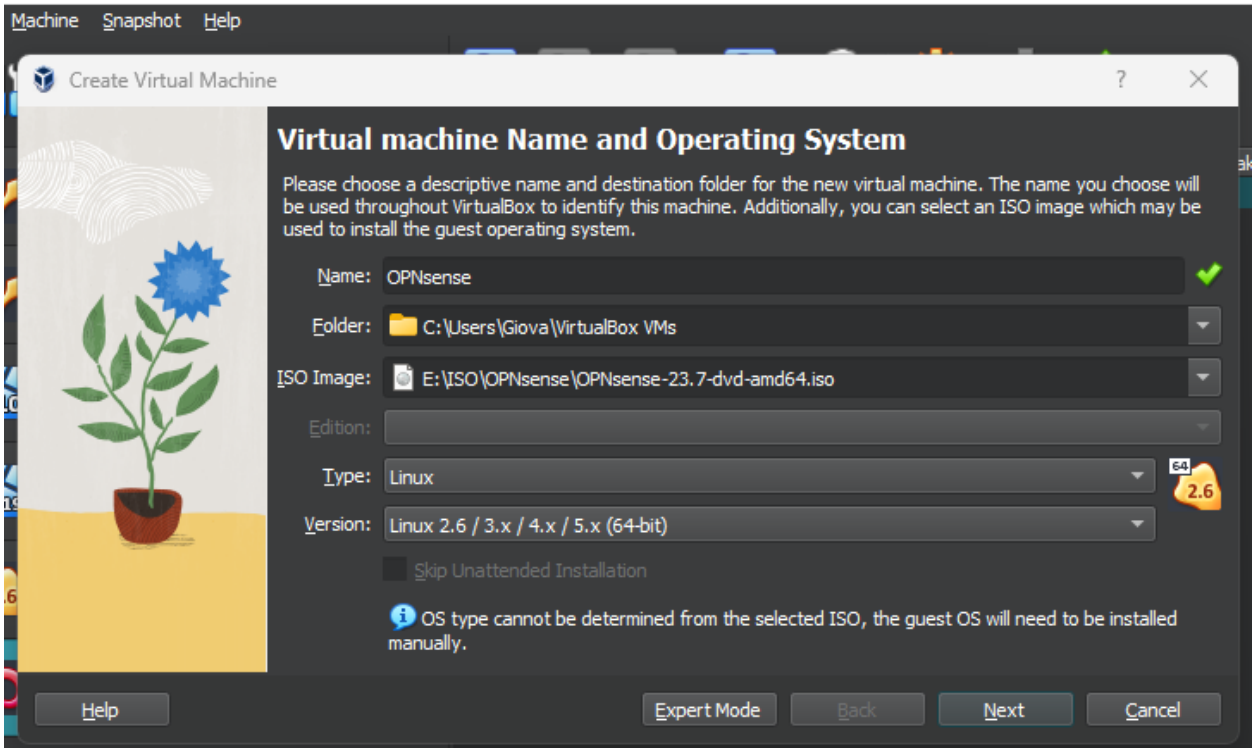
On to the next installation.

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.

Lets start.

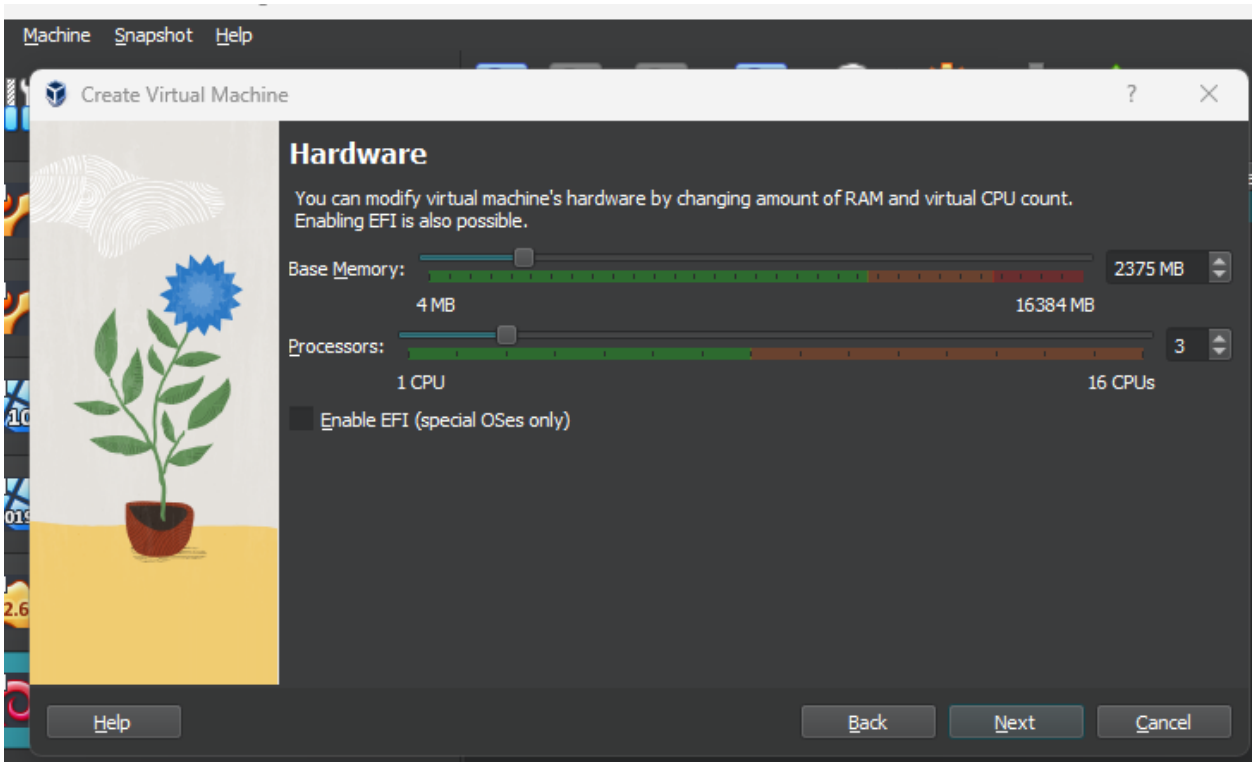
For opnsense we will need to download it from the official website.

This installation will be through iso.



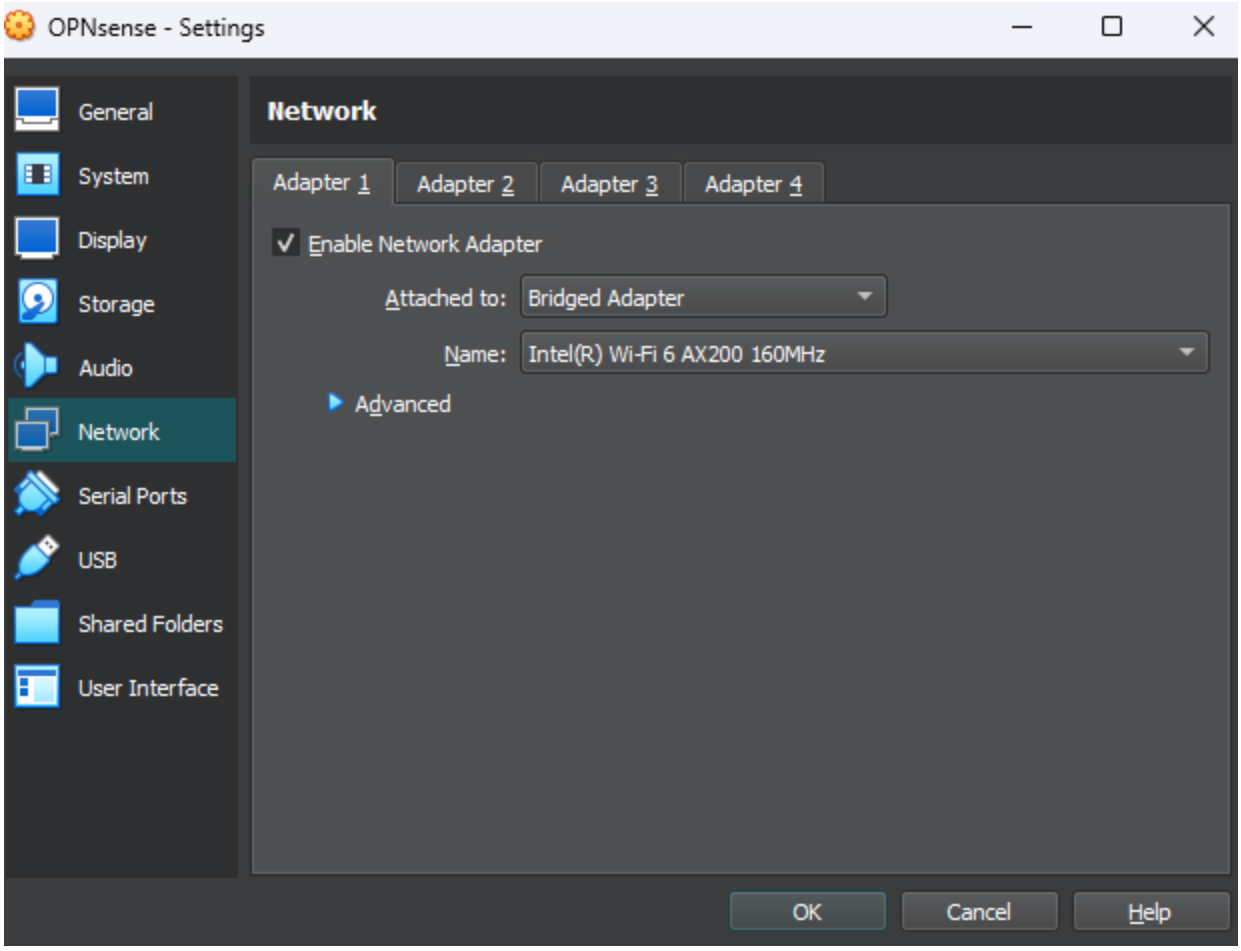
Click next

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



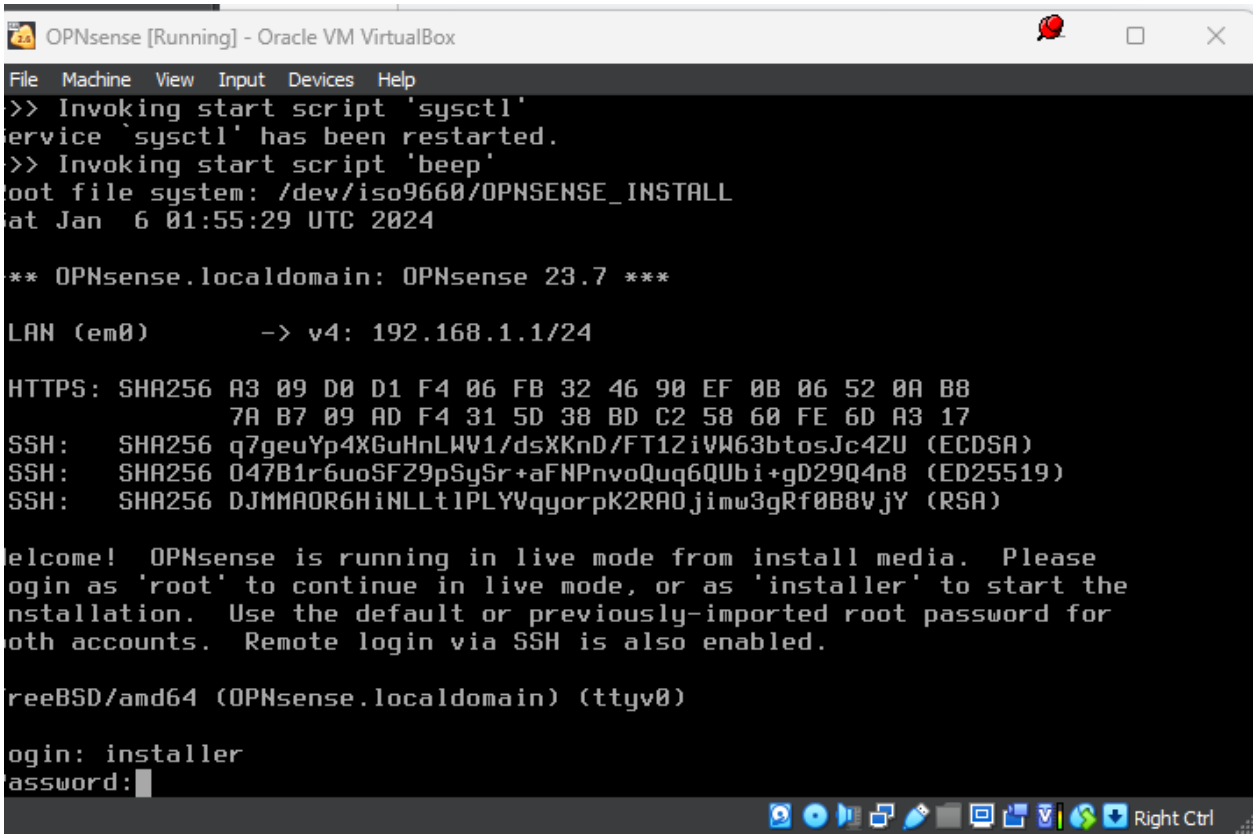
Click next, and then next until you ge to the last panel and click finish.

Make sure to check that this machine has bridged adapter.

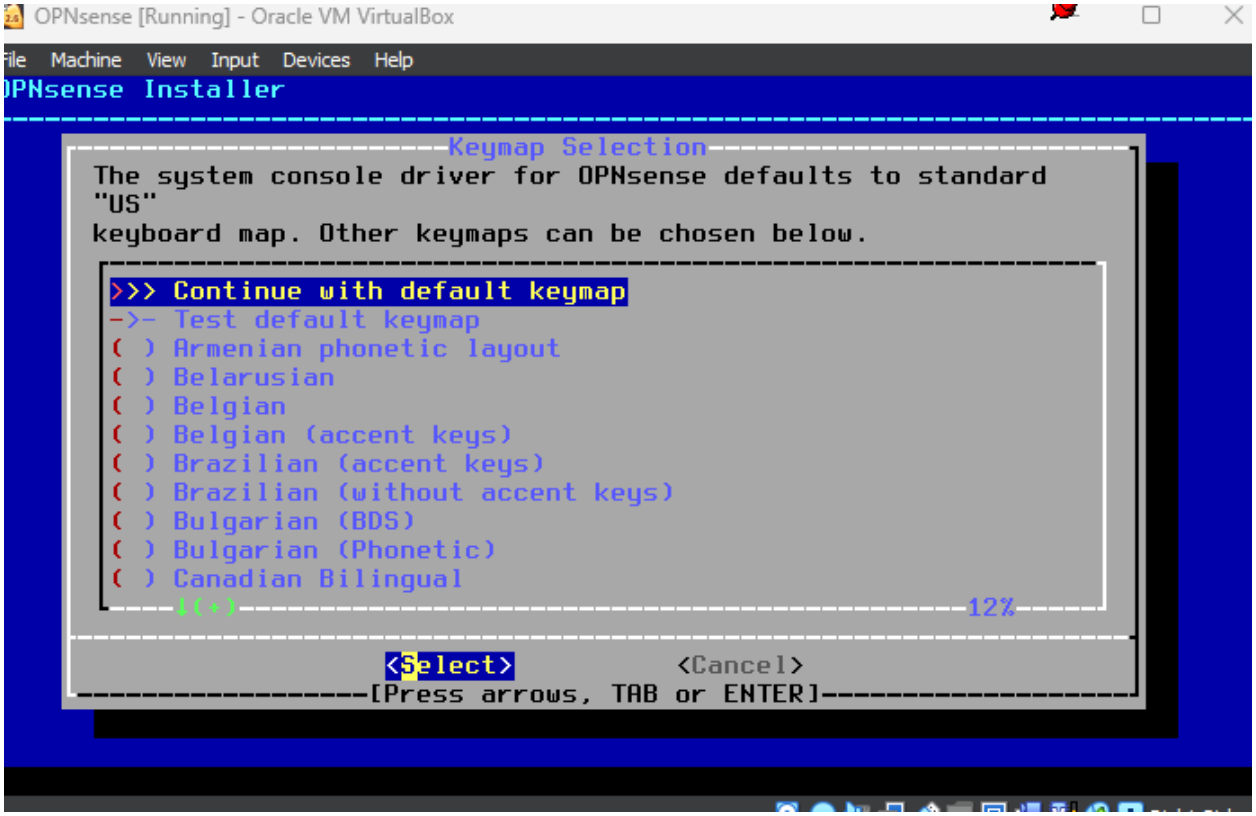


Now we can start it up.

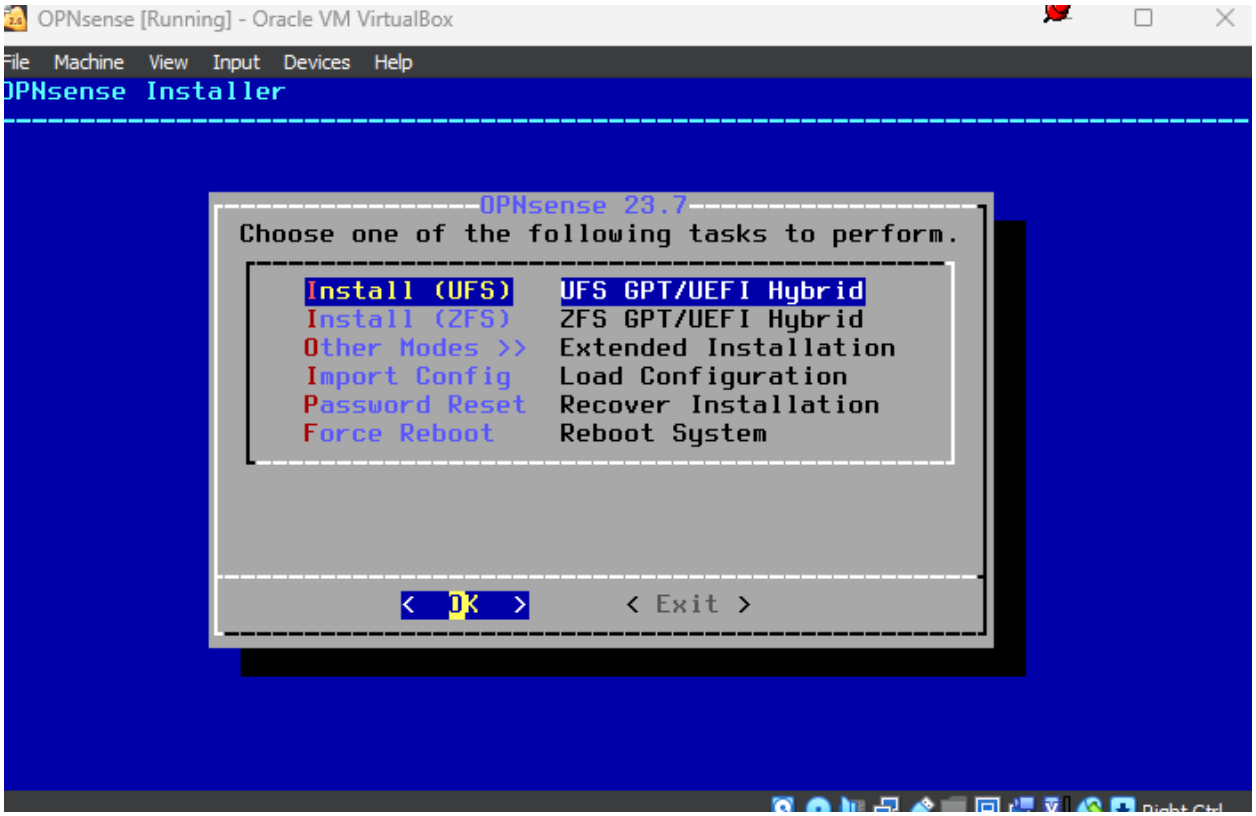
The login for the first boot is username root and password opnsense.


OPNsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
>> Invoking start script 'sysctl'
ervice `sysctl' has been restarted.
>> Invoking start script 'beep'
oot file system: /dev/iso9660/OPNSENSE_INSTALL
at Jan 6 01:55:29 UTC 2024
** 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
SSH: SHA256 q7geuYp4XGuHnLWV1/dsXKnD/FT1ZiVW63btosJc4ZU (ECDSA)
SSH: SHA256 O47B1r6uoSFZ9pSySr+aFNPnvoQuq6QUbi+gD29Q4n8 (ED25519)
SSH: SHA256 DJMMAOR6HiNLLtlPLYVqyorpK2RAOjimw3gRf0B8VjY (RSA)
elcome! OPNsense is running in live mode from install media. Please
ogin as 'root' to continue in live mode, or as 'installer' to start the
nstallation. Use the default or previously-imported root password for
oth accounts. Remote login via SSH is also enabled.
reeBSD/amd64 (OPNsense.localdomain) (ttyv0)
ogin: installer
assword:
Right Ctrl

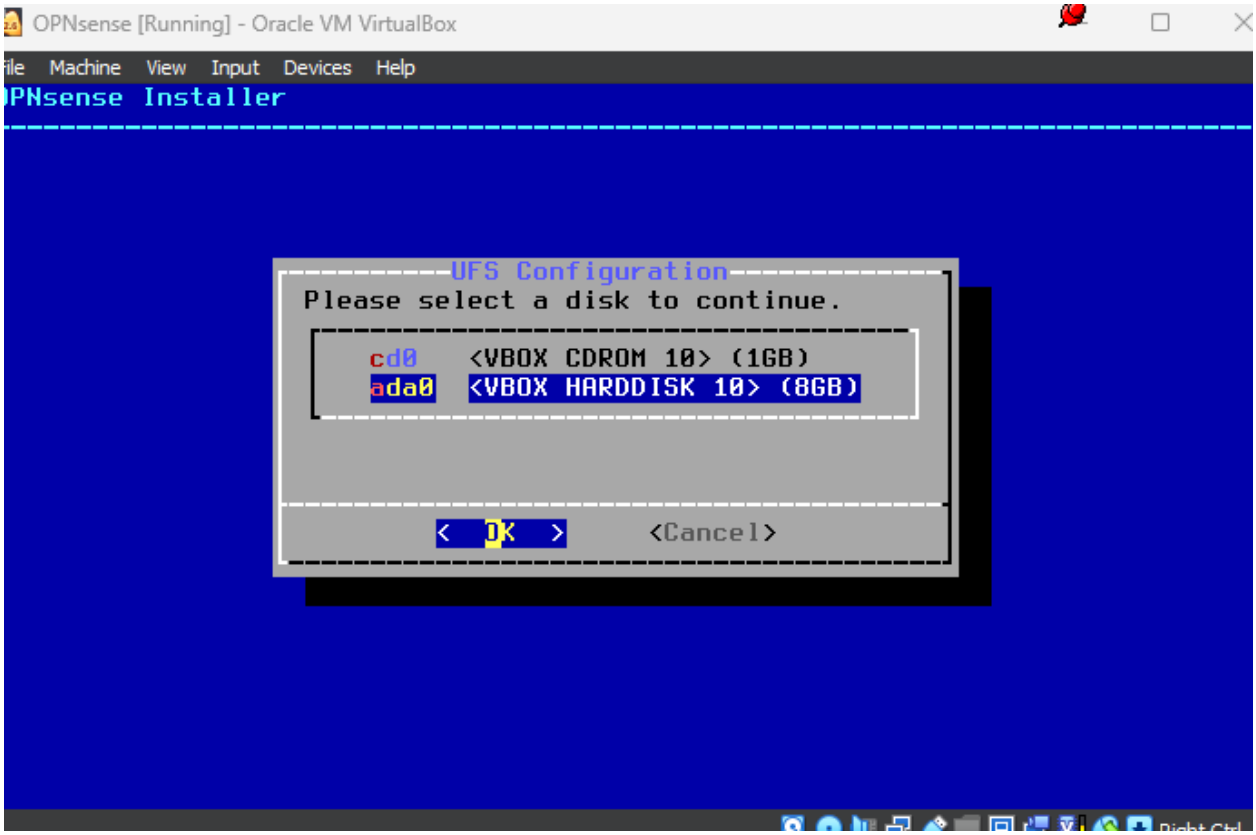
Press enter



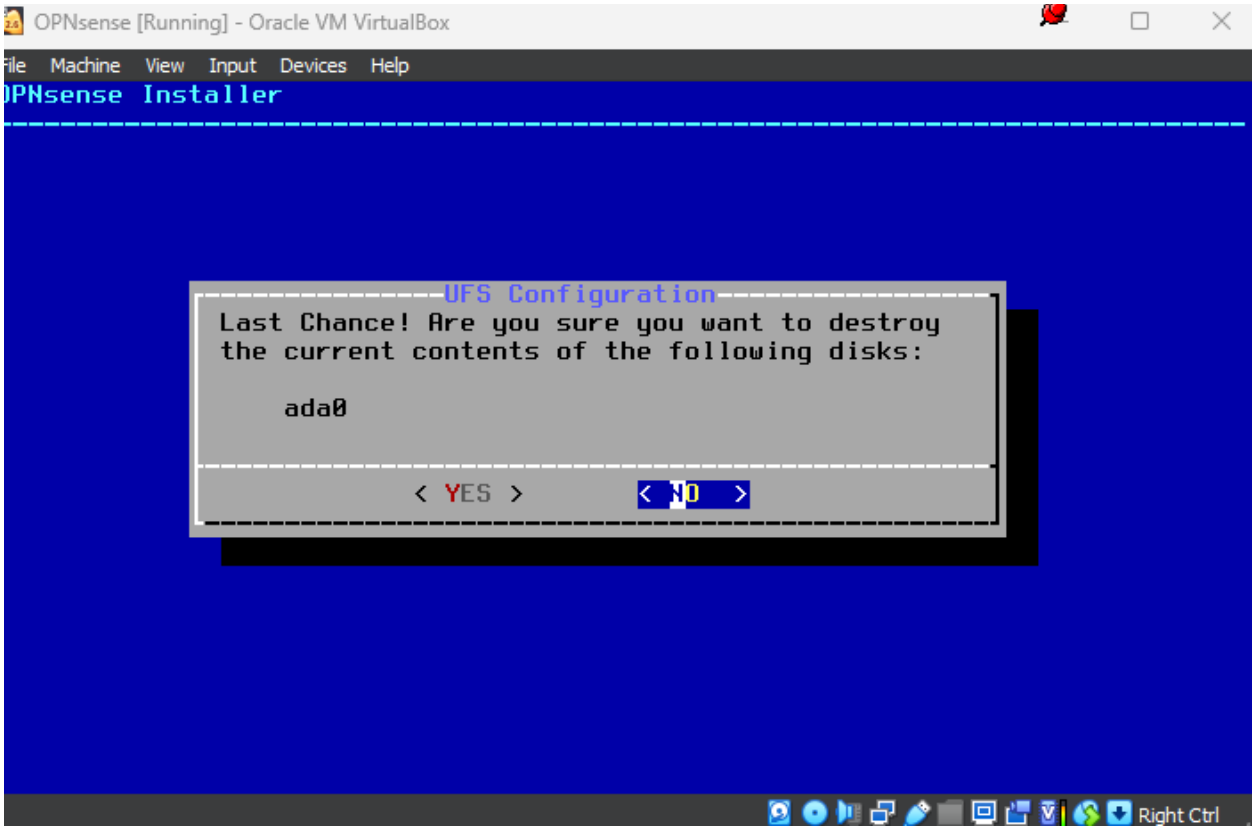
Press enter again.



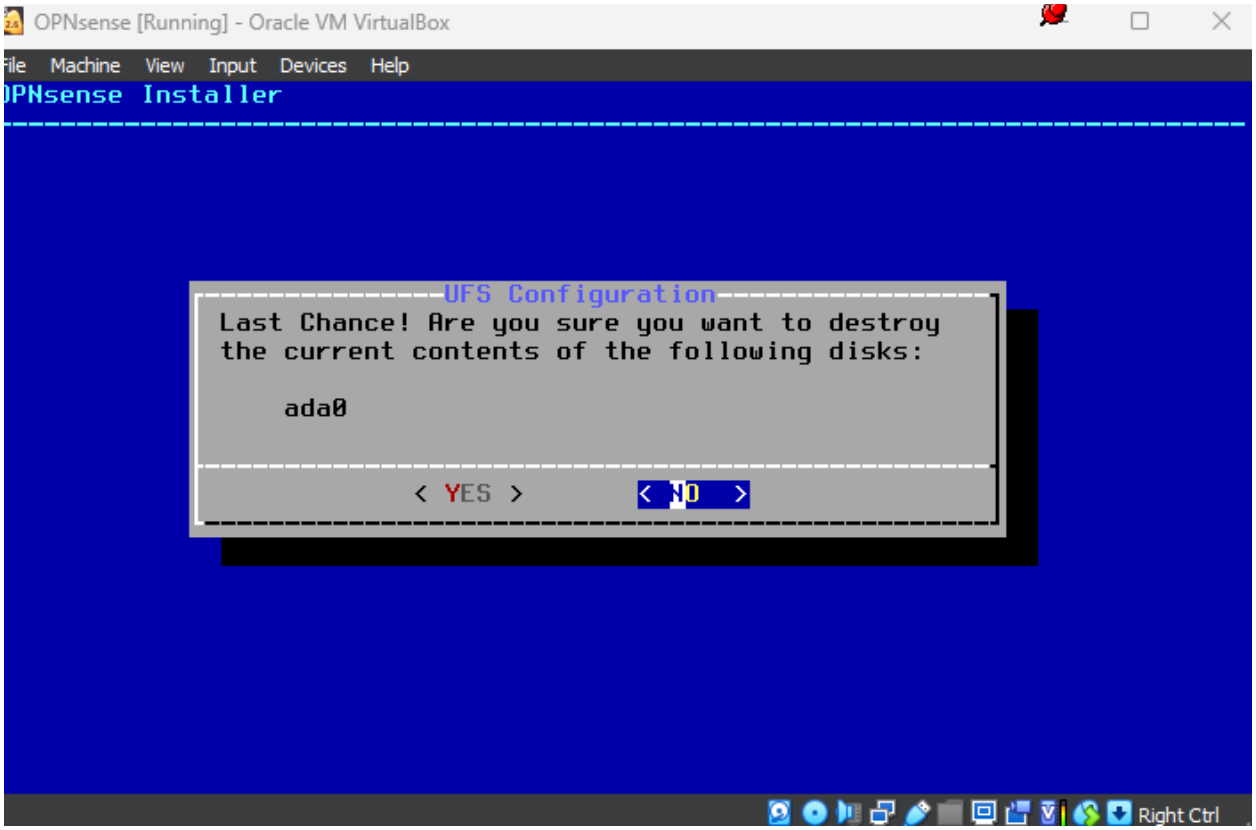
Press down arrow and then press enter.



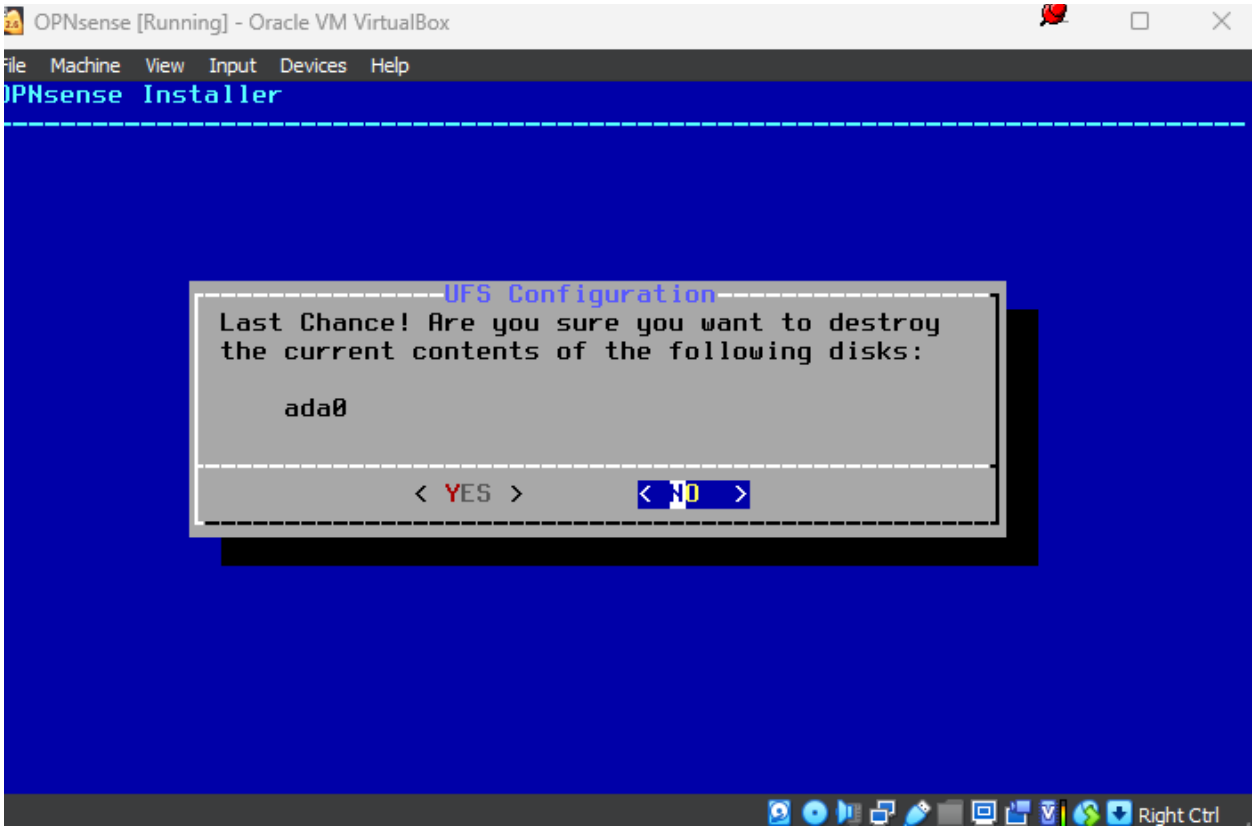
Right arrow and press enter



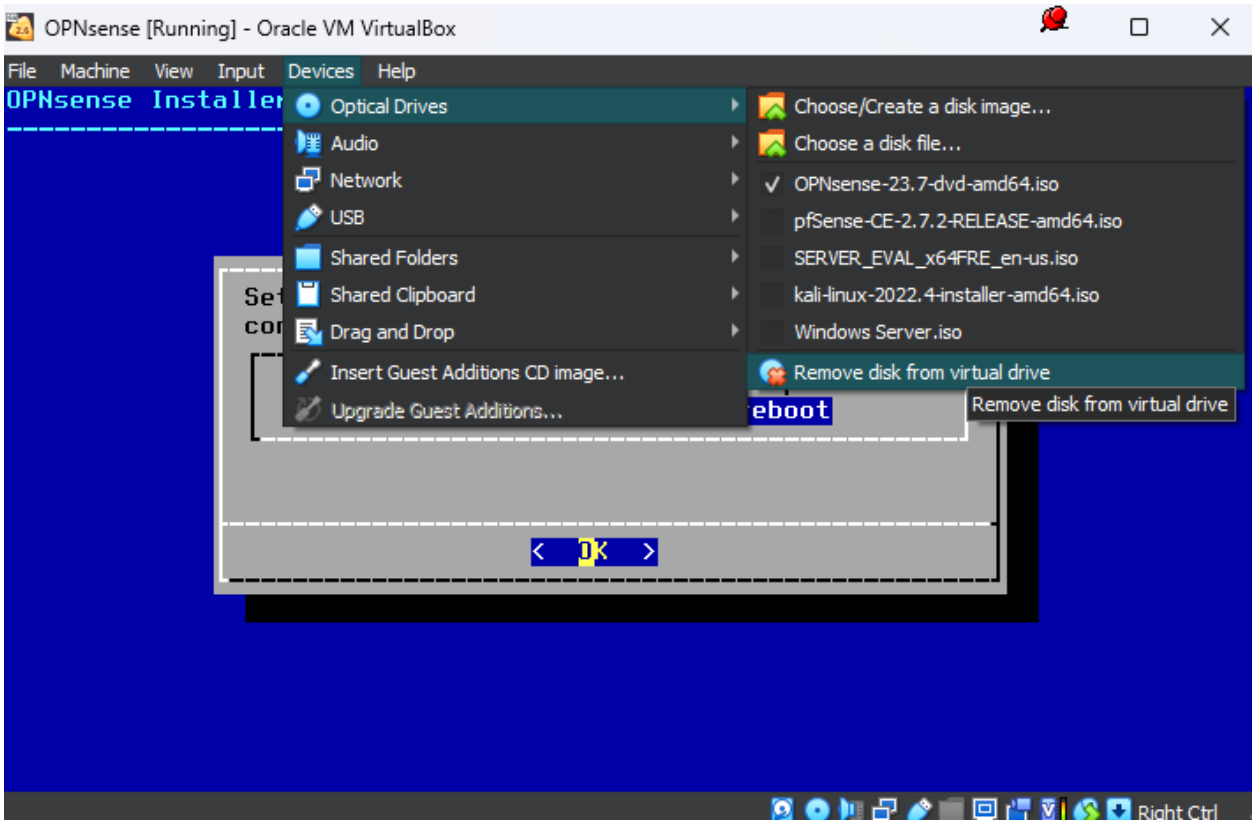
It should now be installing



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

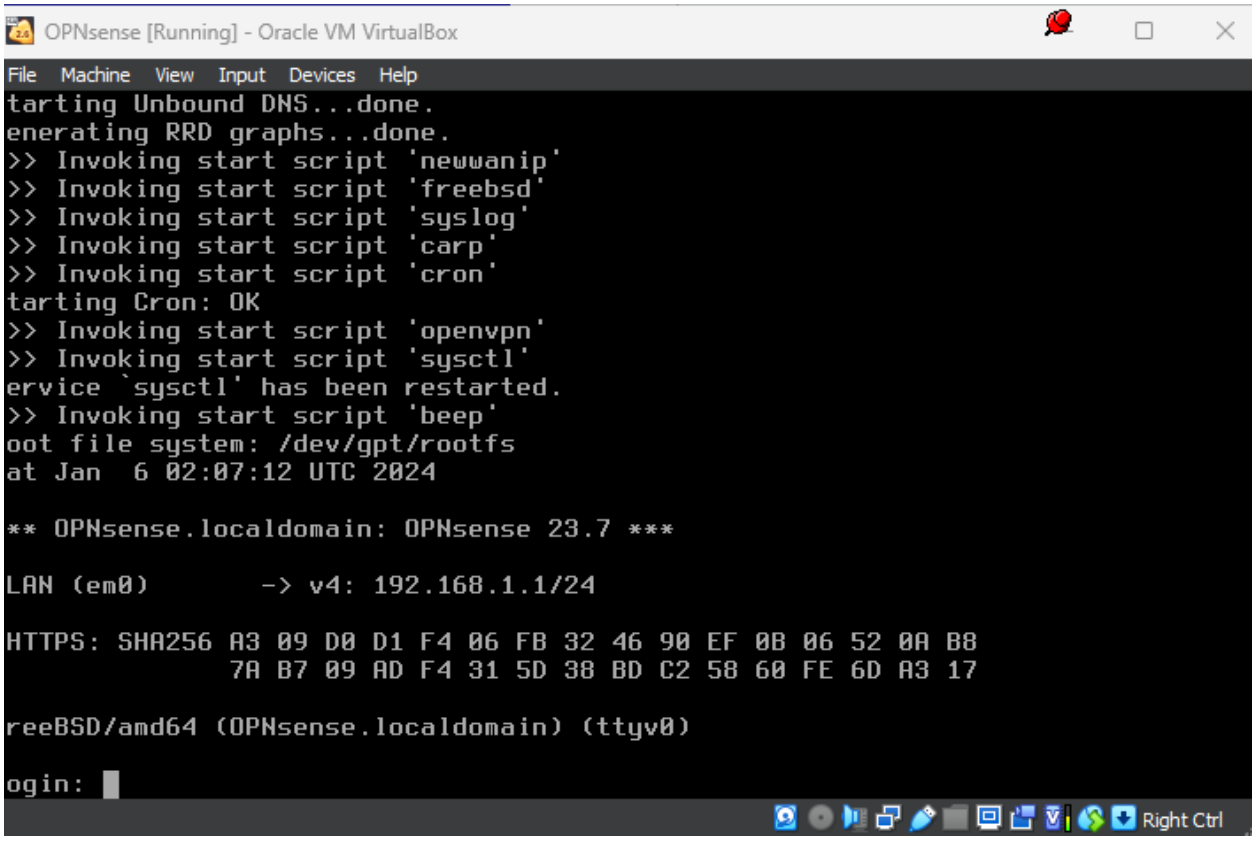


But while its shutting down, head to the devices tab > optical drives > remove disk from virtual drive.



This will have us avoid a boot loop since that is a known issue when it comes to installing this firewall.

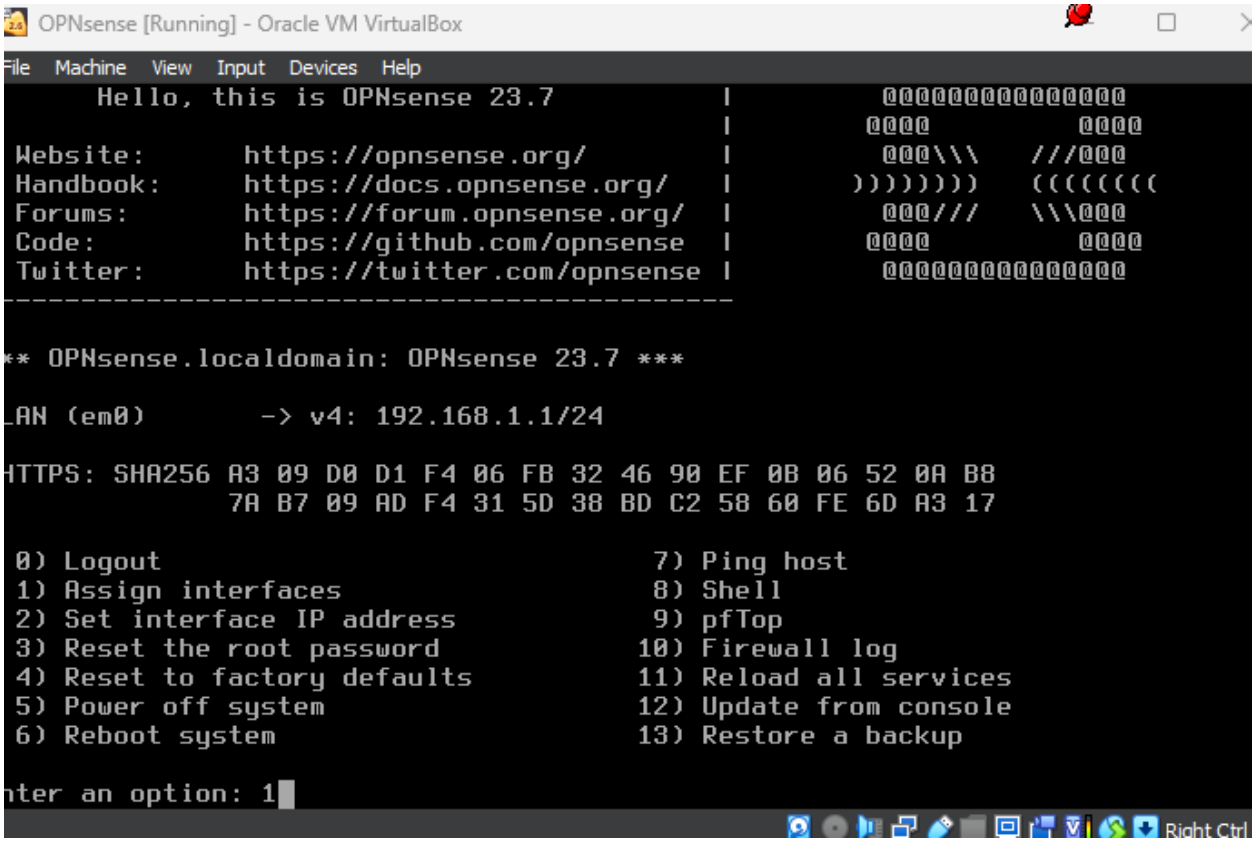
Now you should be on this screen



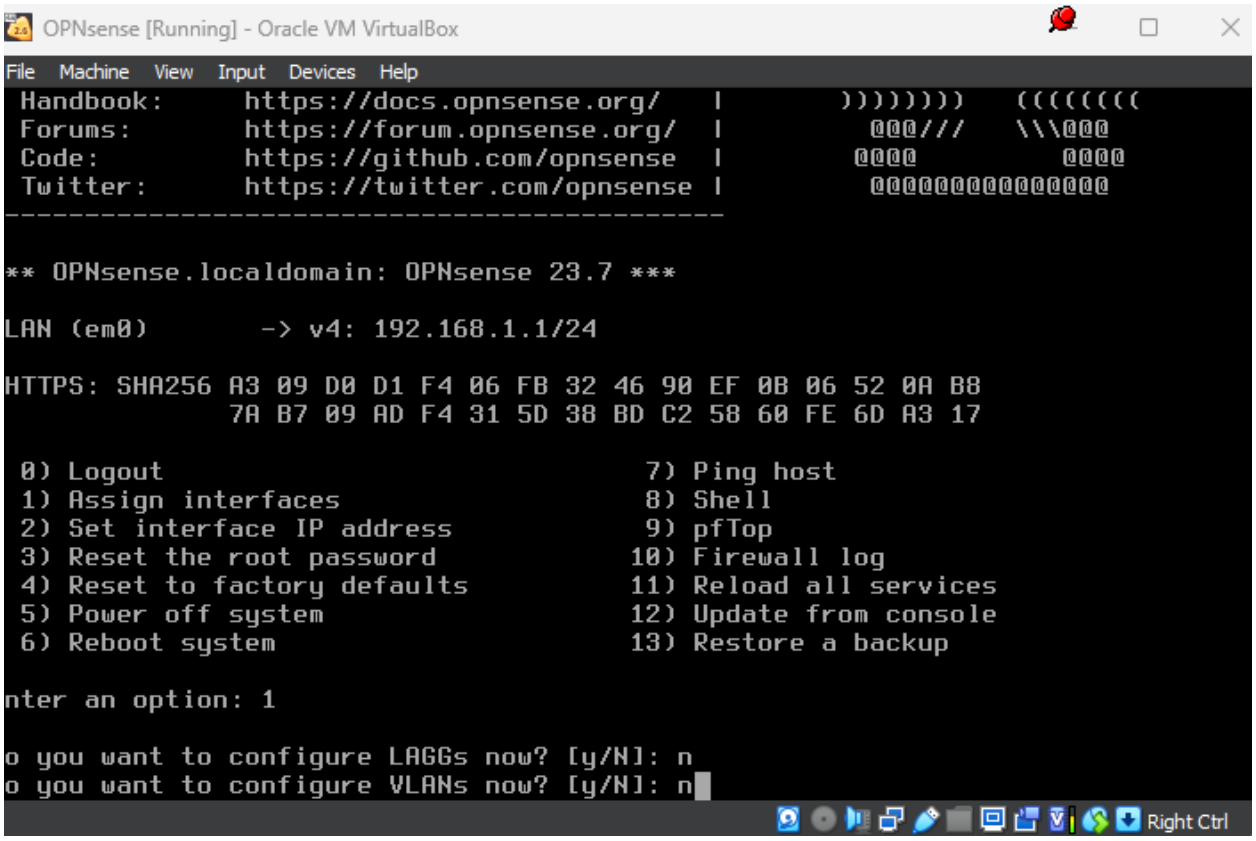
The new username is root and the password is still opnsense. Login.

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

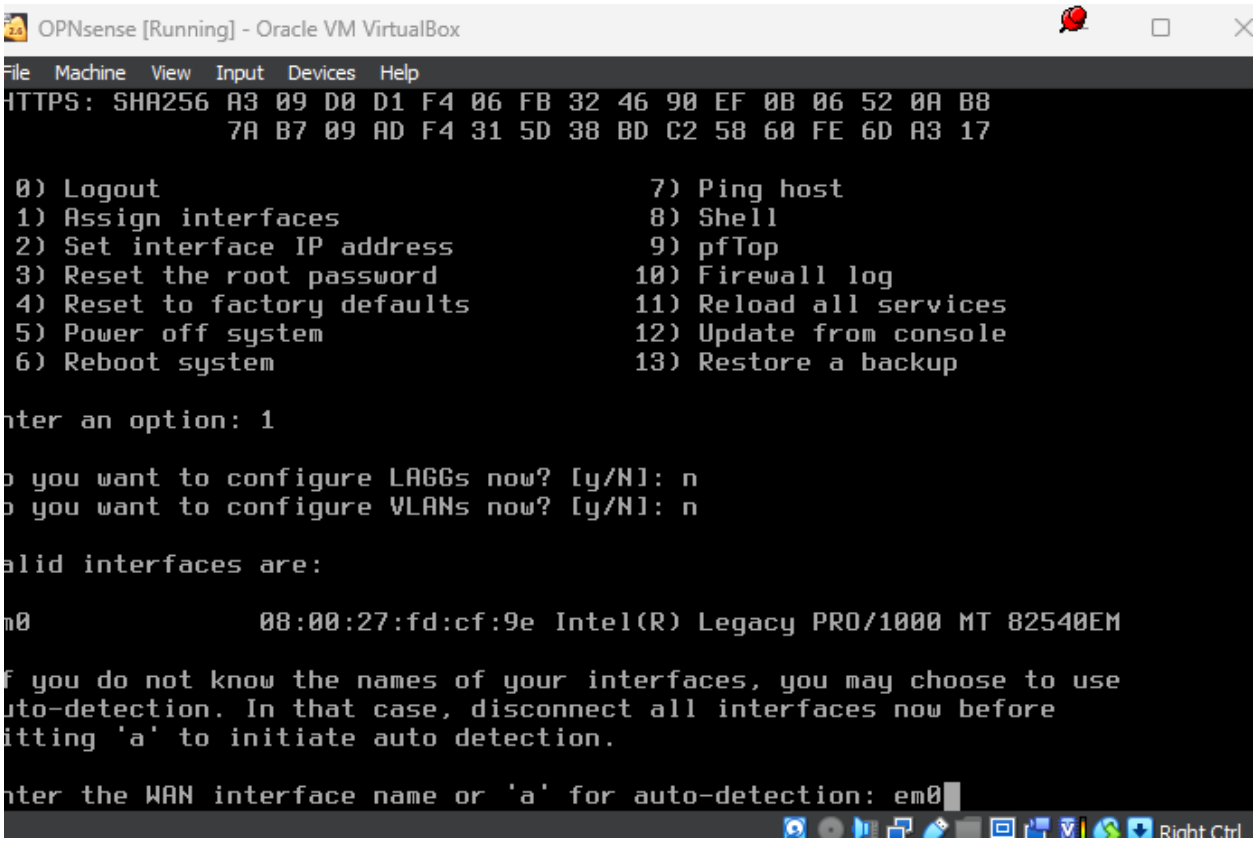
Press 1 to assign interfaces.



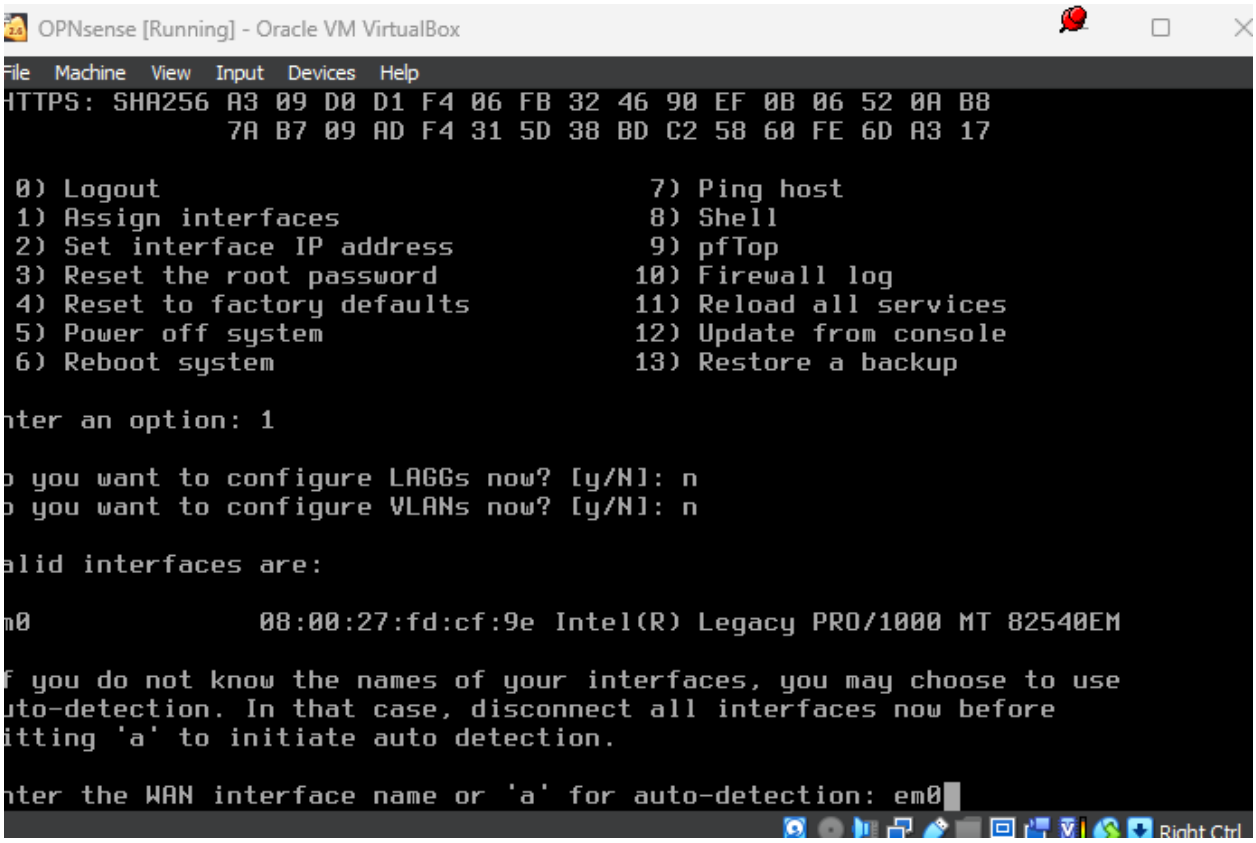
Type n on both of these options.



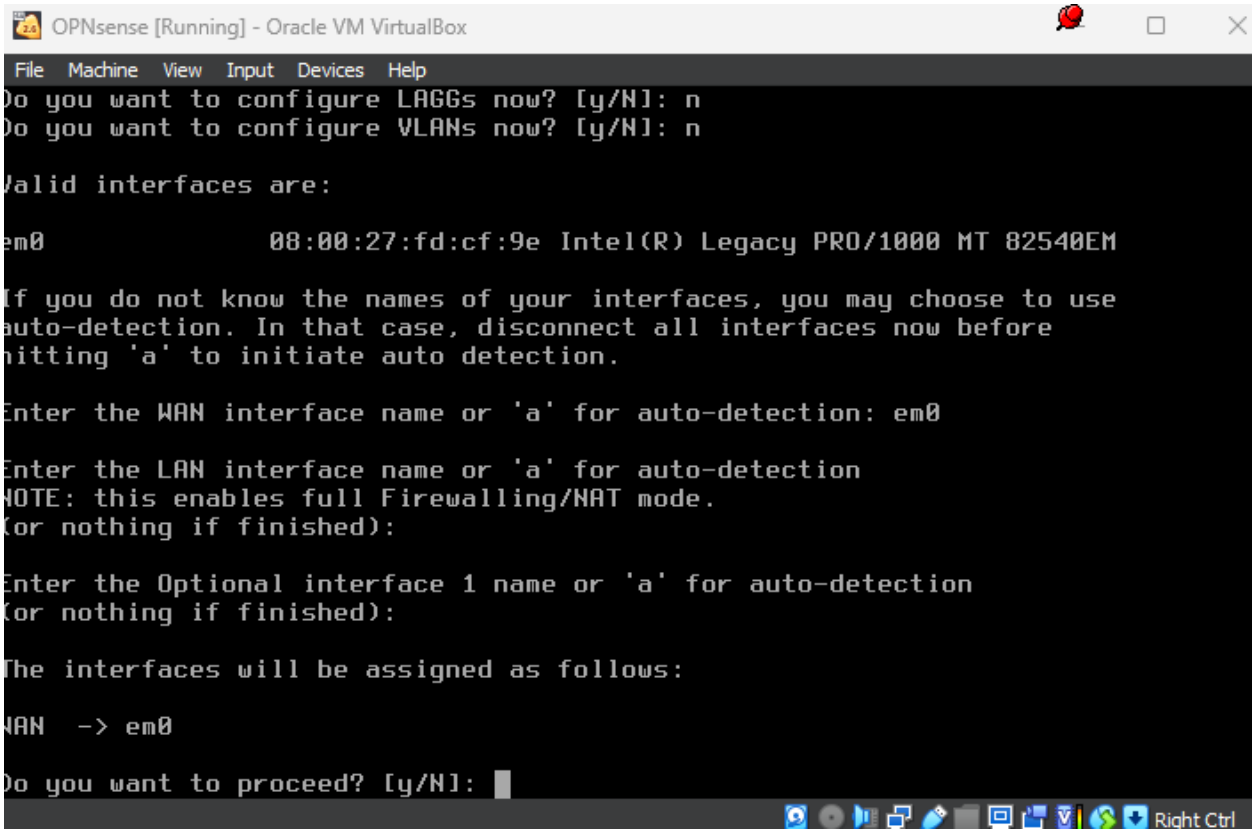
Here we will type em0 which is our bridged network.



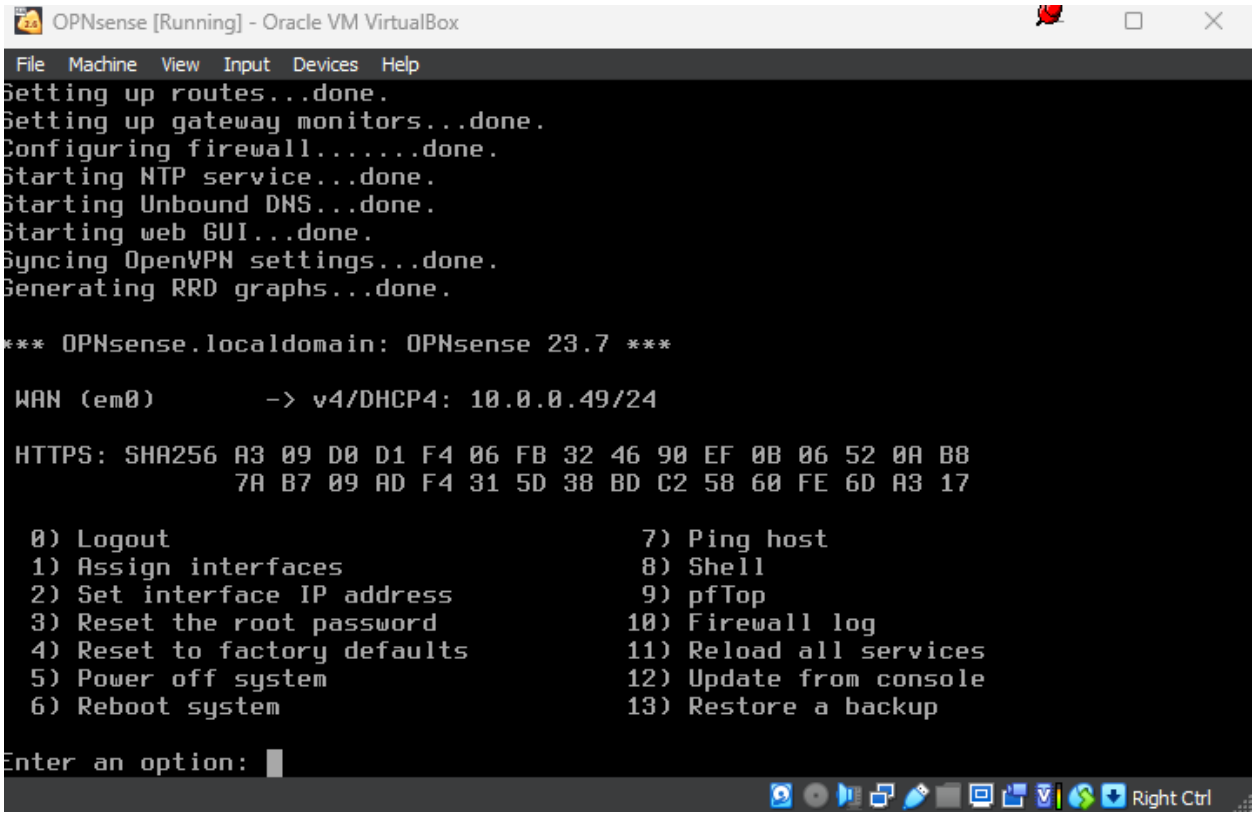
After pressing enter you wil be prompted to enter more options. Ignore them as we only need our WAN.



Press y for yes



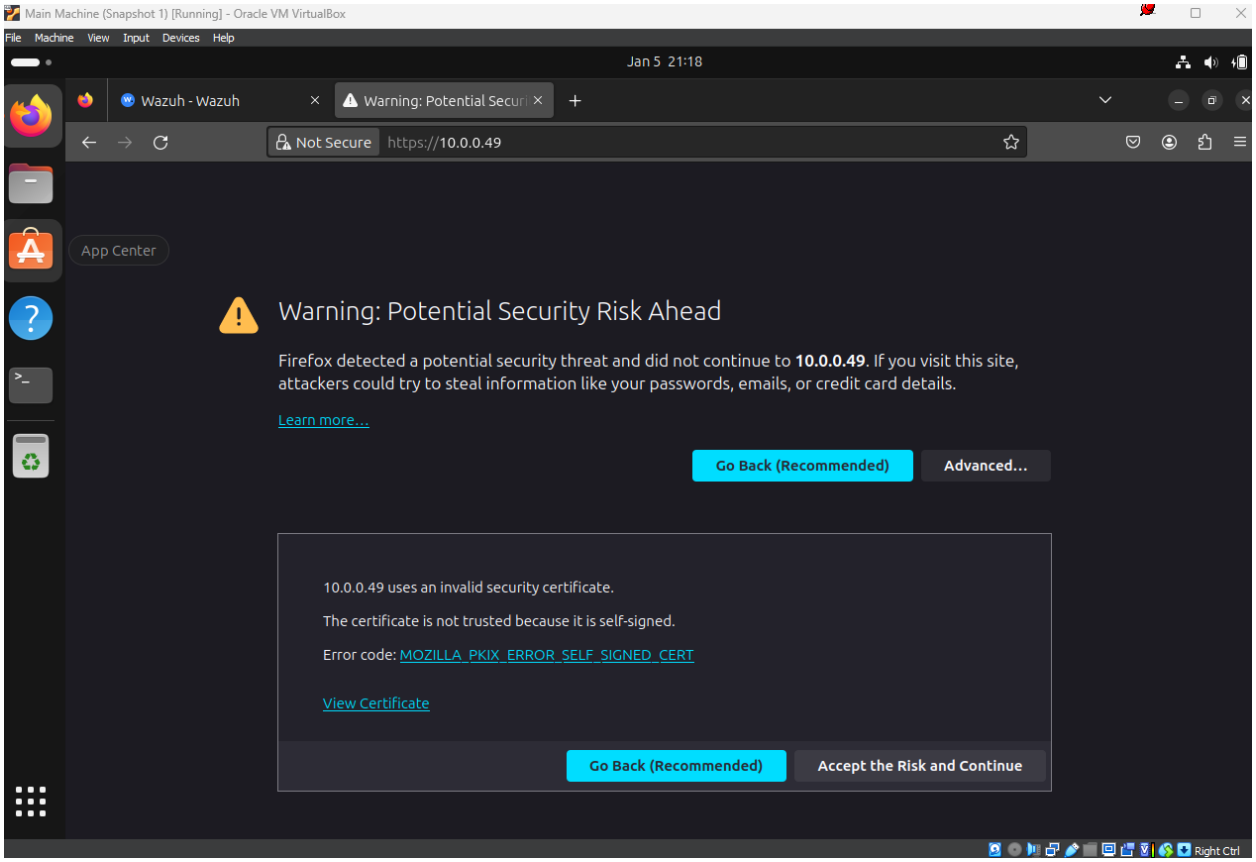
Take note of the new address, this will be the address we need to access the webui on our ubuntu desktop.



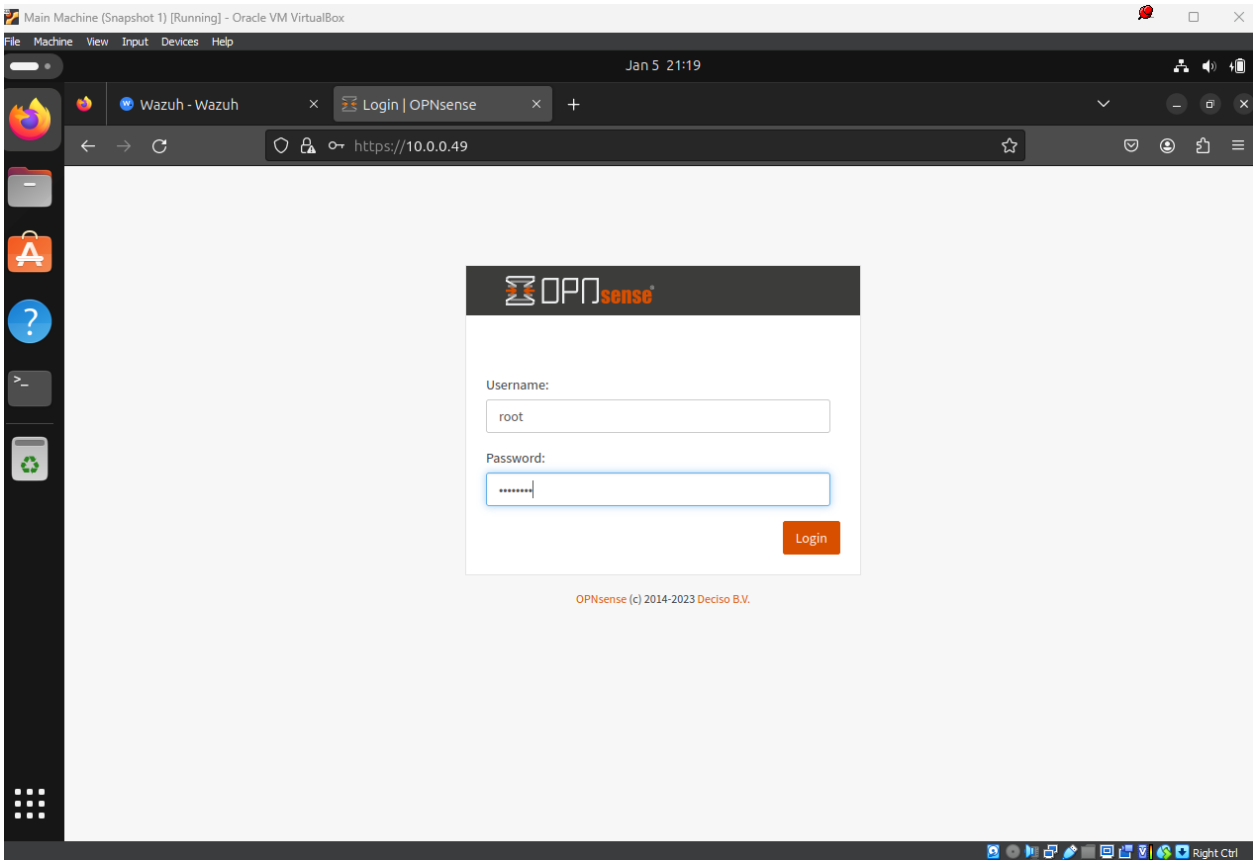
The next steps will now consist of having these machines interact with each other.

Lets go to our ubuntu desktop and type the opnsense address onto the search bar.

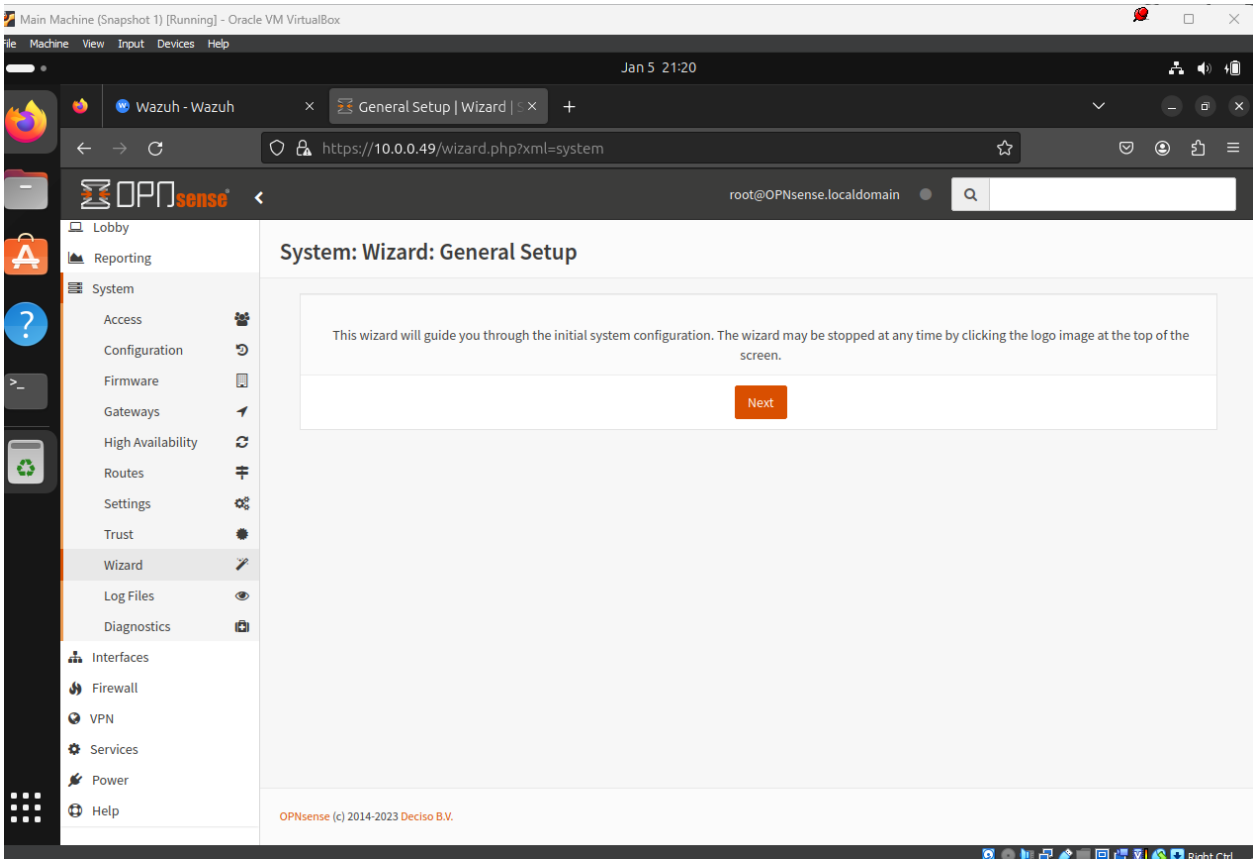
Just like Wazuh, click accept the risks and continue.



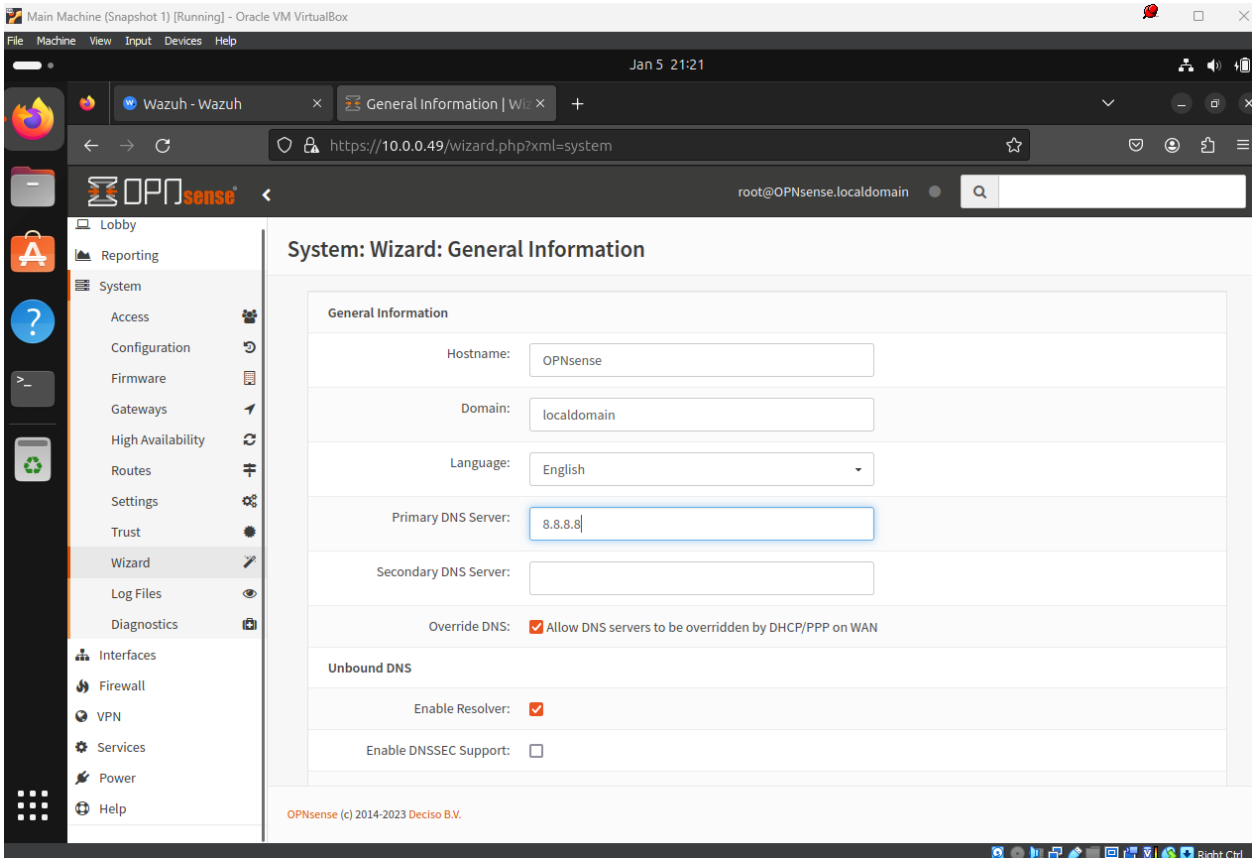
It will use the same password and username as the opnsense server


Main Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 5 21:19
Wazuh - Wazuh
Login | OPNsense
https://10.0.0.49
OPNsense
Username:
root
Password:
Login
OPNsense (c) 2014-2023 Deciso B.V.
Right Ctrl

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

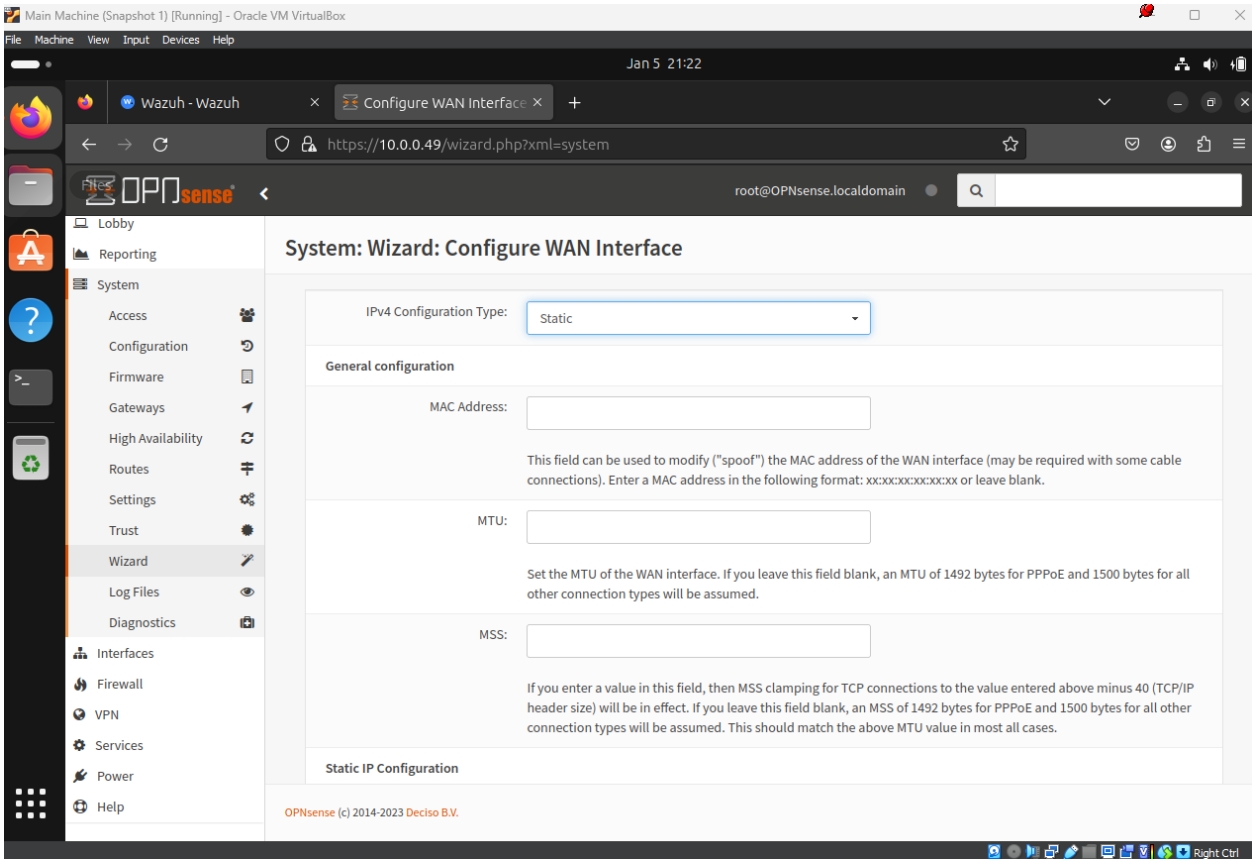


Follow these configurations. Then click next



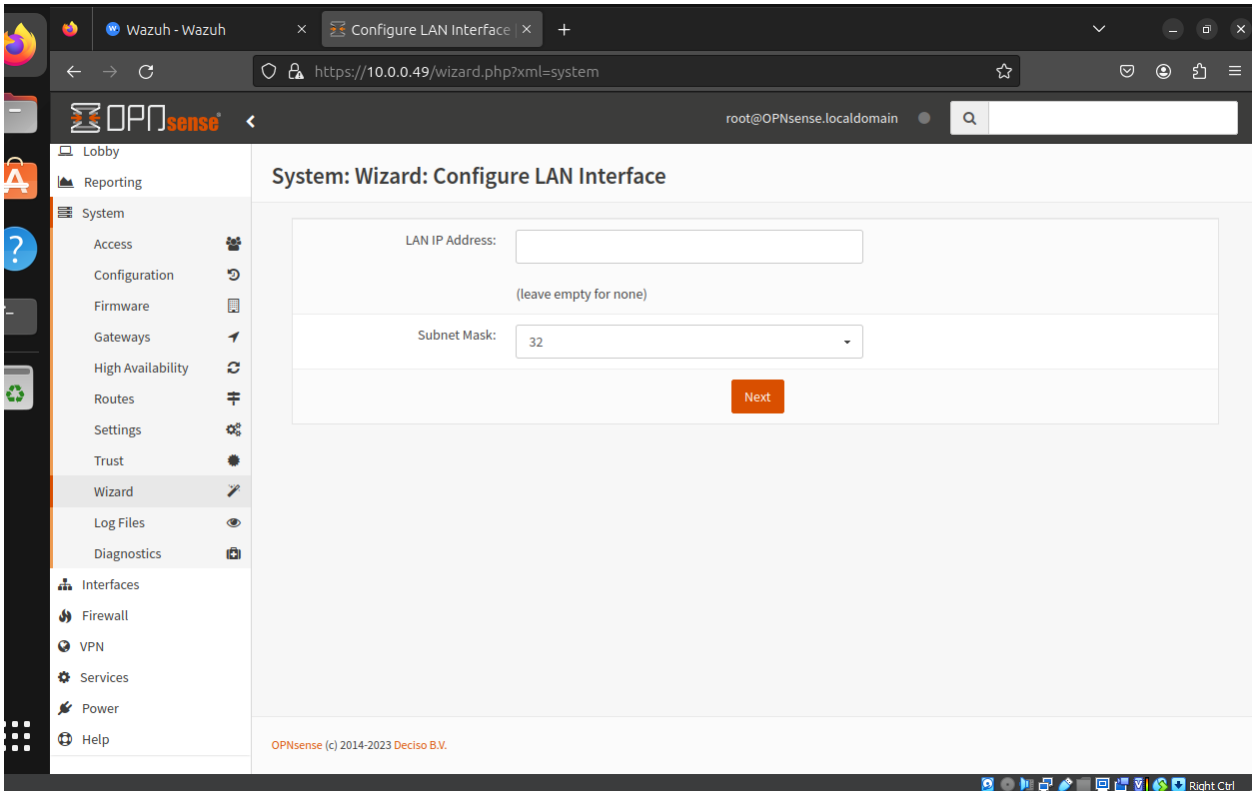
Click next again for time configuration.

We want to change it to static.

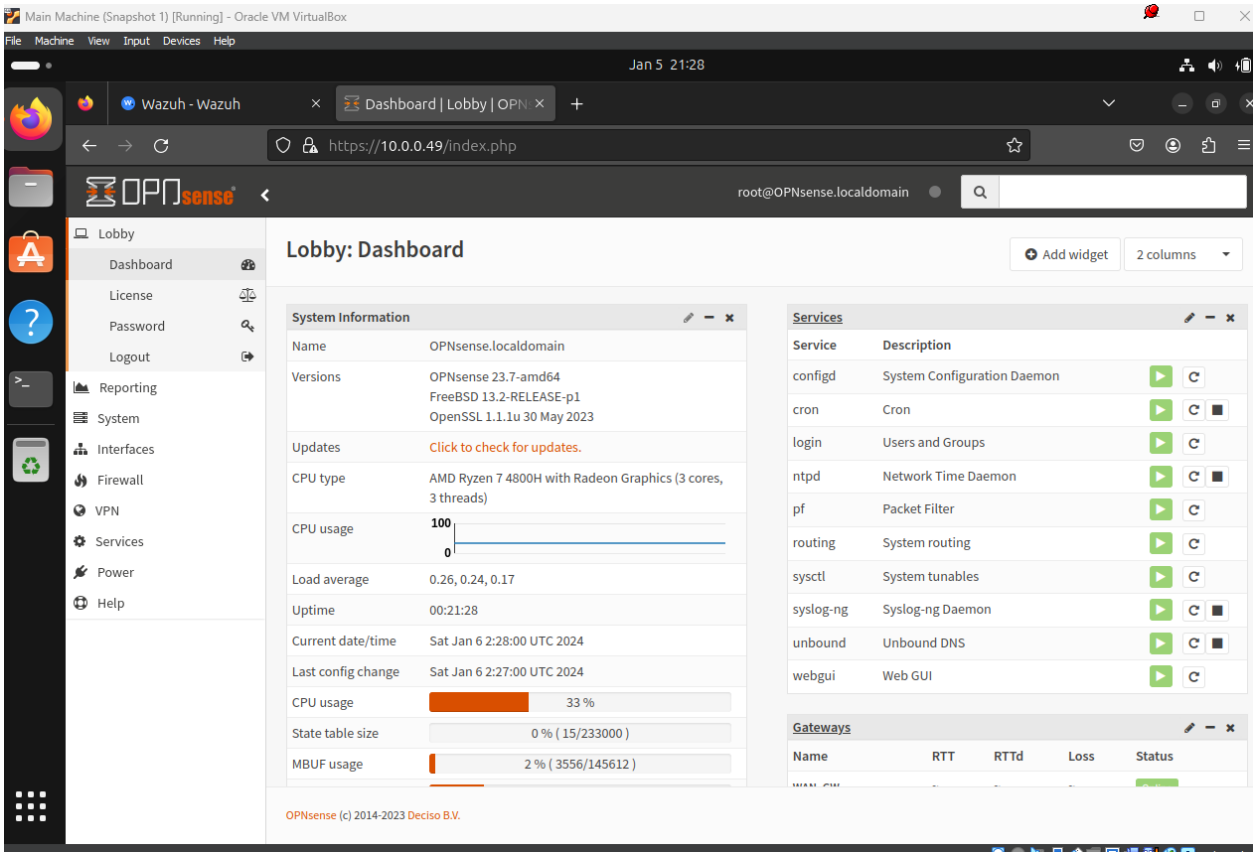


Then enter the same address you are using to access opnsense web gui with a subnet of 24. To look for your gateway, use cmd on your host windows and type ipconfig. You should see you IPv4 address along with the default gateway. That is what I am using here. Click next after this part.

Leave this blank

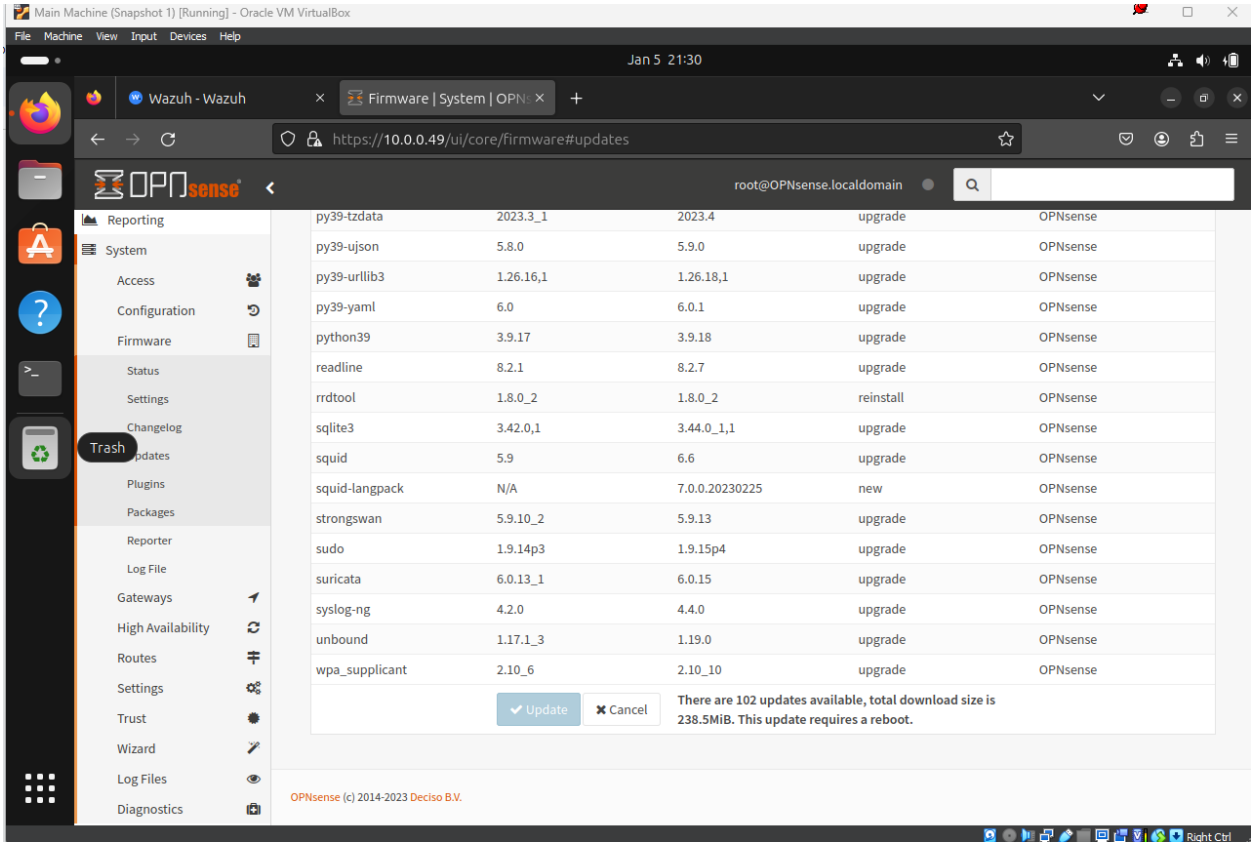


You will be prompted to change your password, that is up to you. I will leave it as is. Then you finally click reload and once it finishes setting up, it should look like this.



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.

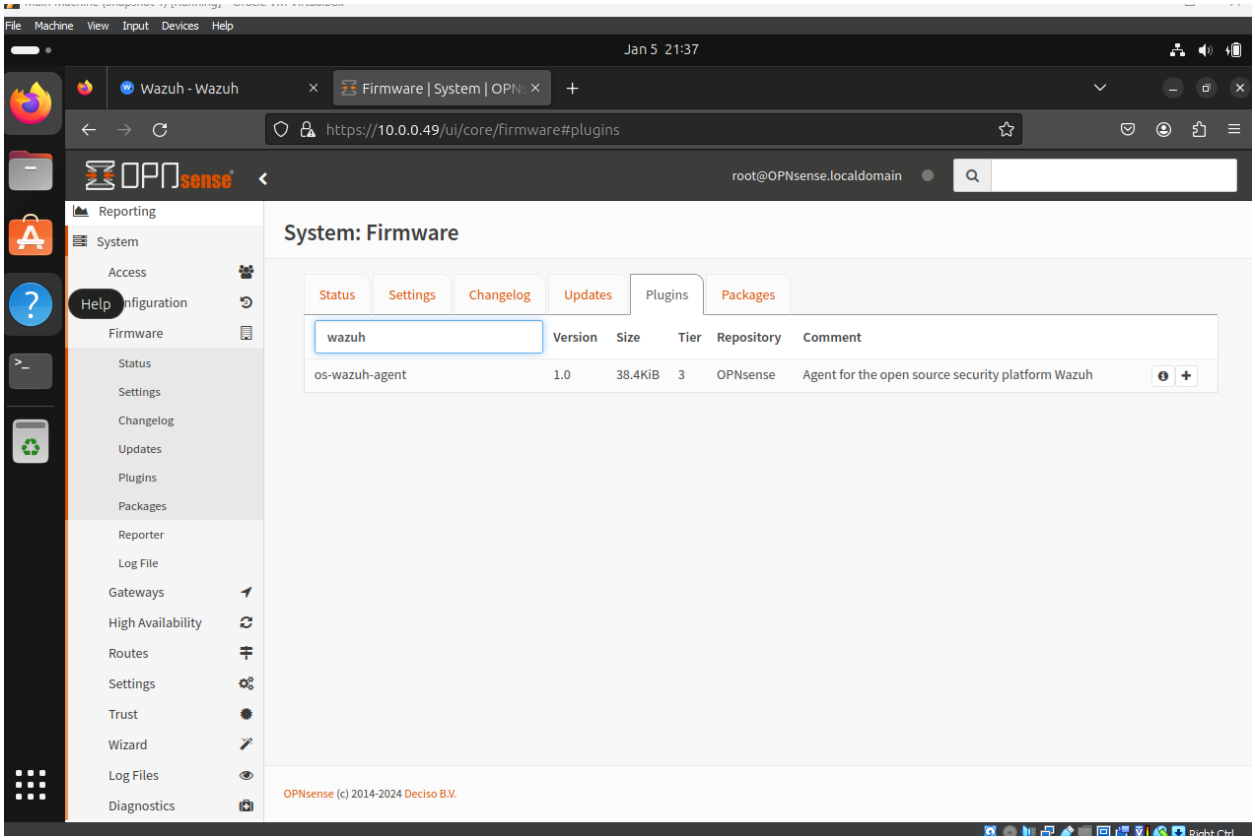


Updating will be crucial since we need the latest version to allow our Wazuh connection.

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

Will start by going to System>Firmware>Plugins

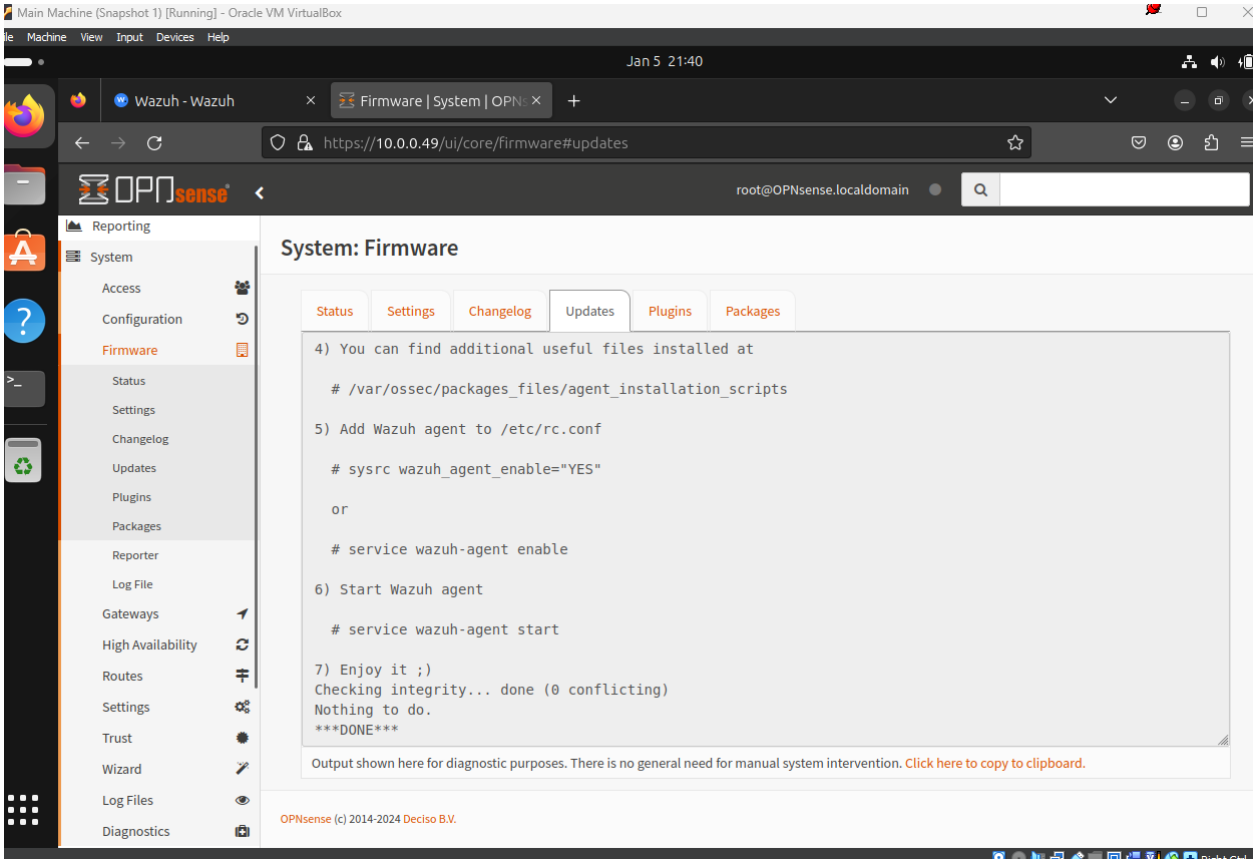
Then search for wazuh like shown below.



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

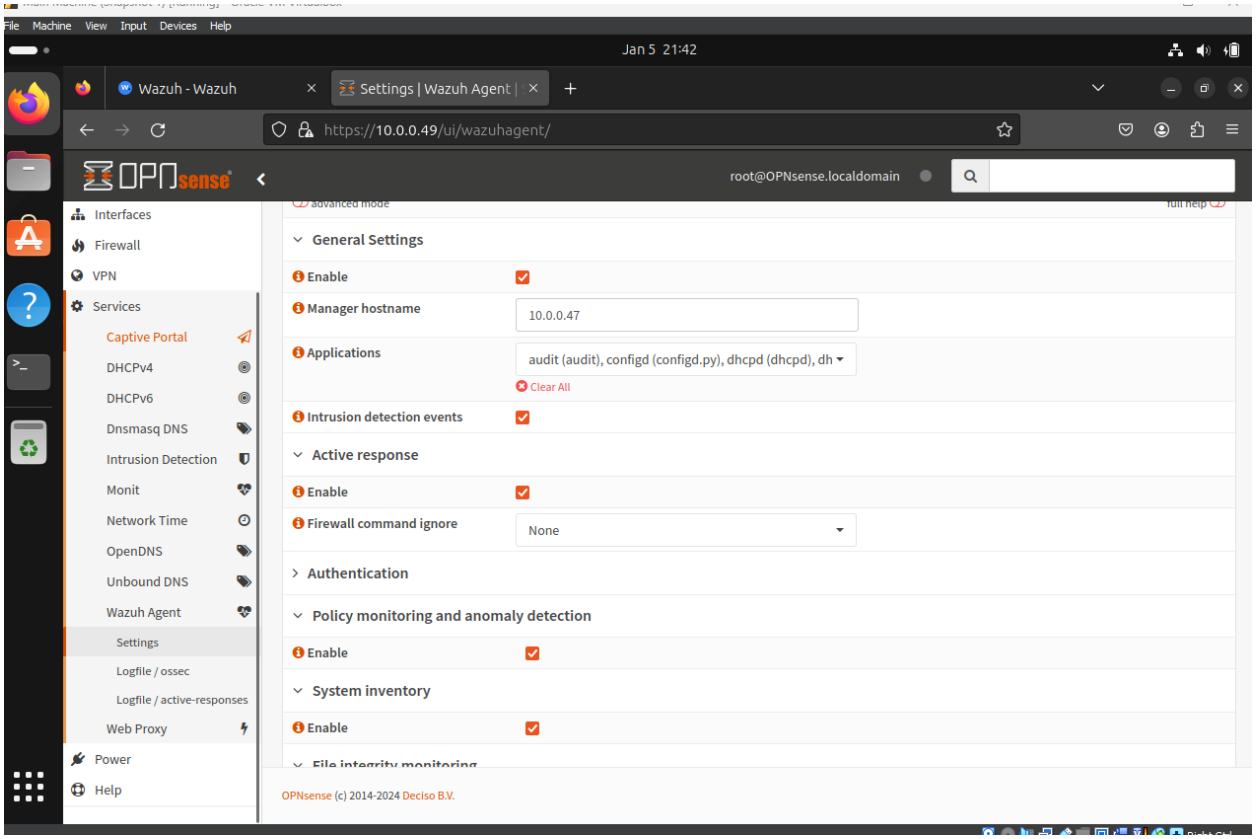
But now click the plus icon on the right and install.

You should be met with this



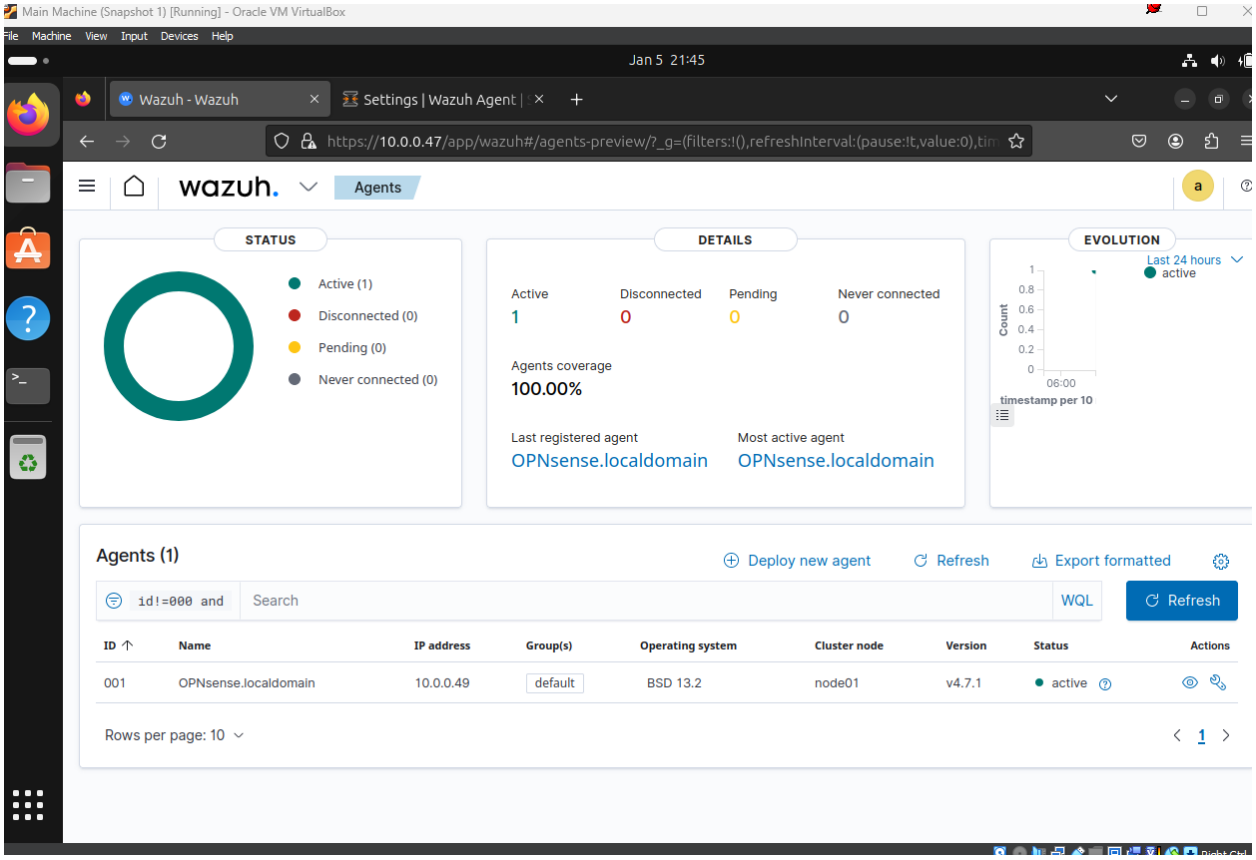
GNow reload the page and then head to Services> Wazuh Agent> Settings

Follow my configurations. Your wazuh ip address will be different than mine.



Finally click apply.

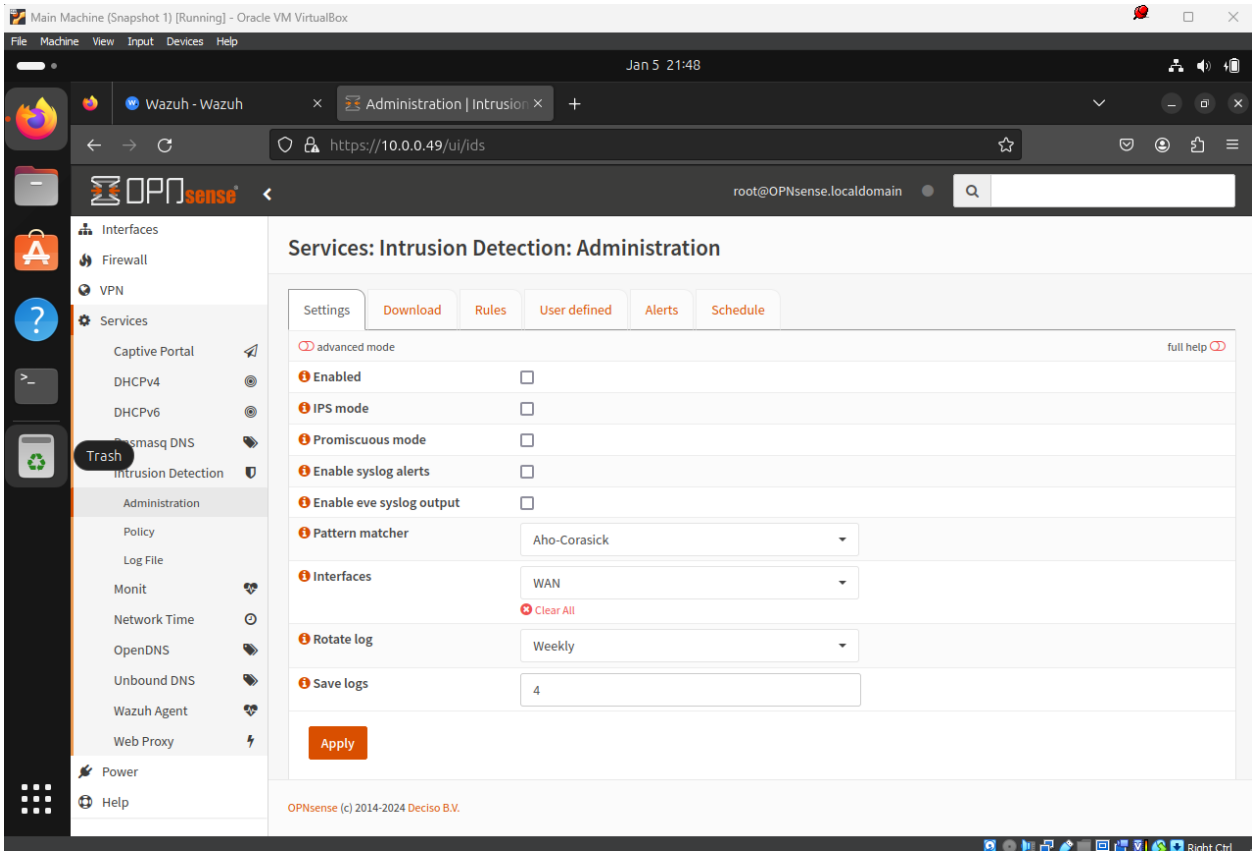
Check back on the wazuh dashboard and we should now have been connected!



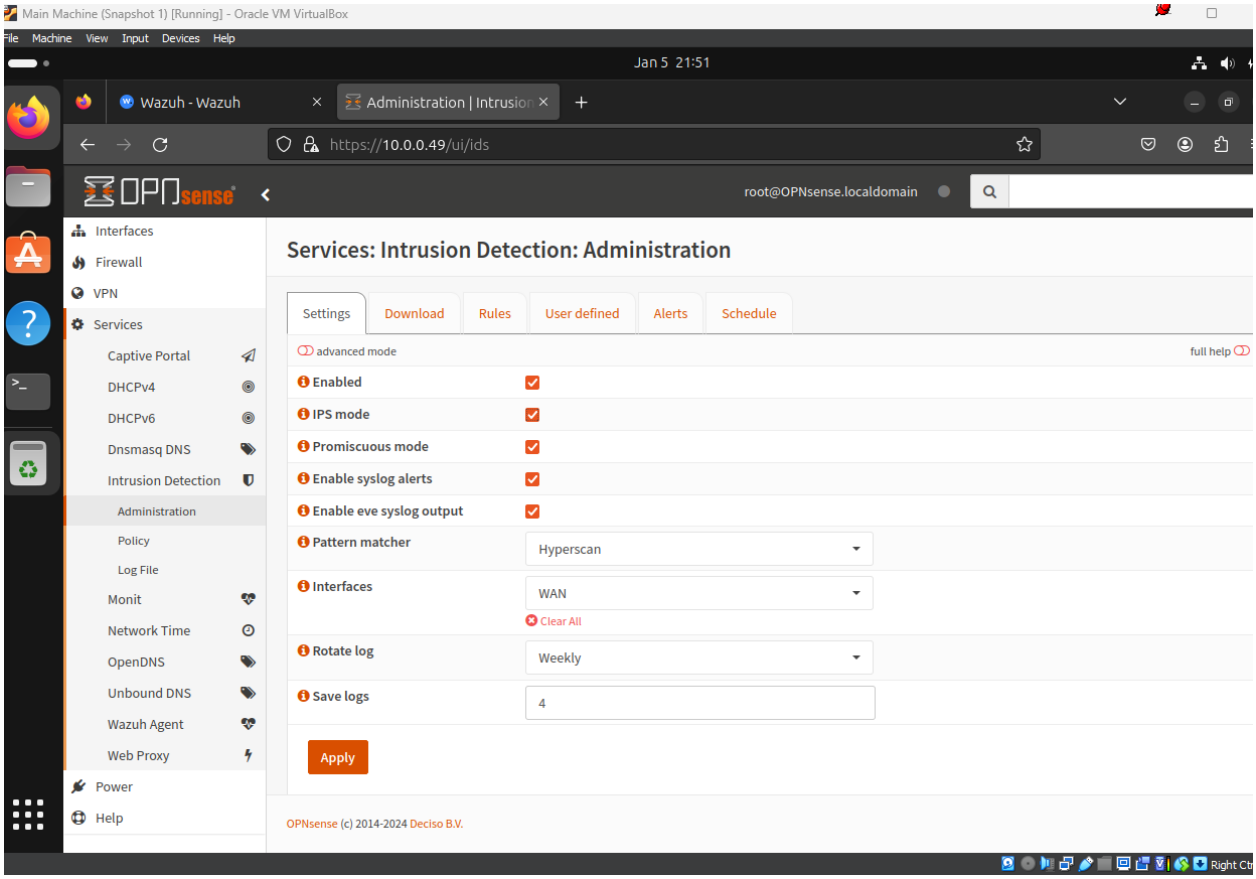
Next, we will activate our built in suricata for ips/ids monitoring.

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

You should end up here.



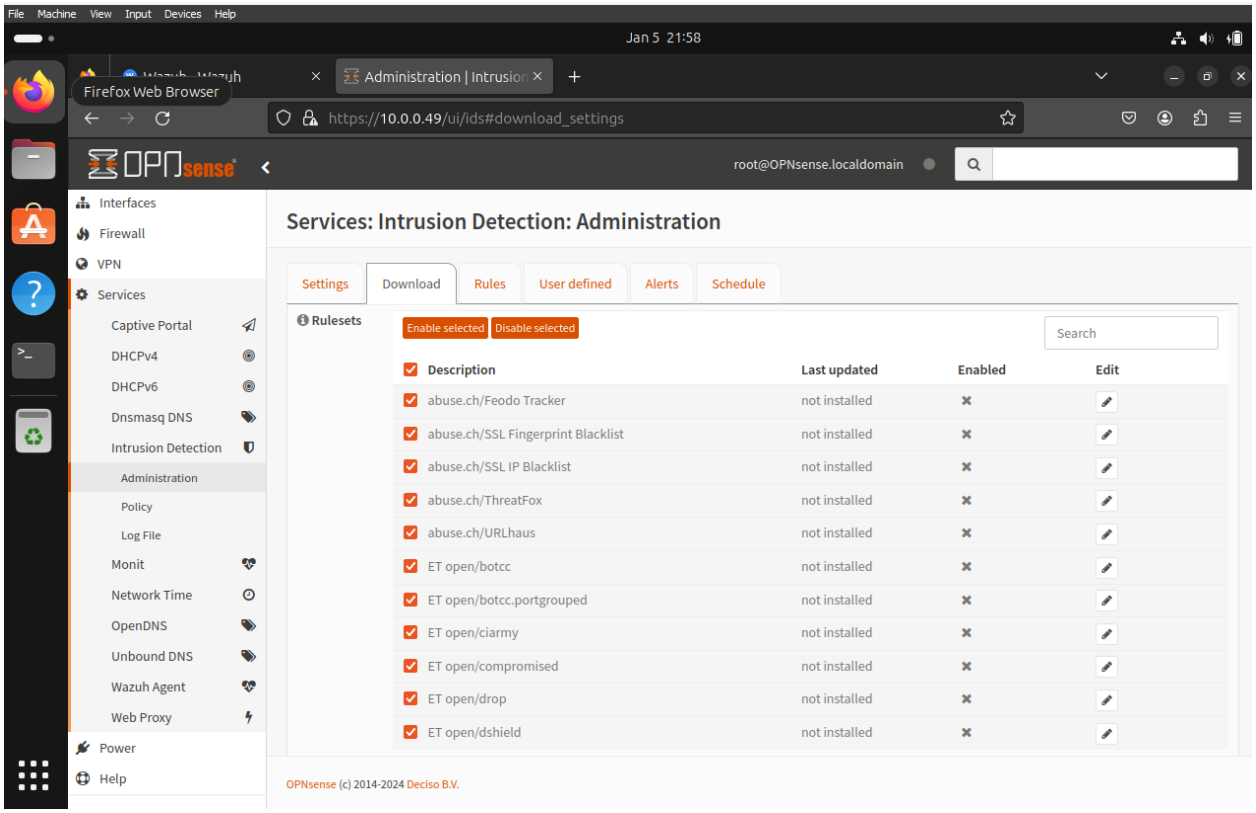
Now follow these configurations.



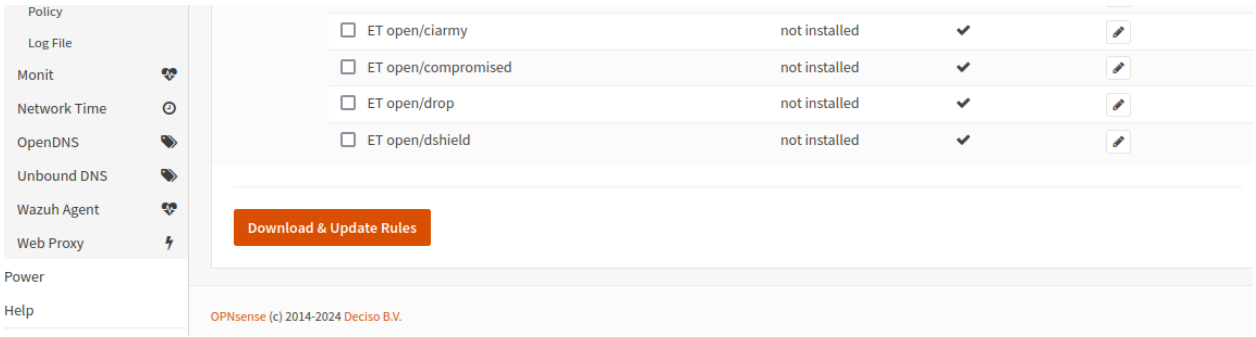
Then click apply.

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

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

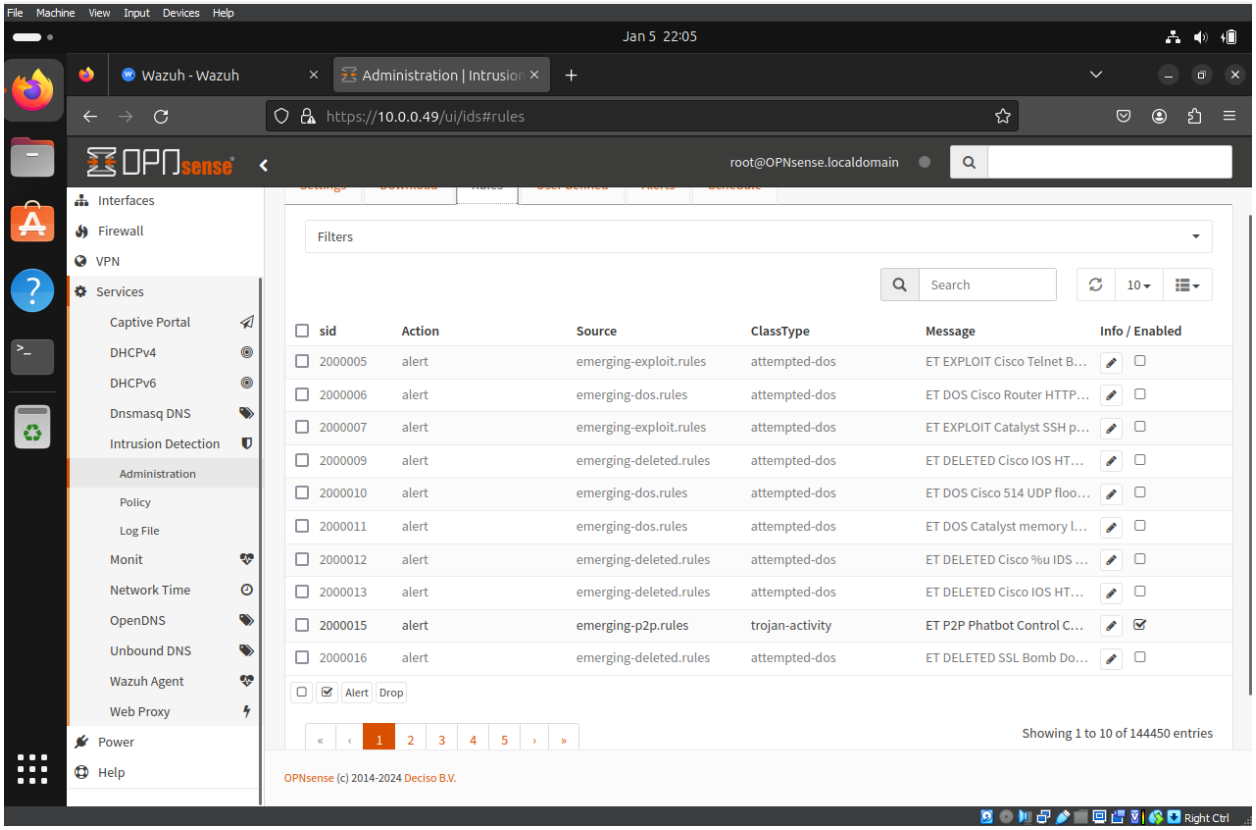


Then click download and update rules



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

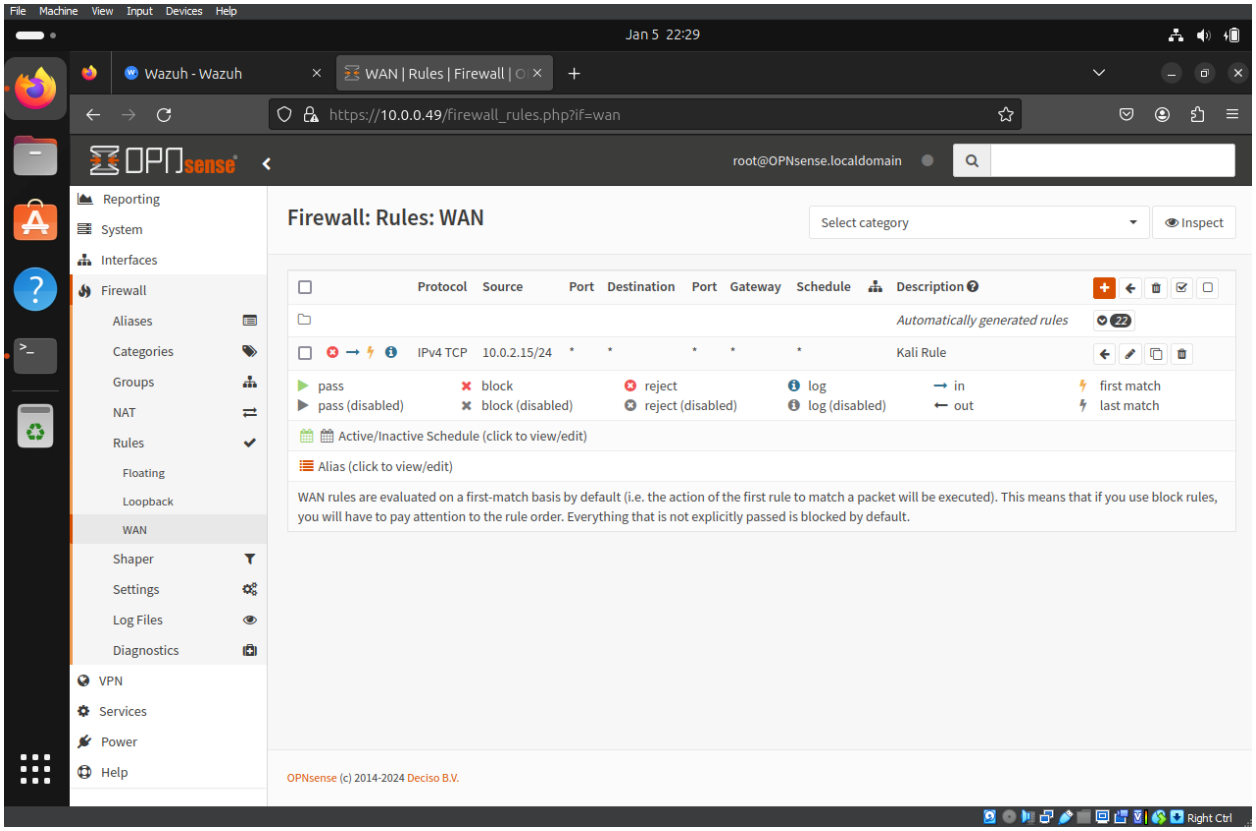
After the download finishes, head to the rules tab and you should now have a ton of rules set for any attack!



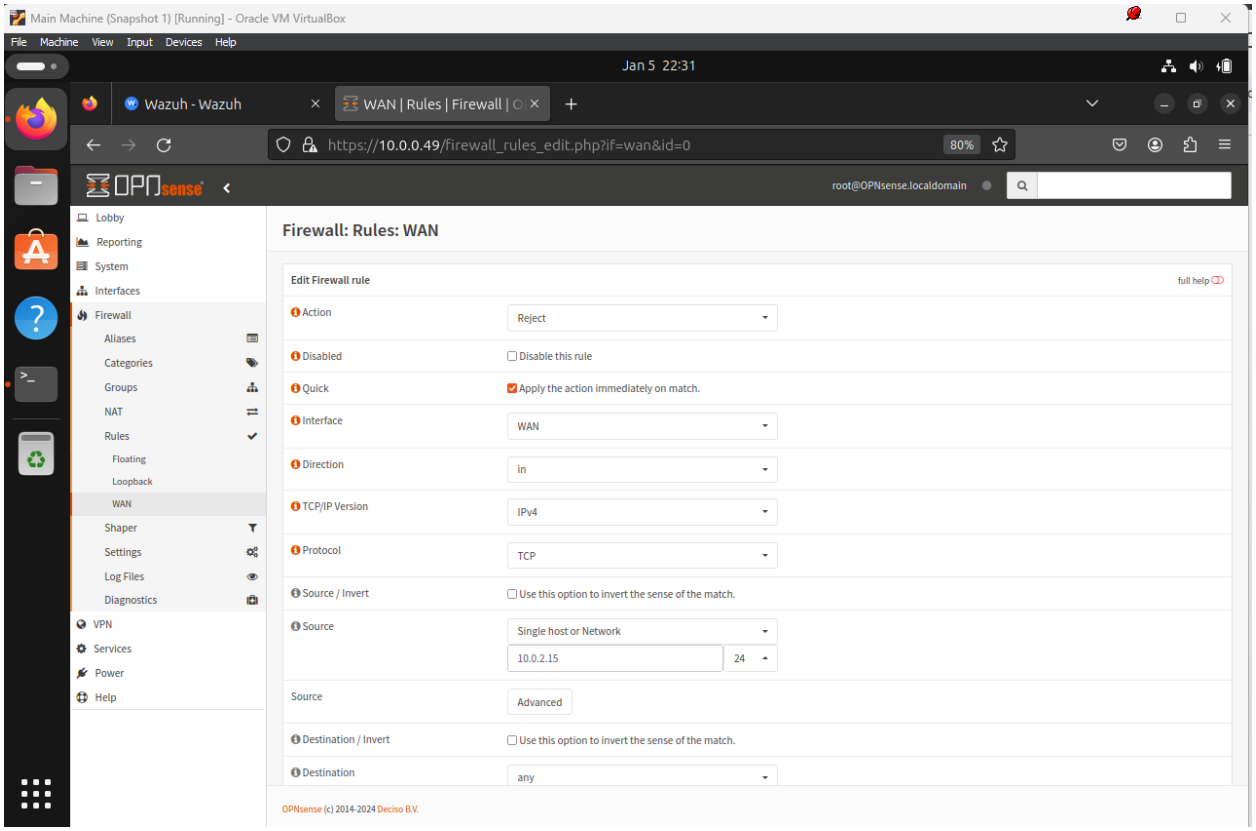
We will now try to make alerts for Suricata to pick up along with Wazuh.

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.

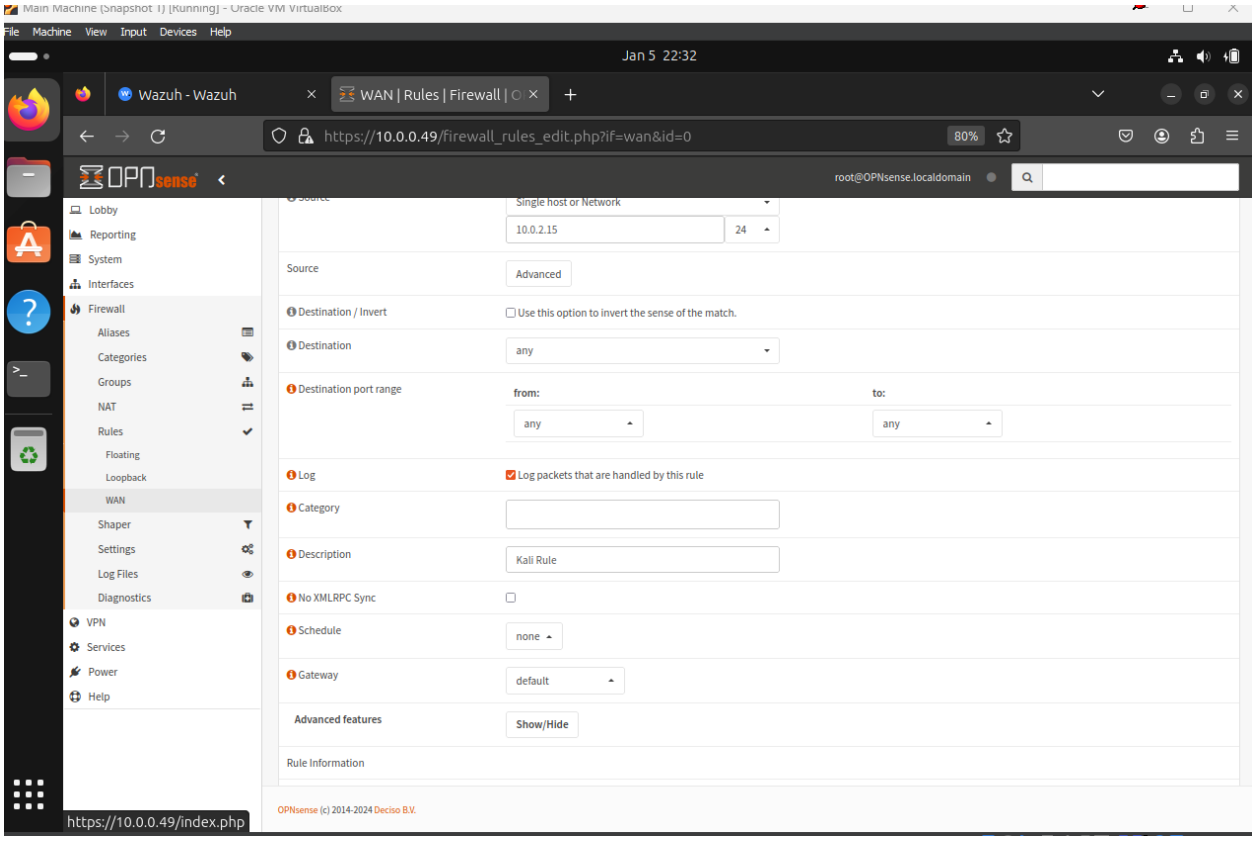


As you can see I already set up my firewall rule called Kali but I will show you what I set up.



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

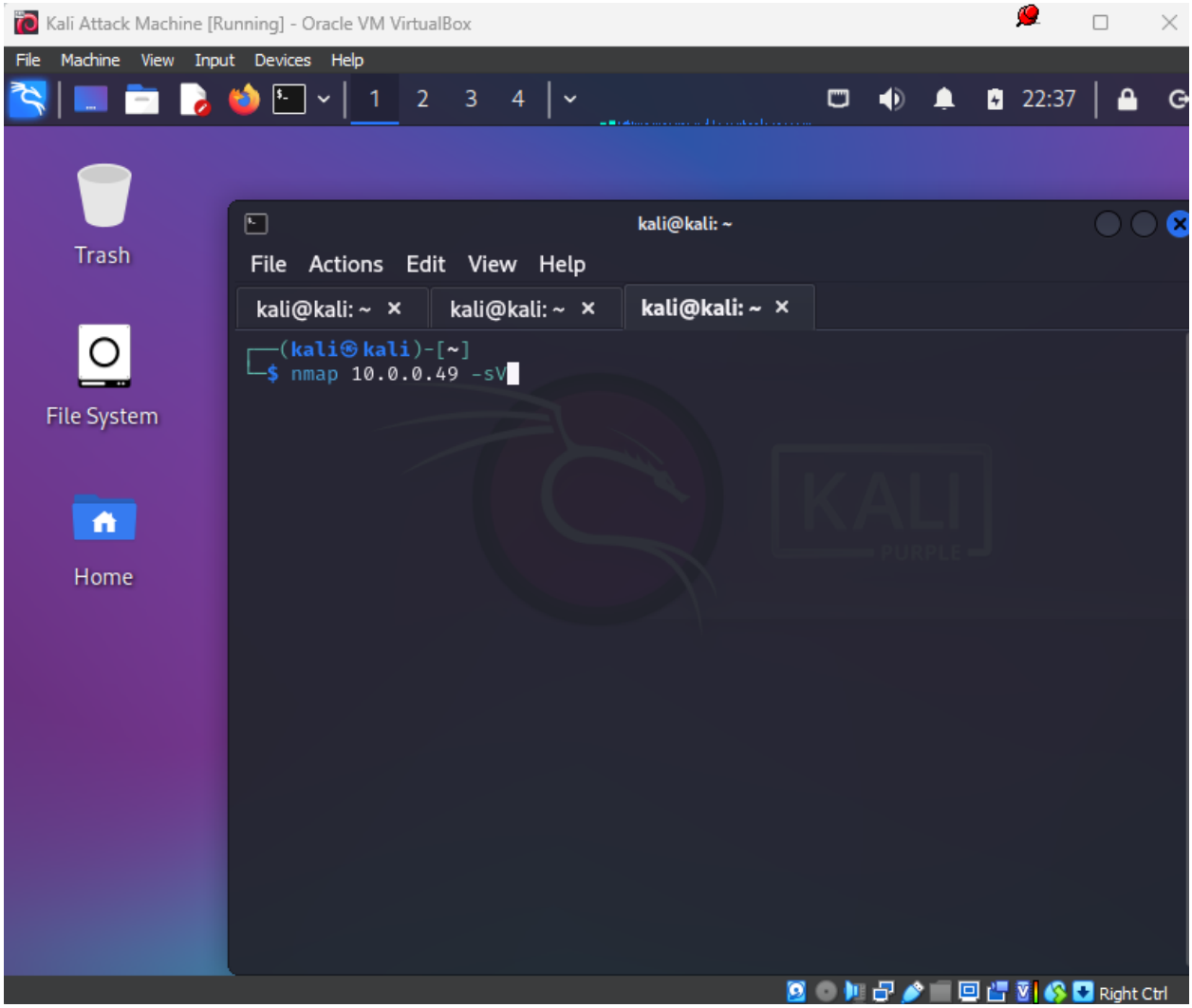
Scrolling a bit lower, we have to make sure to tick the box for collecting logs. After that, we can save and exit.



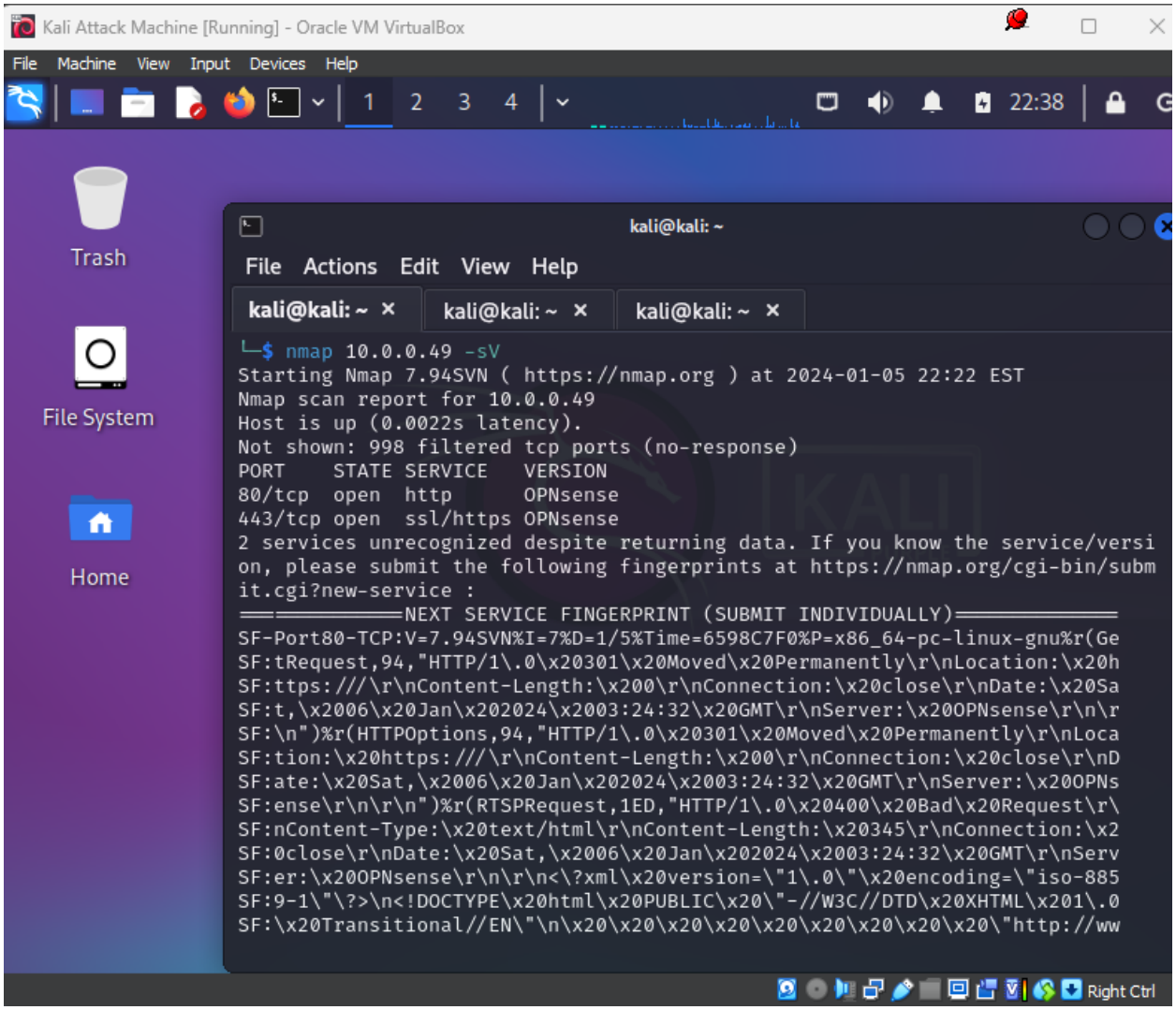
You will get a blue box telling you to apply changes, click apply and that should do it. Without applying changes the firewall will not take effect.

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

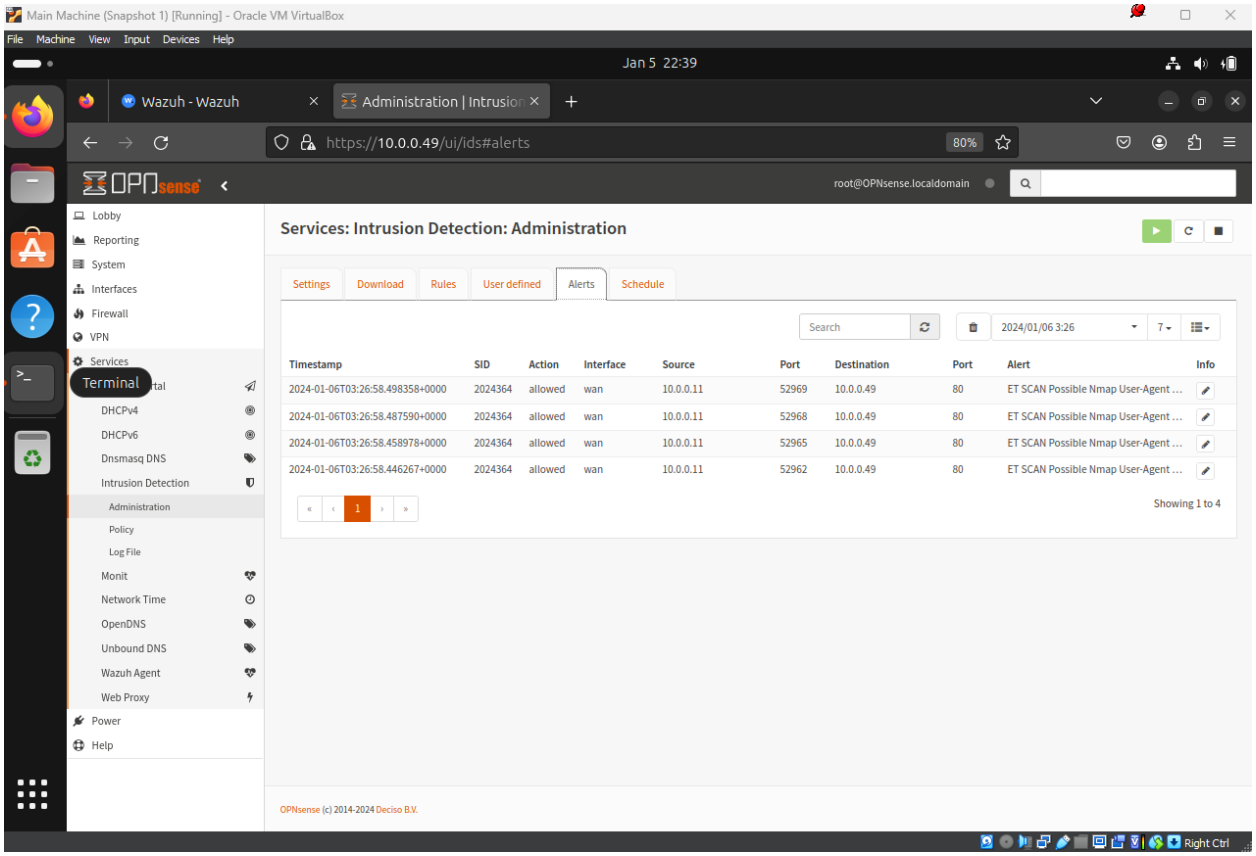
Lets try using this.

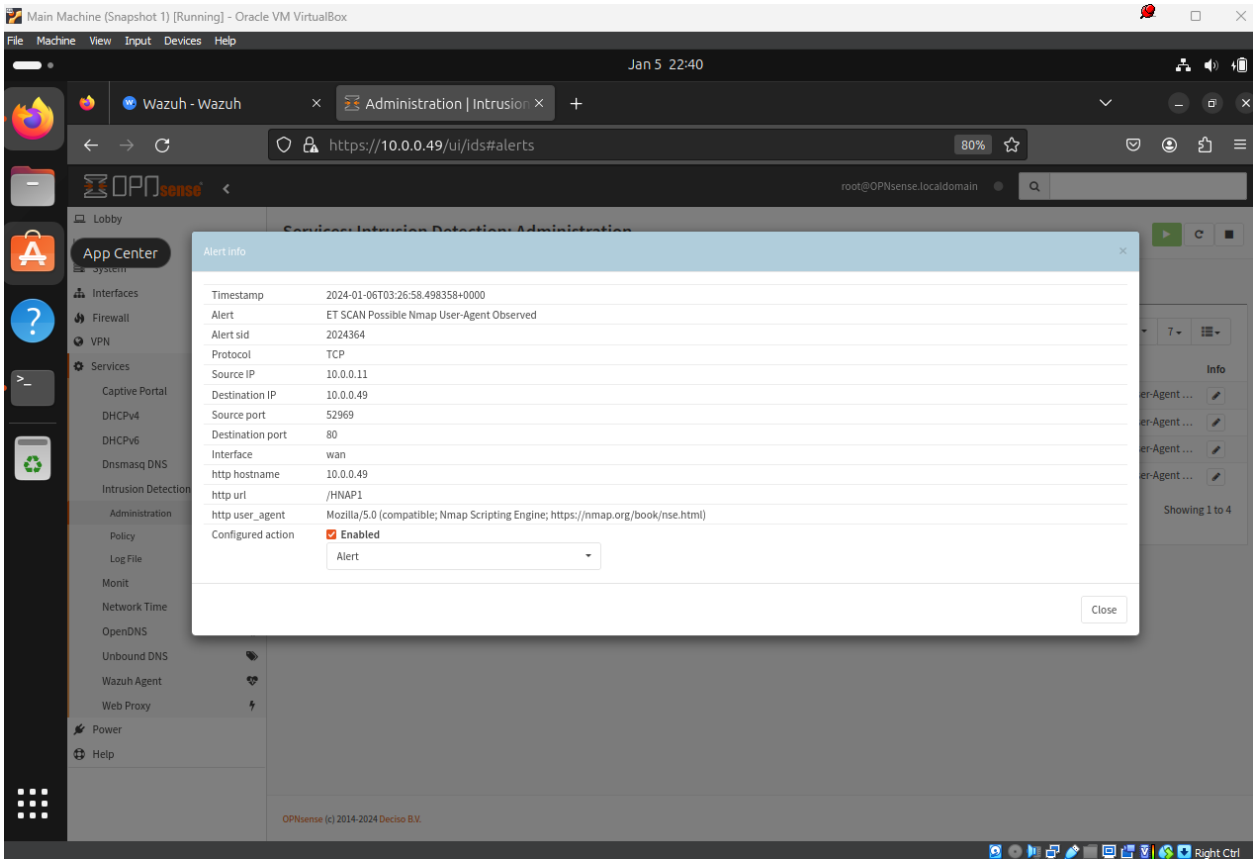


And here are the results,

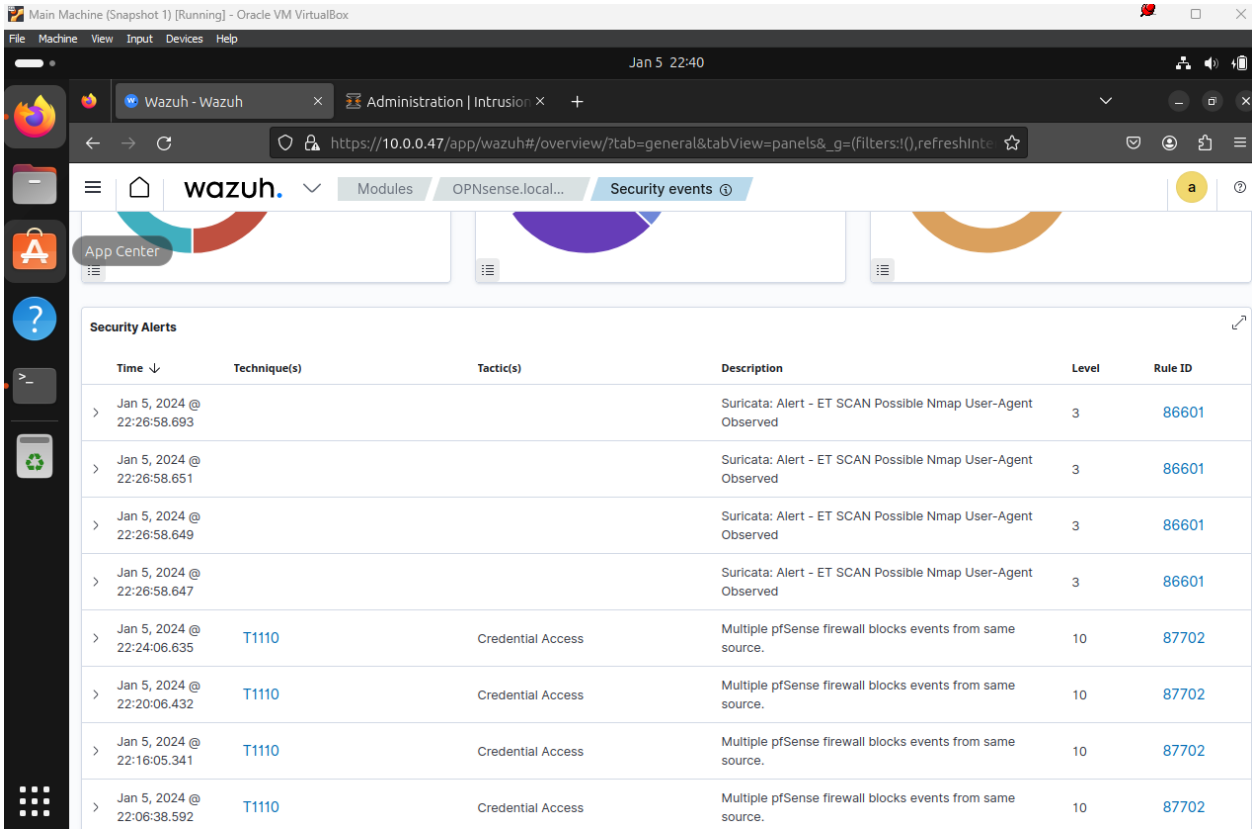


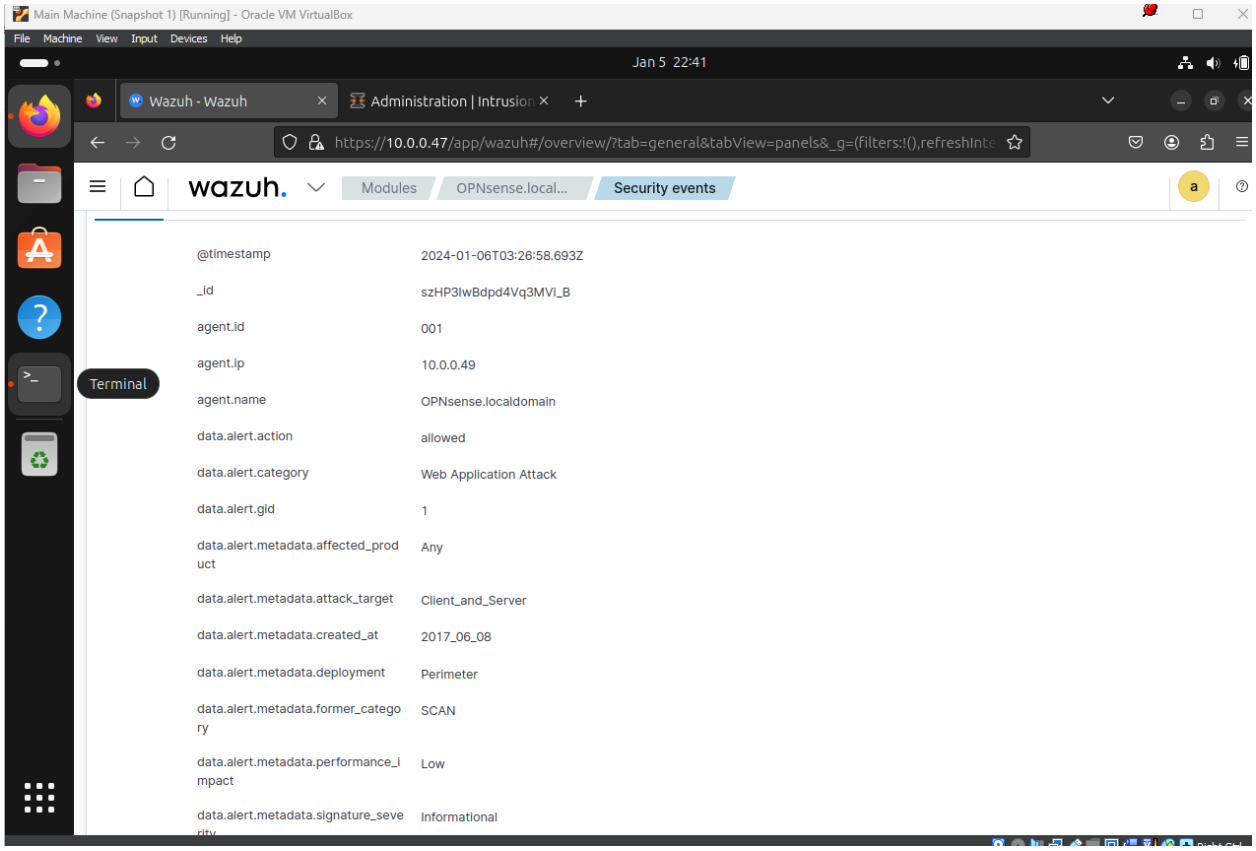
Now if we take a look at our Suricata, we get this,

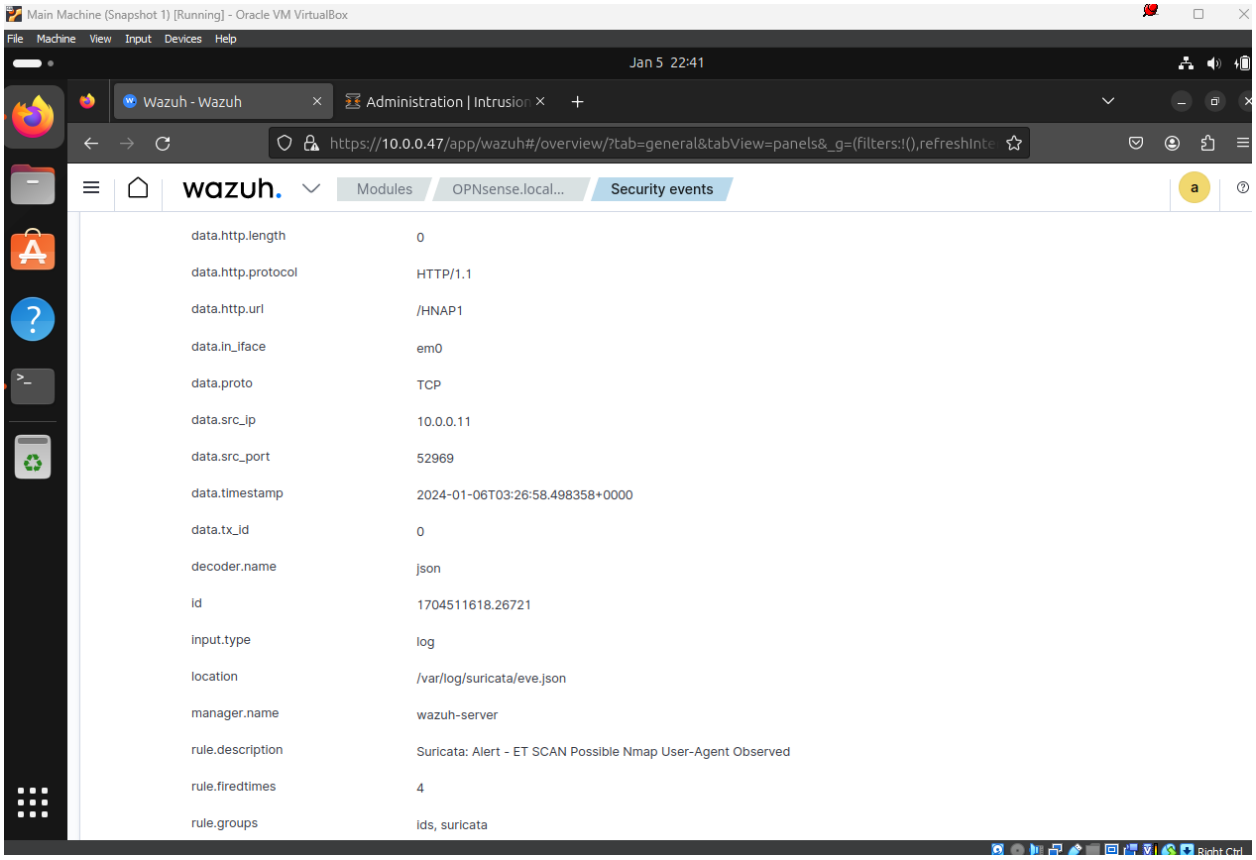

Main Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 5 22:39
Wazuh - Wazuh
Administration | Intrusion
https://10.0.0.49/ui/ids#alerts
80%
root@OPNsense.localdomain
Terminal
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
DHCPv4
DHCPv6
Dnsmasq DNS
Intrusion Detection
Administration
Policy
Log File
Monit
Network Time
OpenDNS
Unbound DNS
Wazuh Agent
Web Proxy
Power
Help
Services: Intrusion Detection: Administration
Settings
Download
Rules
User defined
Alerts
Schedule
Search
2024/01/06 3:26
Timestamp
SID
Action
Interface
Source
Port
Destination
Port
Alert
Info
2024-01-06T03:26:58.498358+0000 2024364 allowed wan 10.0.0.11 52969 10.0.0.49 80 ET SCAN Possible Nmap User-Agent ...
2024-01-06T03:26:58.487590+0000 2024364 allowed wan 10.0.0.11 52968 10.0.0.49 80 ET SCAN Possible Nmap User-Agent ...
2024-01-06T03:26:58.458978+0000 2024364 allowed wan 10.0.0.11 52965 10.0.0.49 80 ET SCAN Possible Nmap User-Agent ...
2024-01-06T03:26:58.446267+0000 2024364 allowed wan 10.0.0.11 52962 10.0.0.49 80 ET SCAN Possible Nmap User-Agent ...
Showing 1 to 4
OPNsense (c) 2014-2024 Deciso B.V.
Right Ctrl


Main Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 5 22:40
Wazuh - Wazuh
Administration | Intrusion
https://10.0.0.49/ui/ids#alerts
80%
root@OPNsense.localdomain
App Center
Alert info
Timestamp 2024-01-06T03:26:58.498358+0000
Alert ET SCAN Possible Nmap User-Agent Observed
Alert sid 2024364
Protocol TCP
Source IP 10.0.0.11
Destination IP 10.0.0.49
Source port 52969
Destination port 80
Interface wan
http hostname 10.0.0.49
http url /HNAP1
http user_agent Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Configured action
Enabled
Alert
Close
OPNsense (c) 2014-2024 Deciso B.V.
Right Ctrl

And through Wazuh…




Main Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 5 22:41
Wazuh - Wazuh
Administration | Intrusion
https://10.0.0.47/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInte
wazuh.
Modules
OPNsense.local...
Security events
Terminal
@timestamp 2024-01-06T03:26:58.693Z
_id szHP3IwBdpd4Vq3MVi_B
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.gid 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


Main Machine (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 5 22:41
Wazuh - Wazuh
Administration | Intrusion
https://10.0.0.47/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInte
wazuh.
Modules
OPNsense.local...
Security events
data.http.length 0
data.http.protocol HTTP/1.1
data.http.url /HNAP1
data.in_iface 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.