

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 il 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.

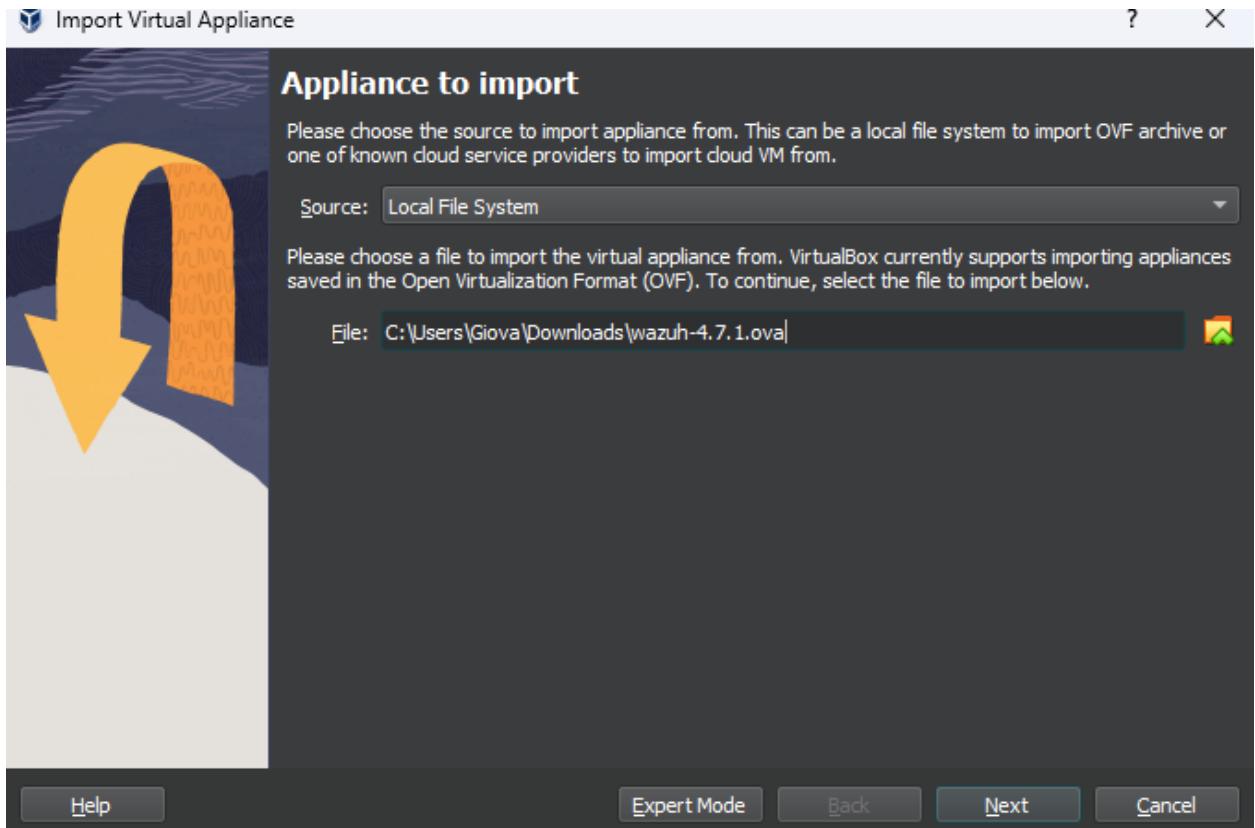
Write down the gateway address on the notepad, in which mine is 10.0.0.1

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.



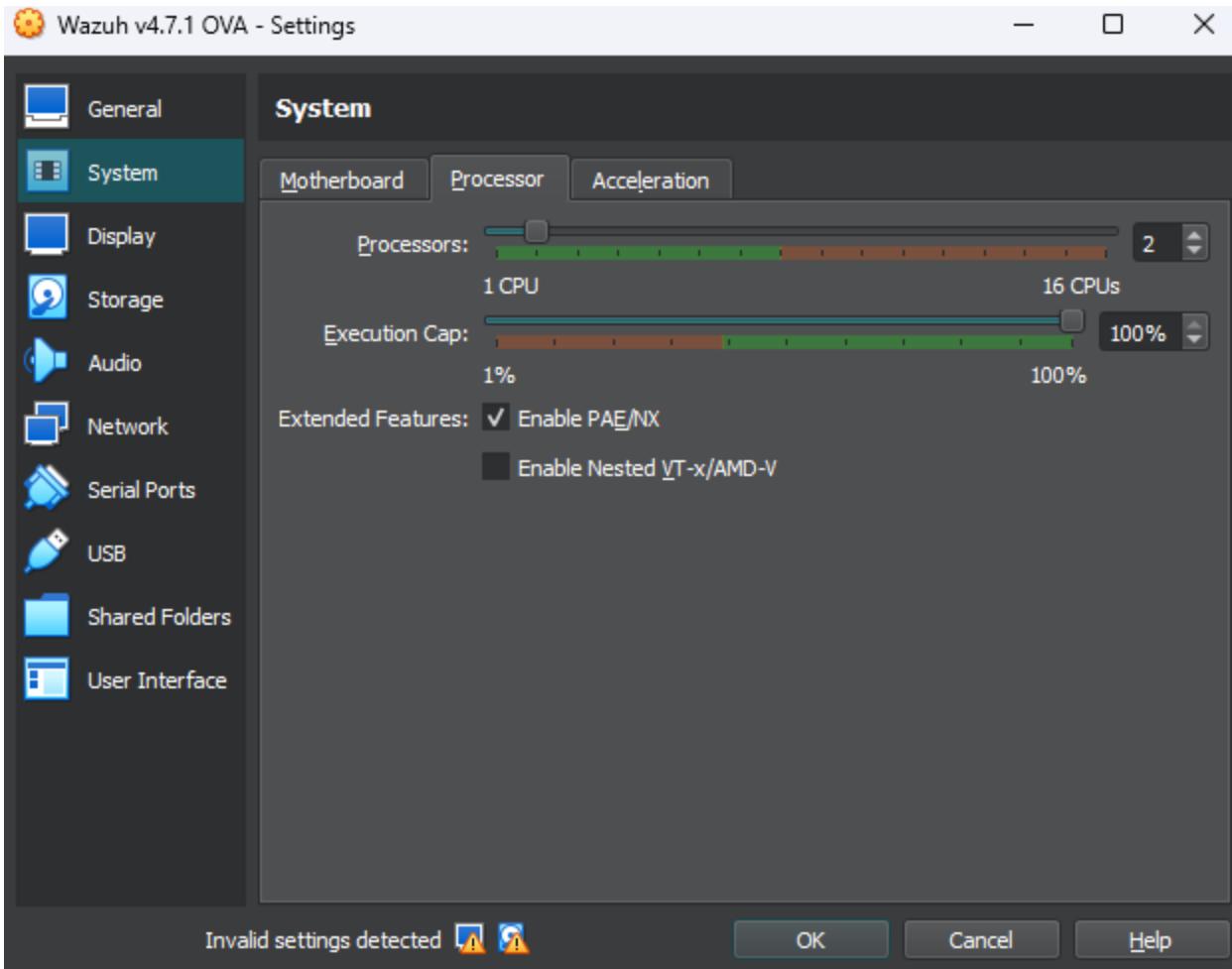
Click next

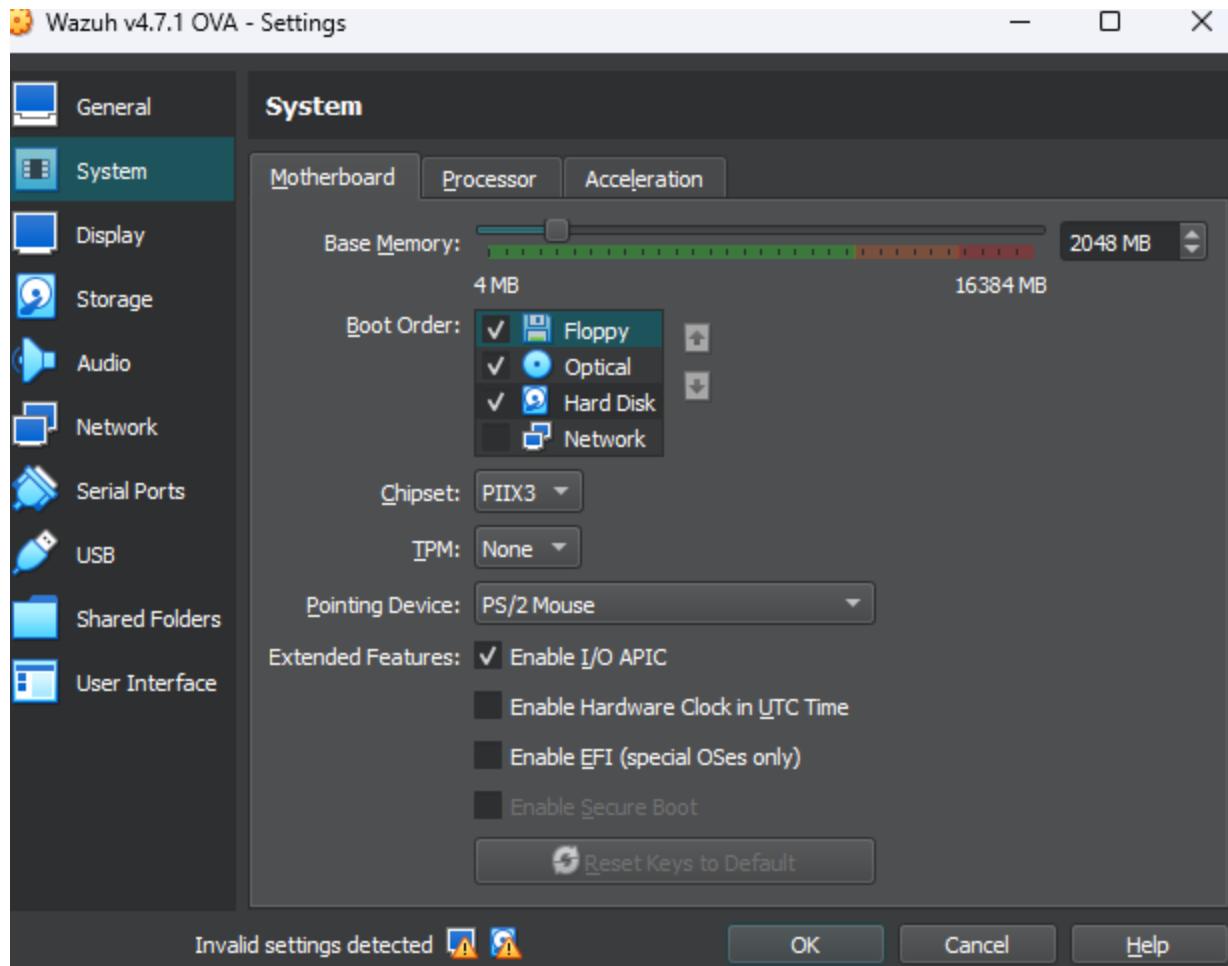
Make sure to give it new MAC addresses



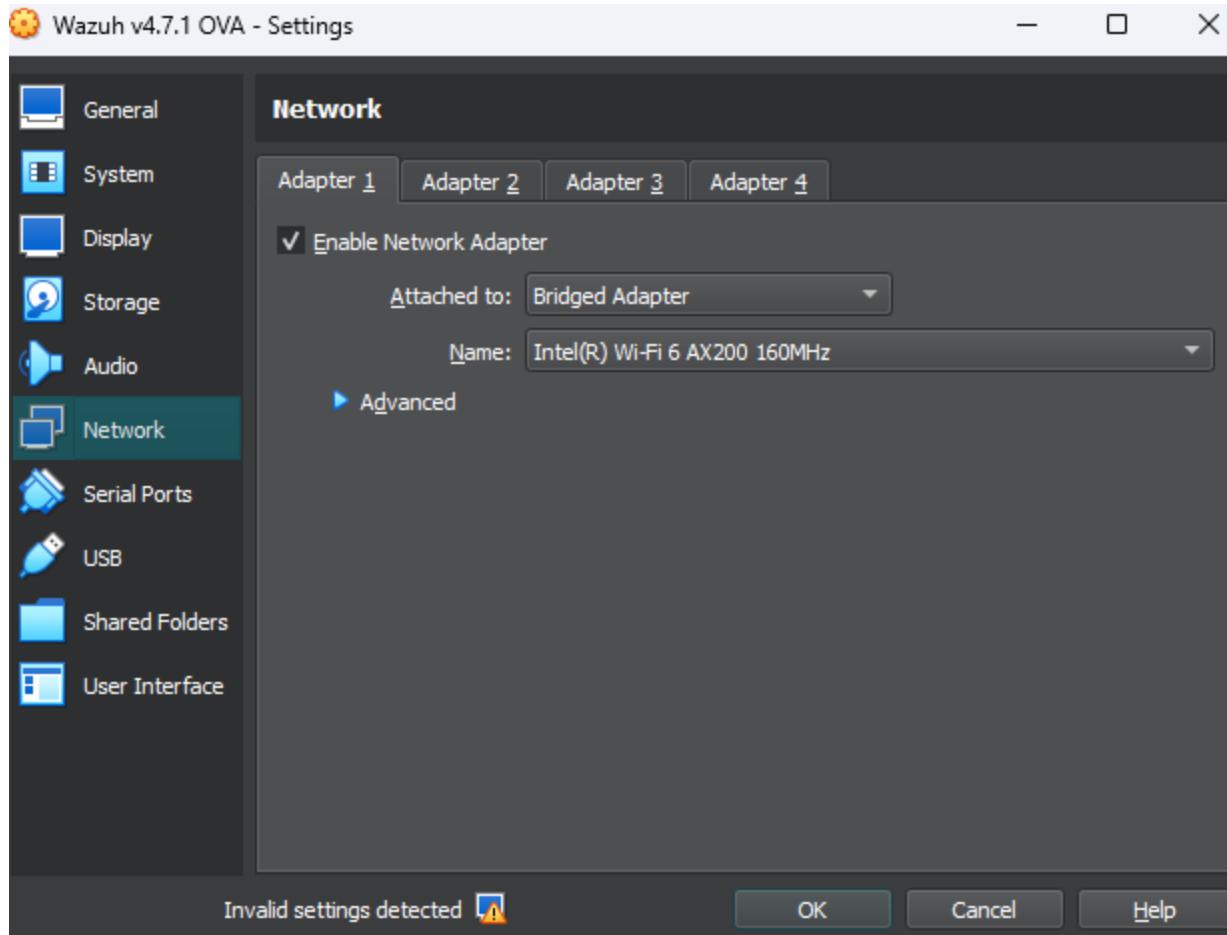
And click finish

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

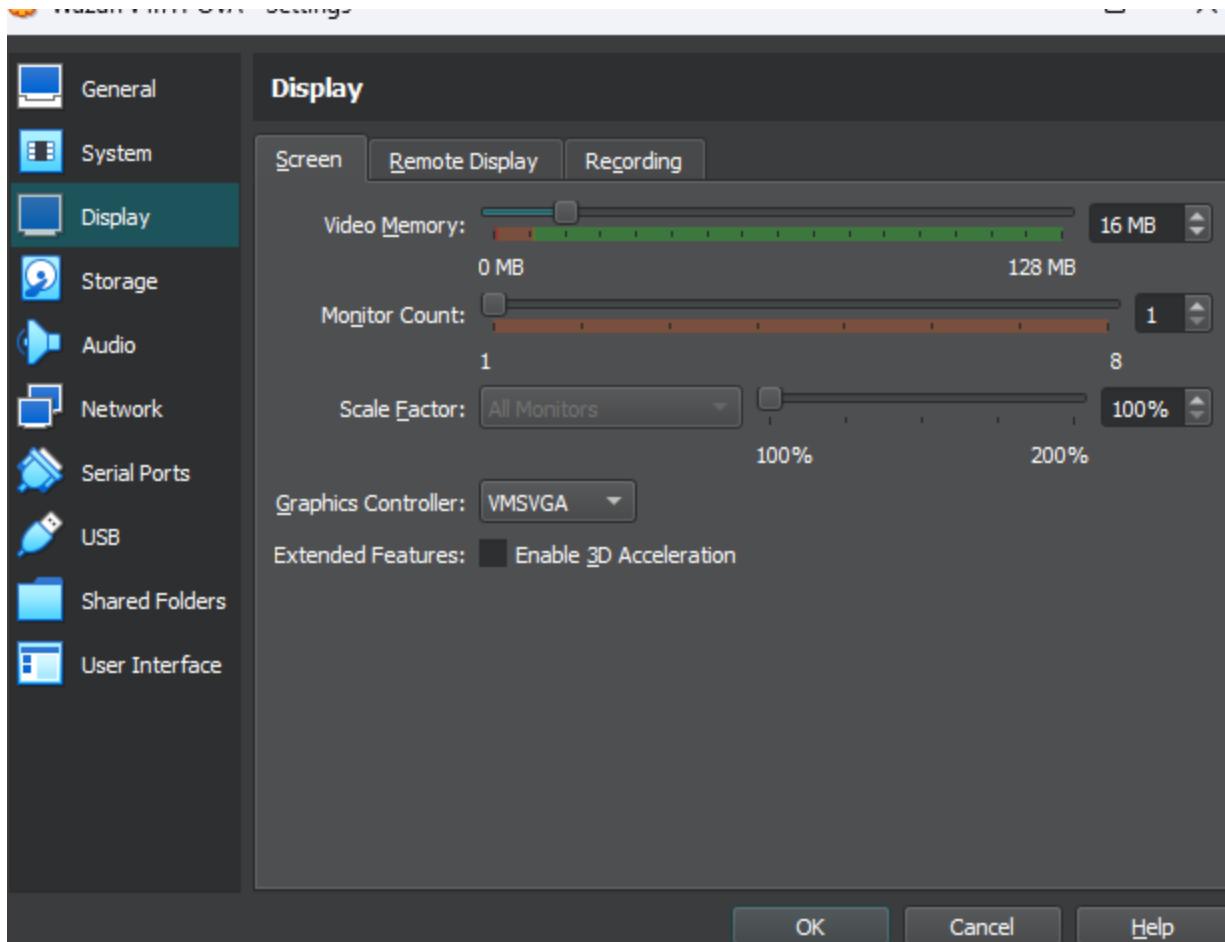




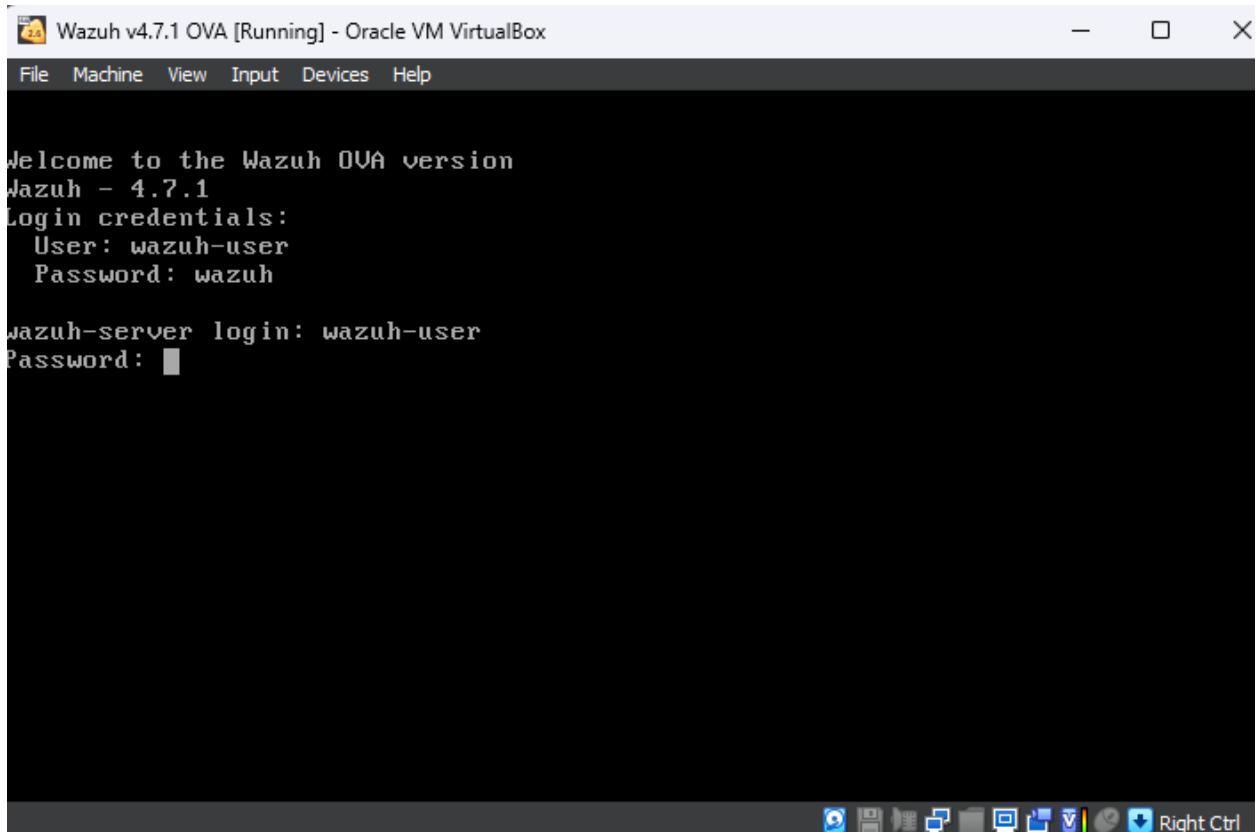
Next we will change the network adapter to Bridged adapter and then finally start the machine.



Change the graphic controller so Wazuh doesn't 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.

```
File Machine View Input Devices Help

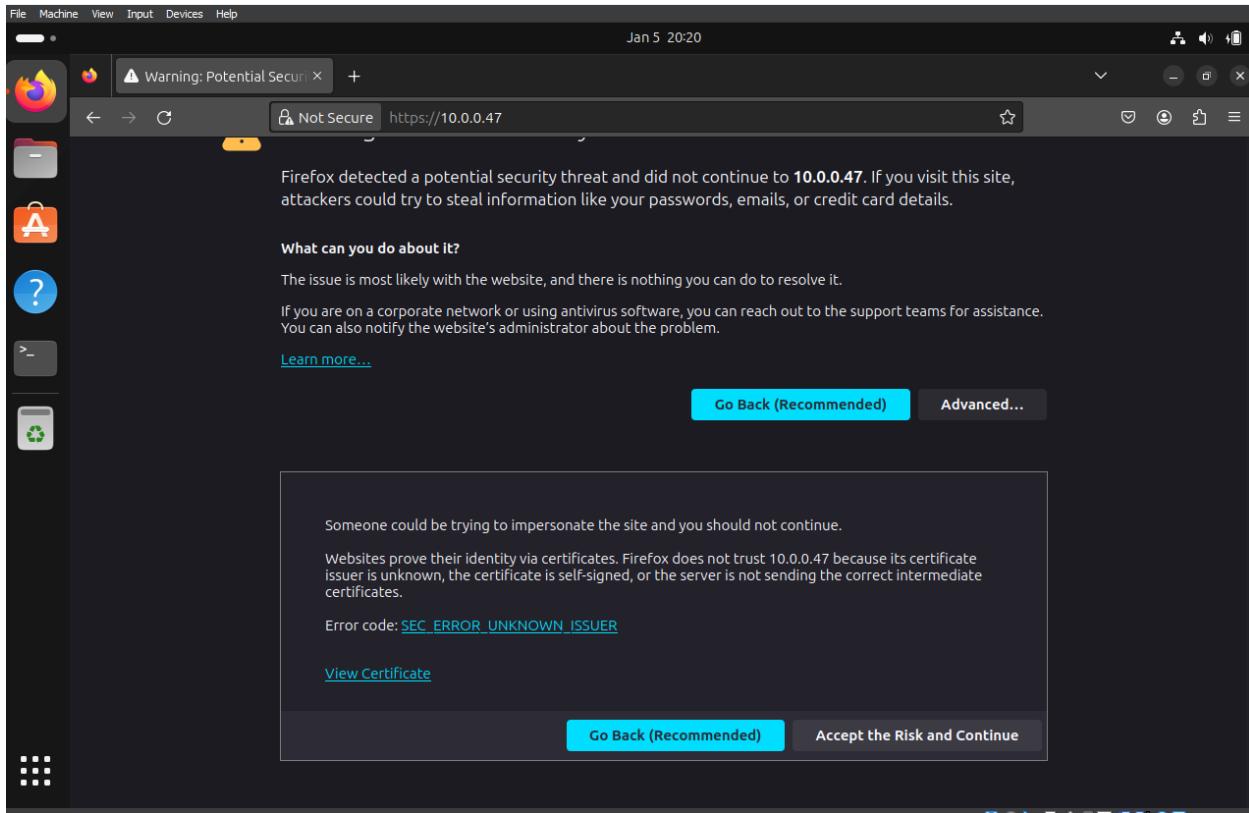
No packages needed for security; 3 packages available
Run "sudo yum update" to apply all updates.
[wazuh-user@wazuh-server ~]$ ifocnifg
-bash: ifocnifg: command not found
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.47 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::a00:27ff:fea: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 ~]$
```

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.

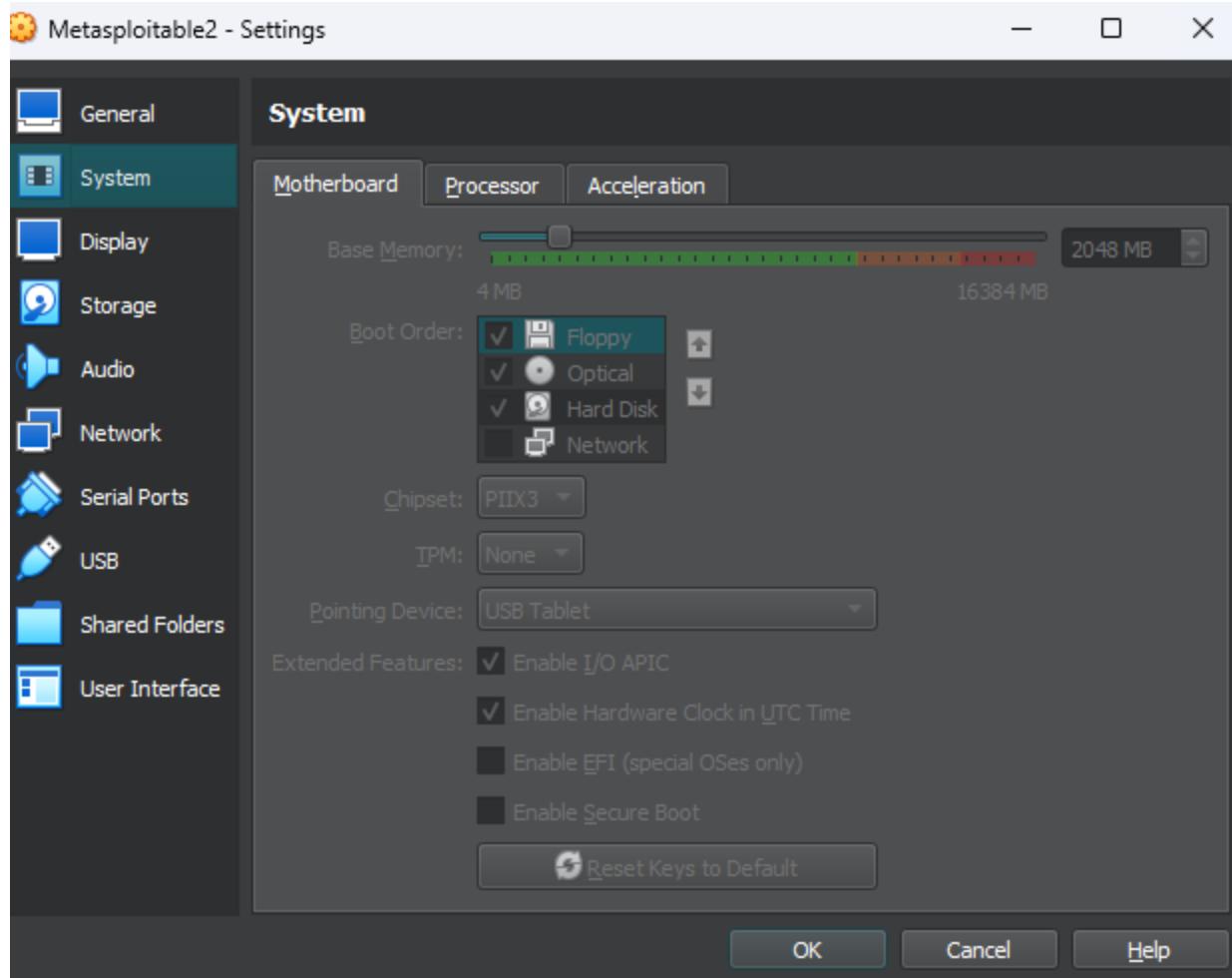
Installing Metasploitable2 is a pretty straightforward process. Just download the iso and install it in virtual box.

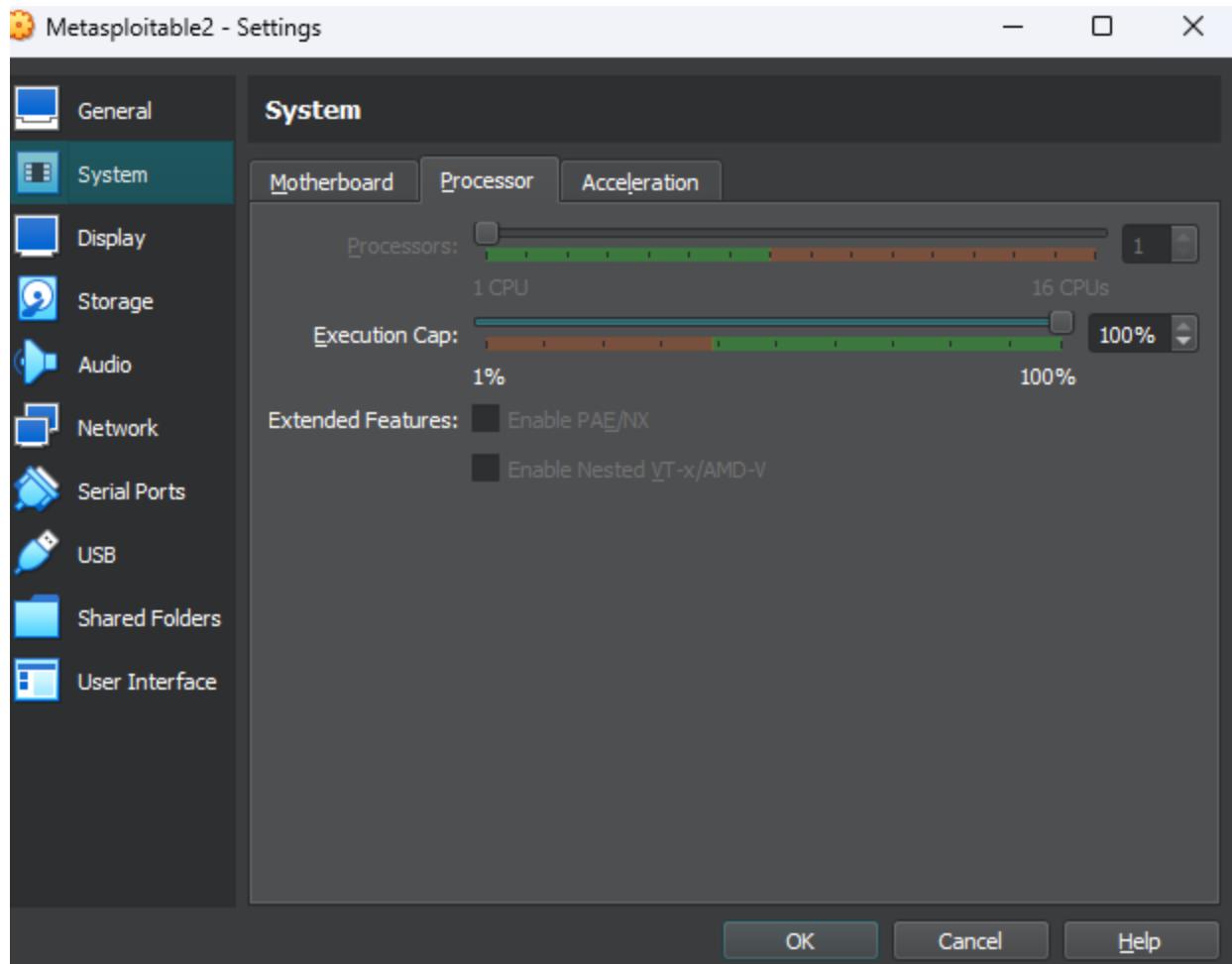
This is a video that helped me install it,

[YouTube: 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.

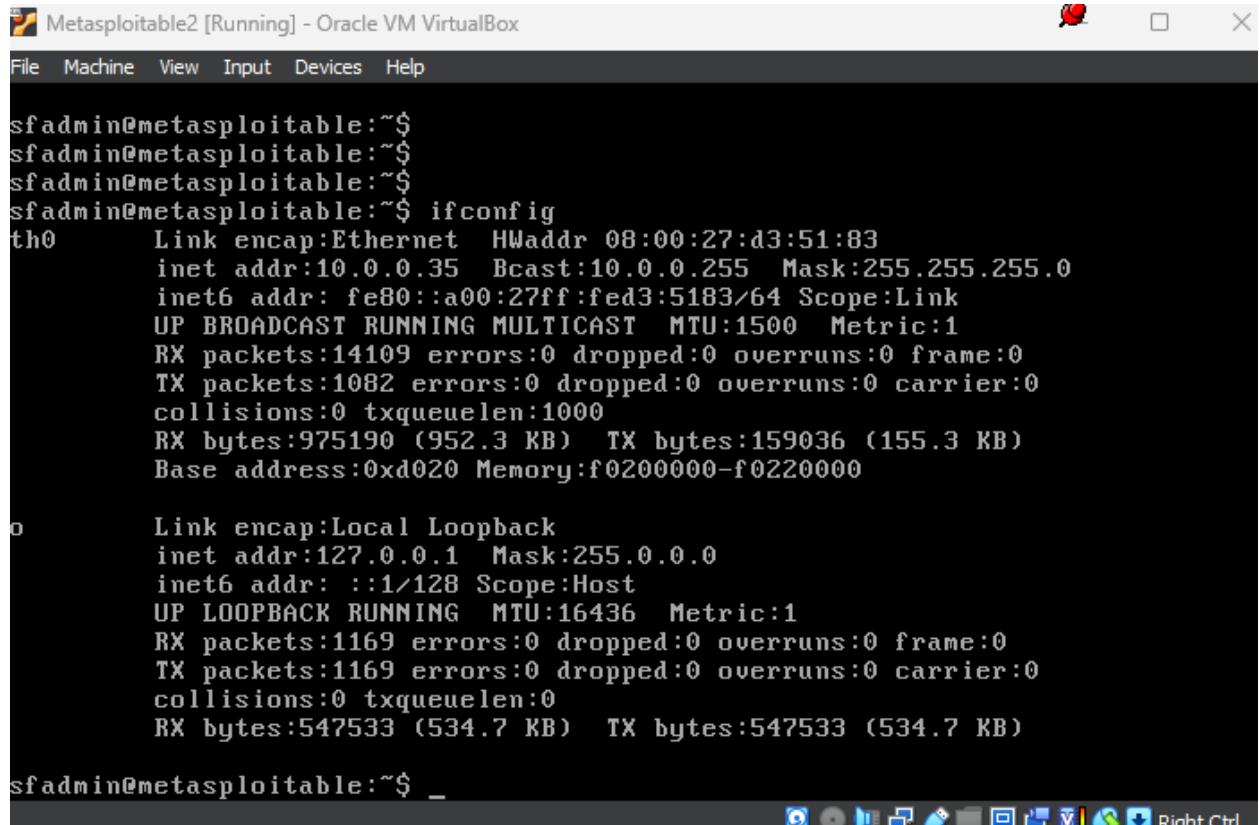
Really you just need it to be on the bridged network like all our other machines and give it 1 processor and 2GB ram.





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.



```
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)

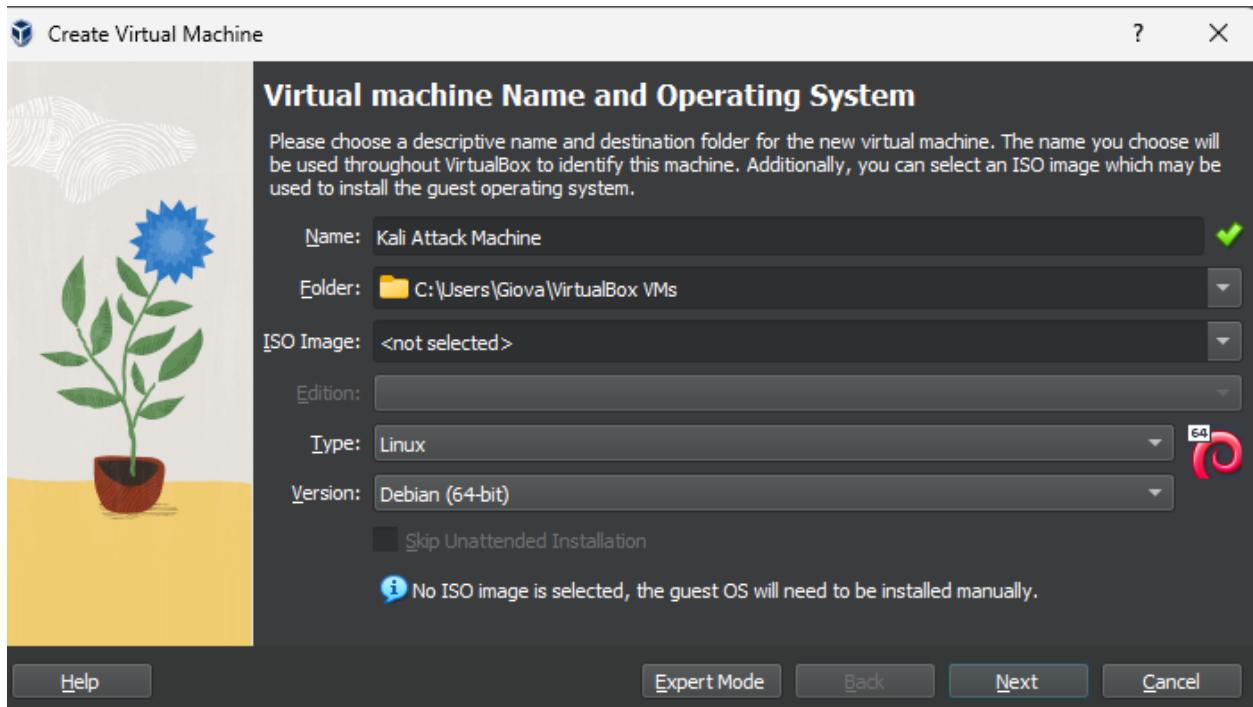
sfadmin@metasploitable:~$ _
```

On to the next installation.

Up next is our attack machine, Kali Linux.

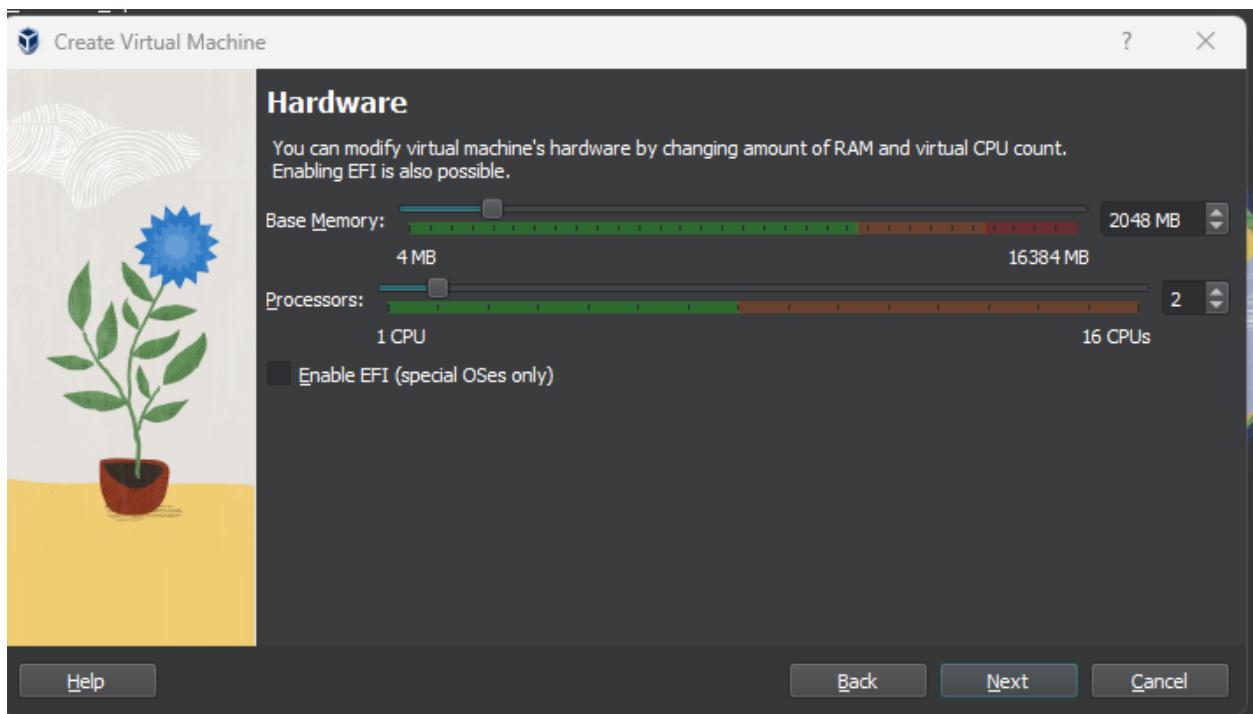
You can either download the prebuilt ova or the iso. In my example I am using the Virtual Hard Disk Drive.

We will not be assigning an iso.

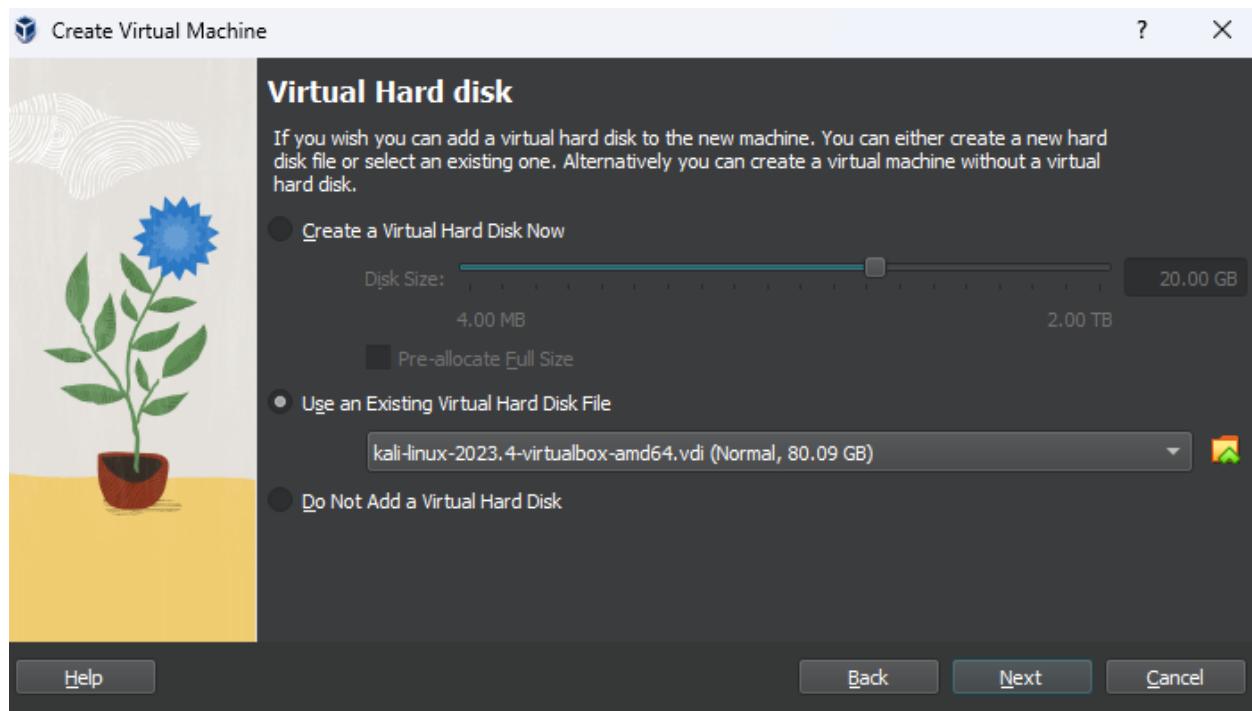


Click next

Give it 2 processors and 2GB ram. Click next

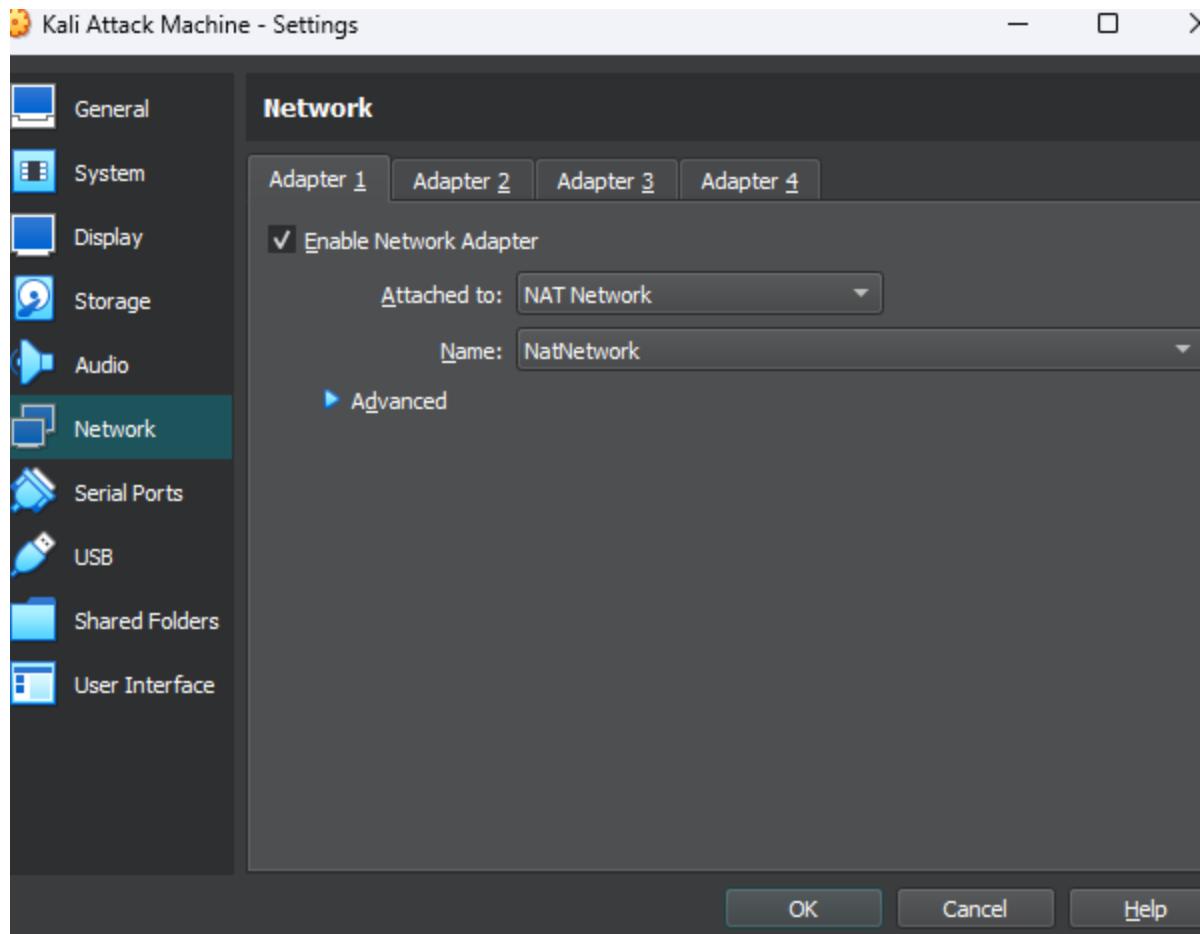


Click on use an existing virtual hard disk drive and look for the Kali vdi. It should have an orange cube icon.

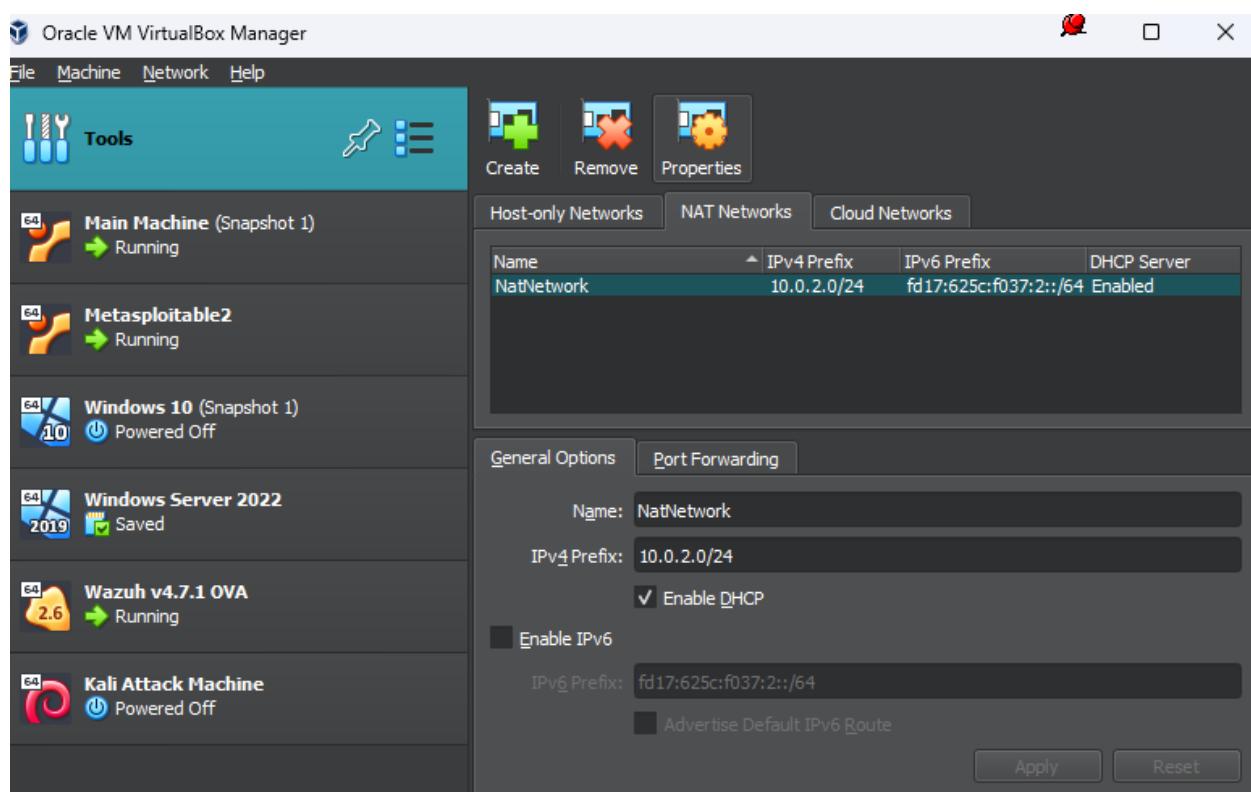


Click next and finish.

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



If you don't have a nat network to work with, simply go to the Virtual Box tools and go to network.

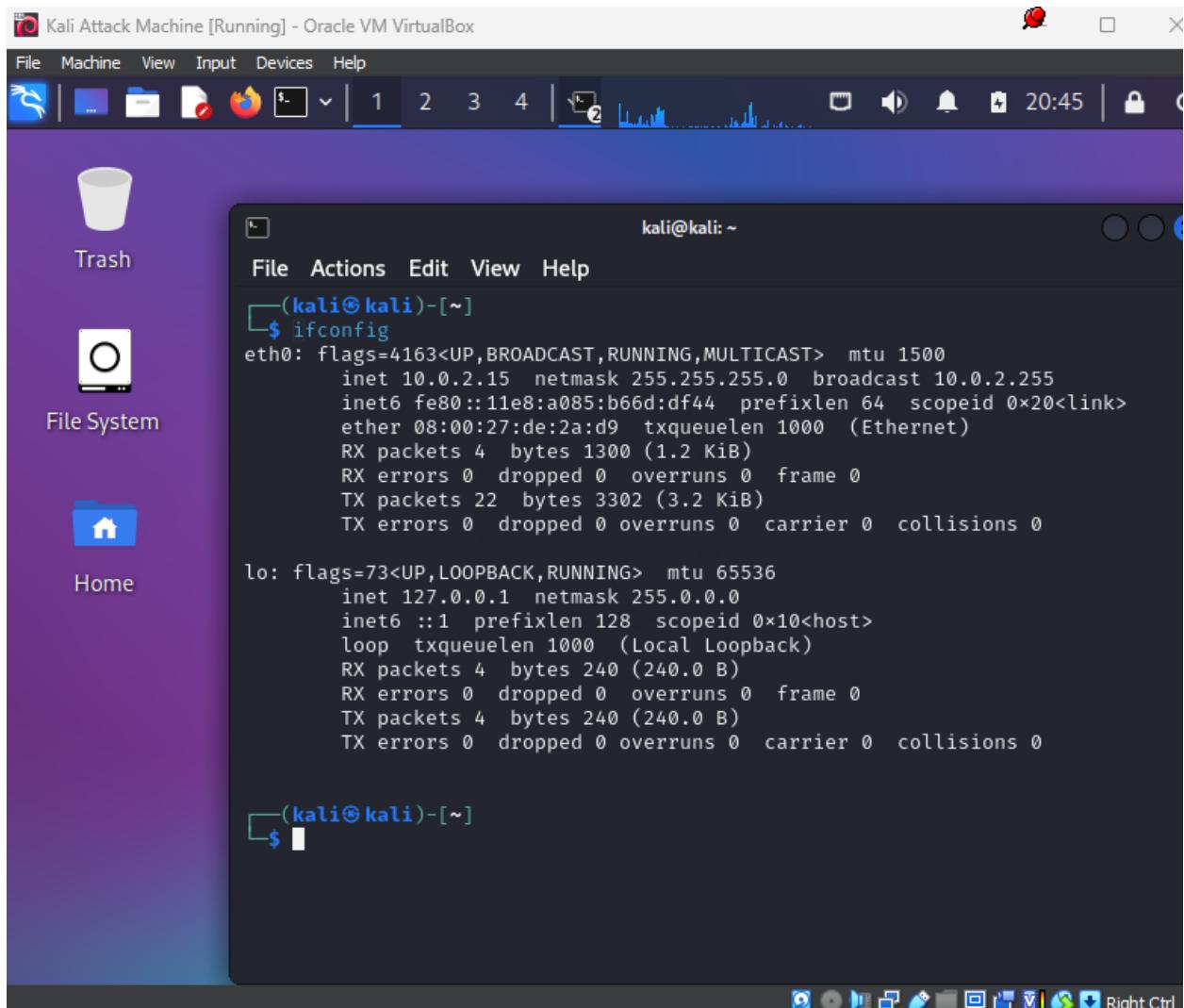


Click on create within the Nat Networks tab to create one, which will be used for our Kali Machine.

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!



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::11e8:a085:b66d:df44 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:de:2a:d9 txqueuelen 1000 (Ethernet)
            RX packets 4 bytes 1300 (1.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 22 bytes 3302 (3.2 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 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[(kali㉿kali)-[~]
$
```

Thats it.

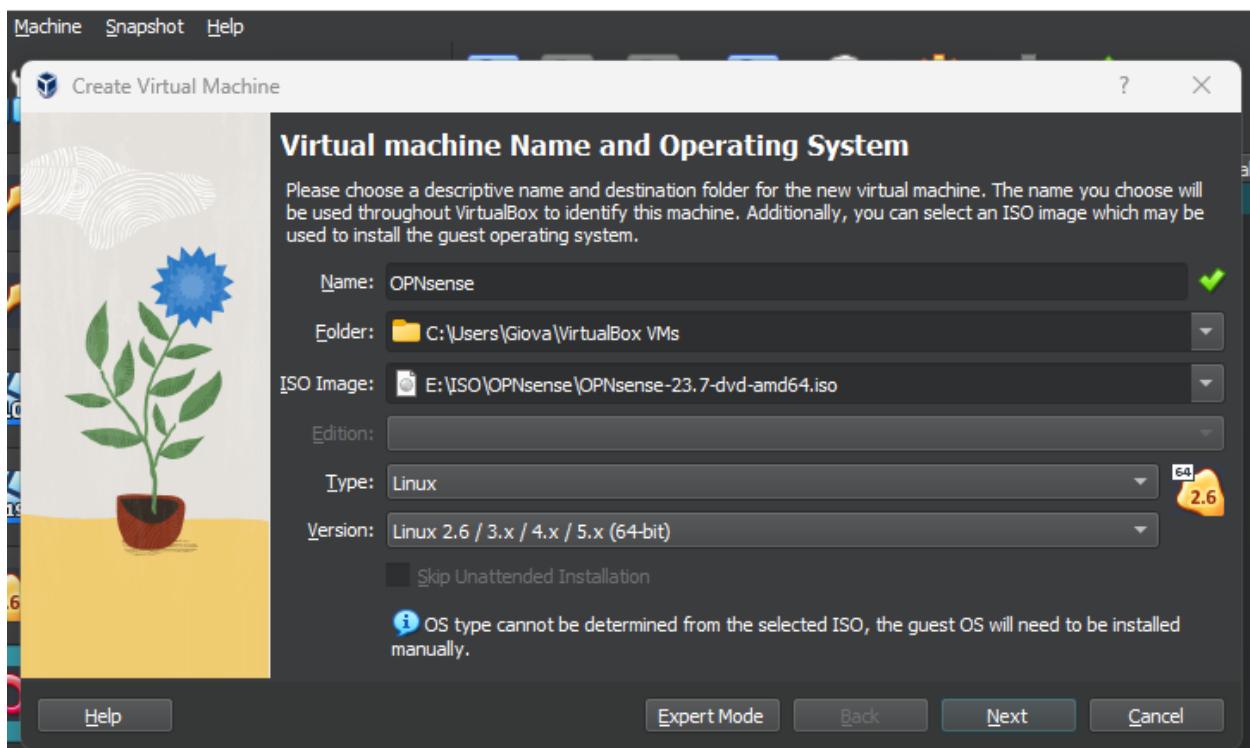
On to the next installation.

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.

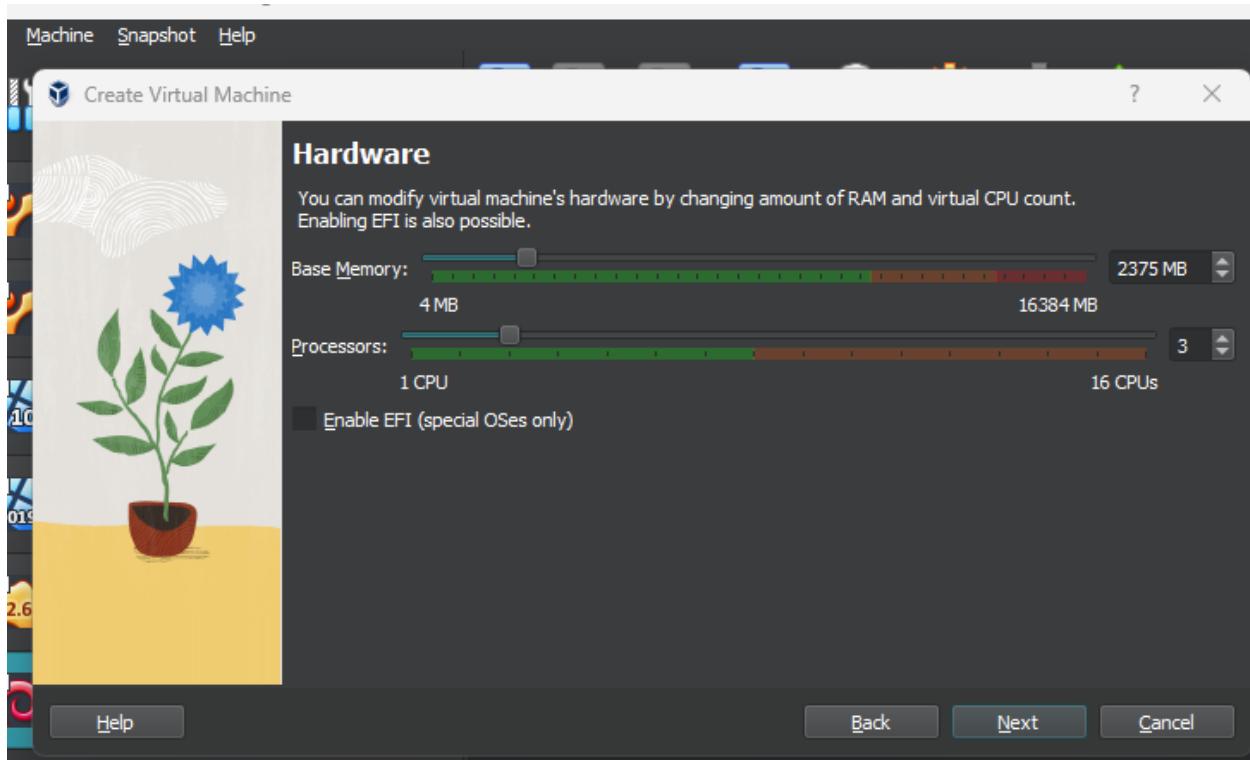
For opnsense we will need to download it from the official website.

This installation will be through iso.



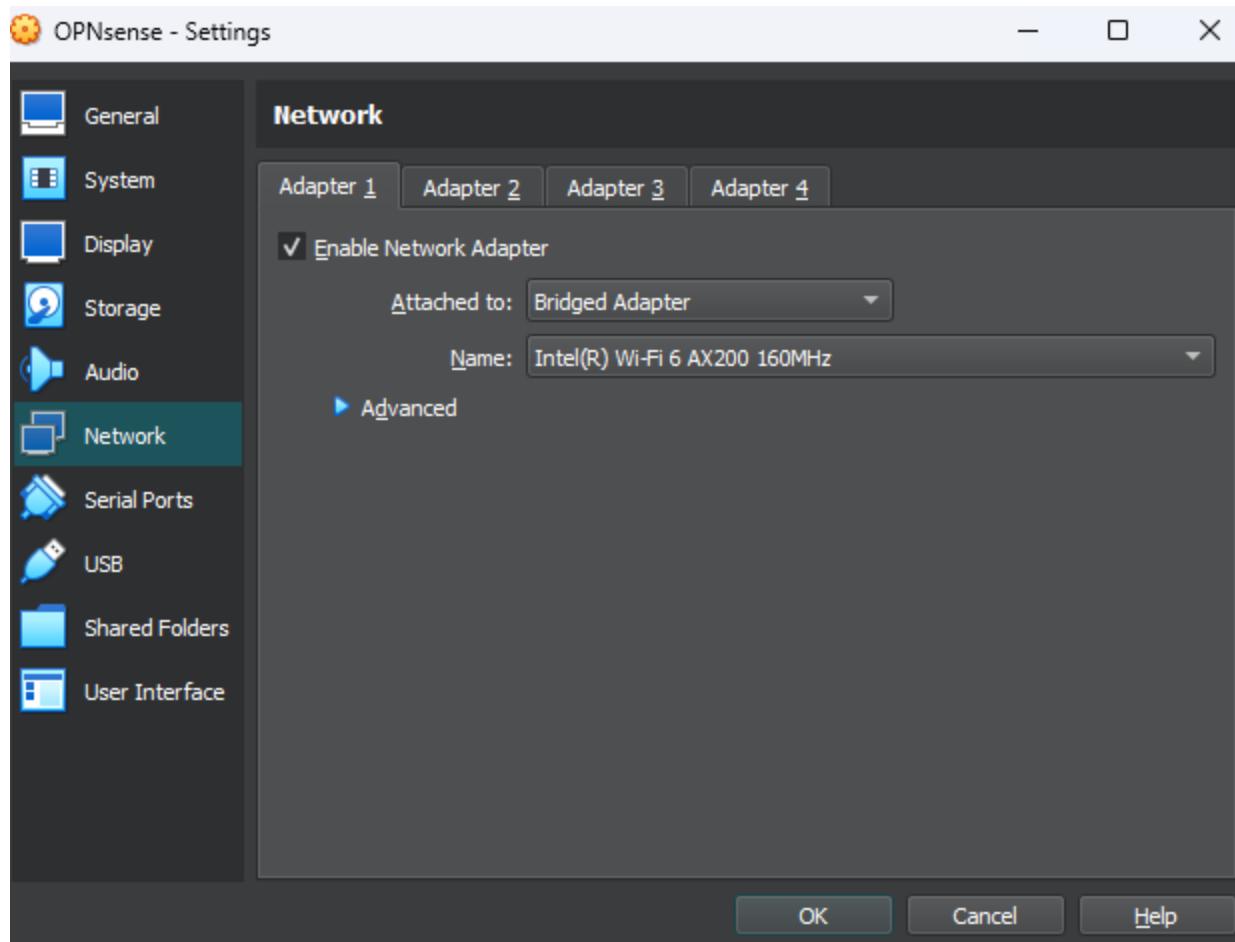
Click next

We will be 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'
service `sysctl' has been restarted.
>> Invoking start script 'beep'
root 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

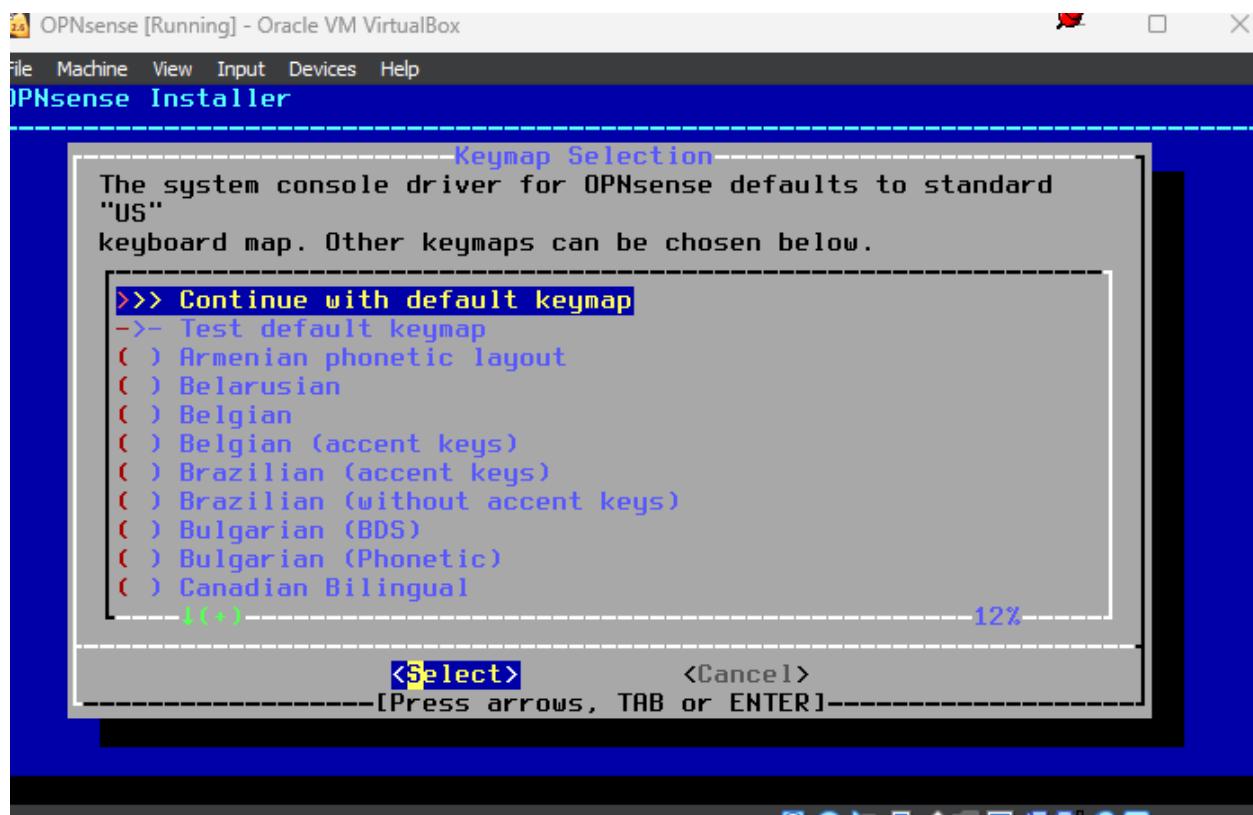
HTTPS: SHA256 A3 09 D0 D1 F4 06 FB 32 46 90 EF 0B 06 52 0A B8
       7A B7 09 AD F4 31 5D 38 BD C2 58 60 FE 6D A3 17
SSH:   SHA256 q7geuYp4XGuHnLWV1/dsXKnD/FT1ZiVW63btosJc42U (ECDSA)
SSH:   SHA256 047B1r6uoSFZ9pSySr+aFNPnvoQuq6QUbi+gD29Q4n8 (ED25519)
SSH:   SHA256 DJMMA0R6HiNLLt1PLYVqqorpK2RA0jimw3gRf0B8VjY (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

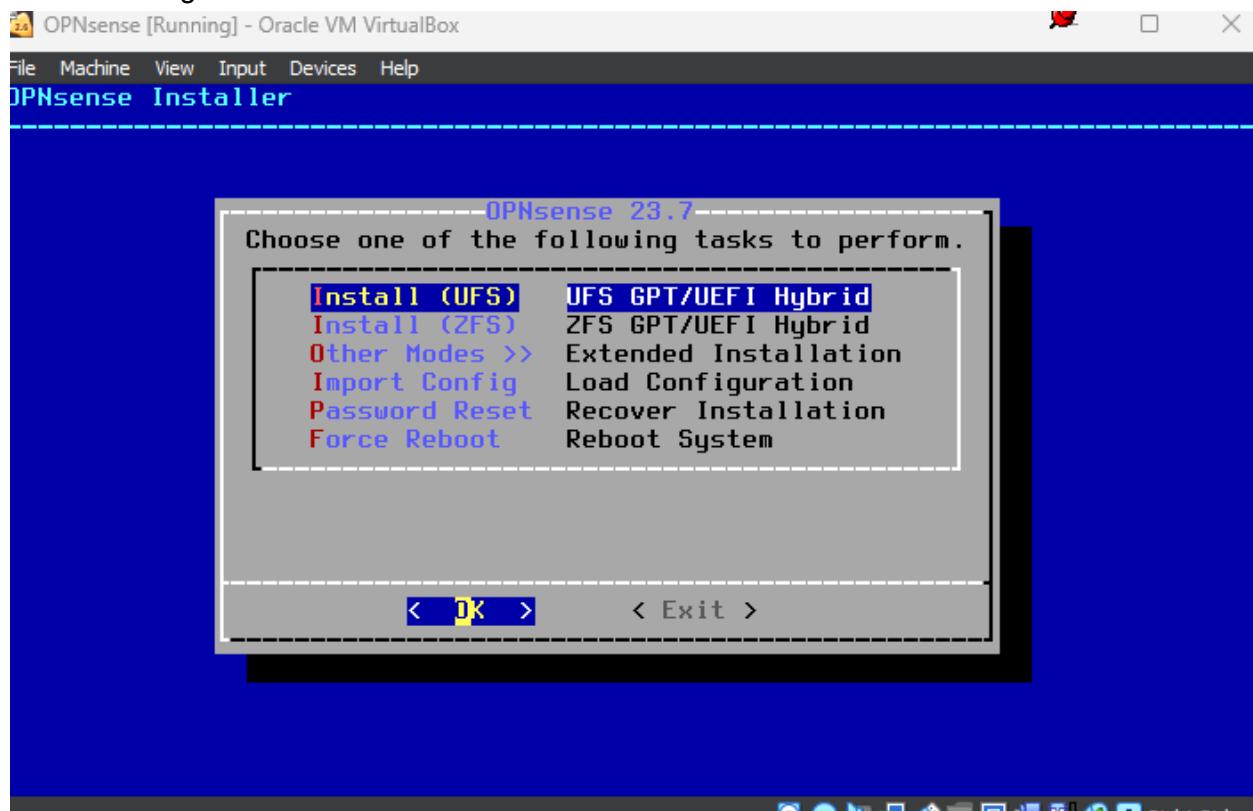
freeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: installer
password: [REDACTED]
```

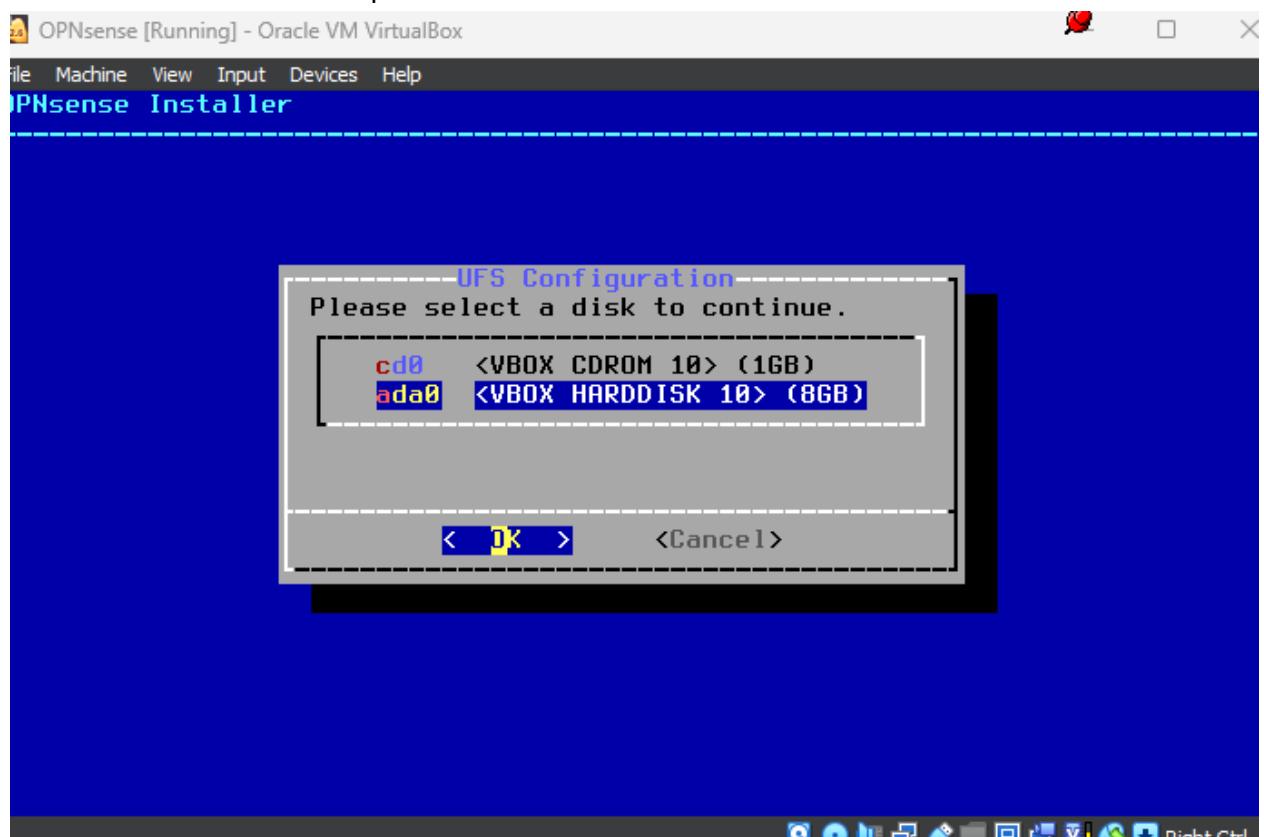
Press enter



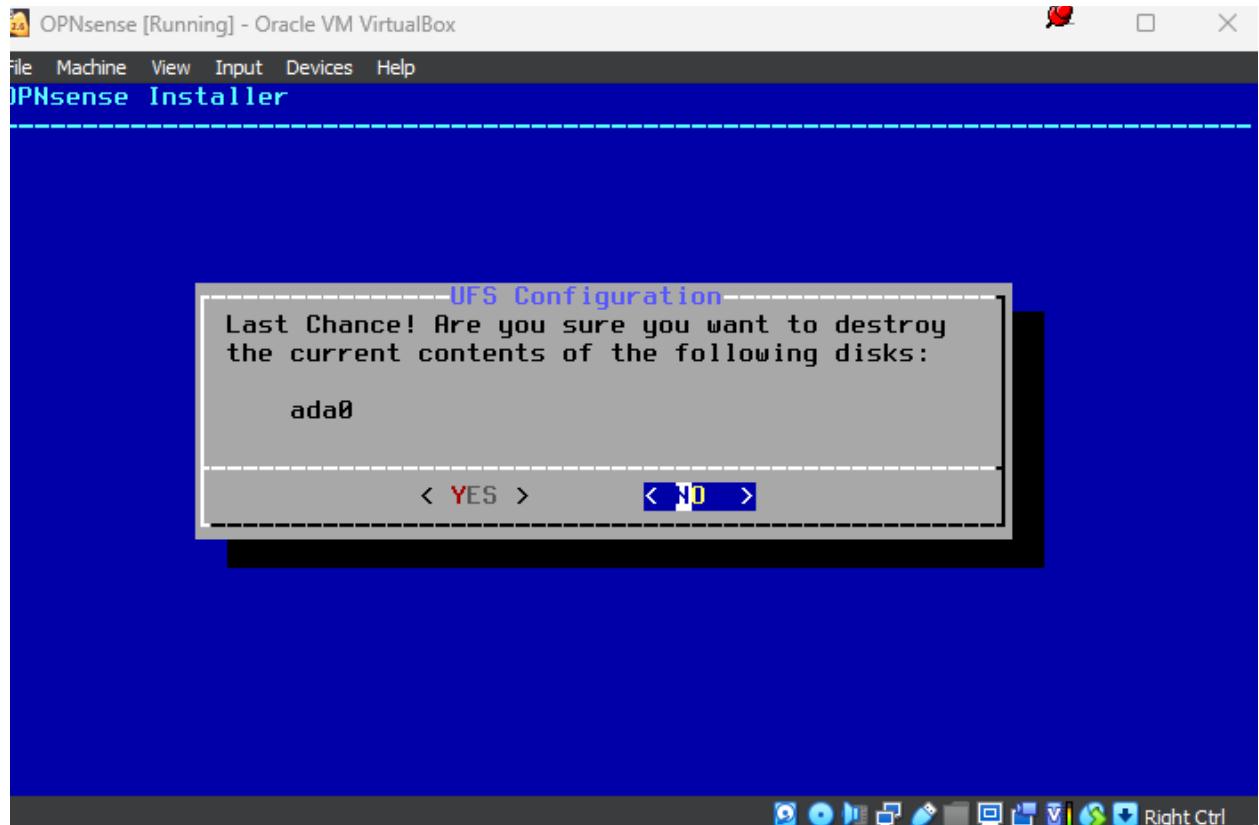
Press enter again.



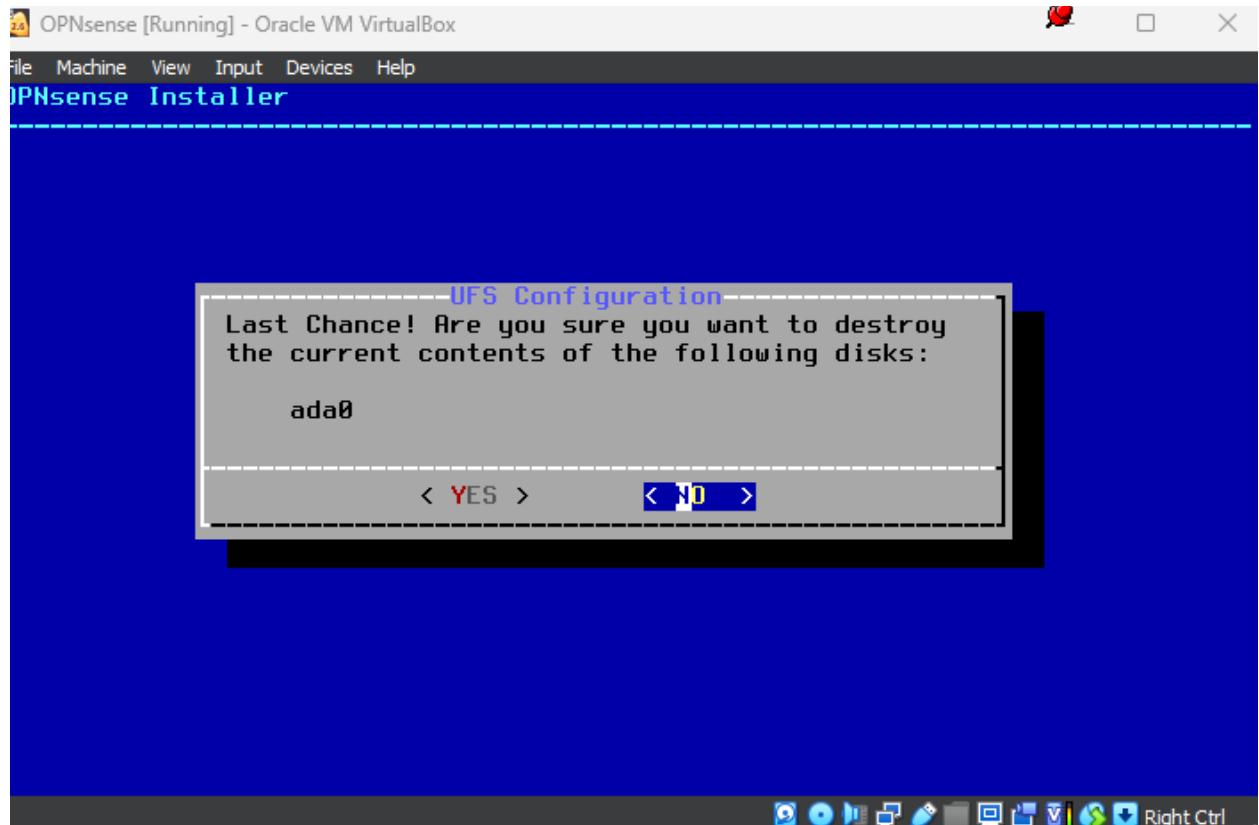
Press down arrow and then press enter.



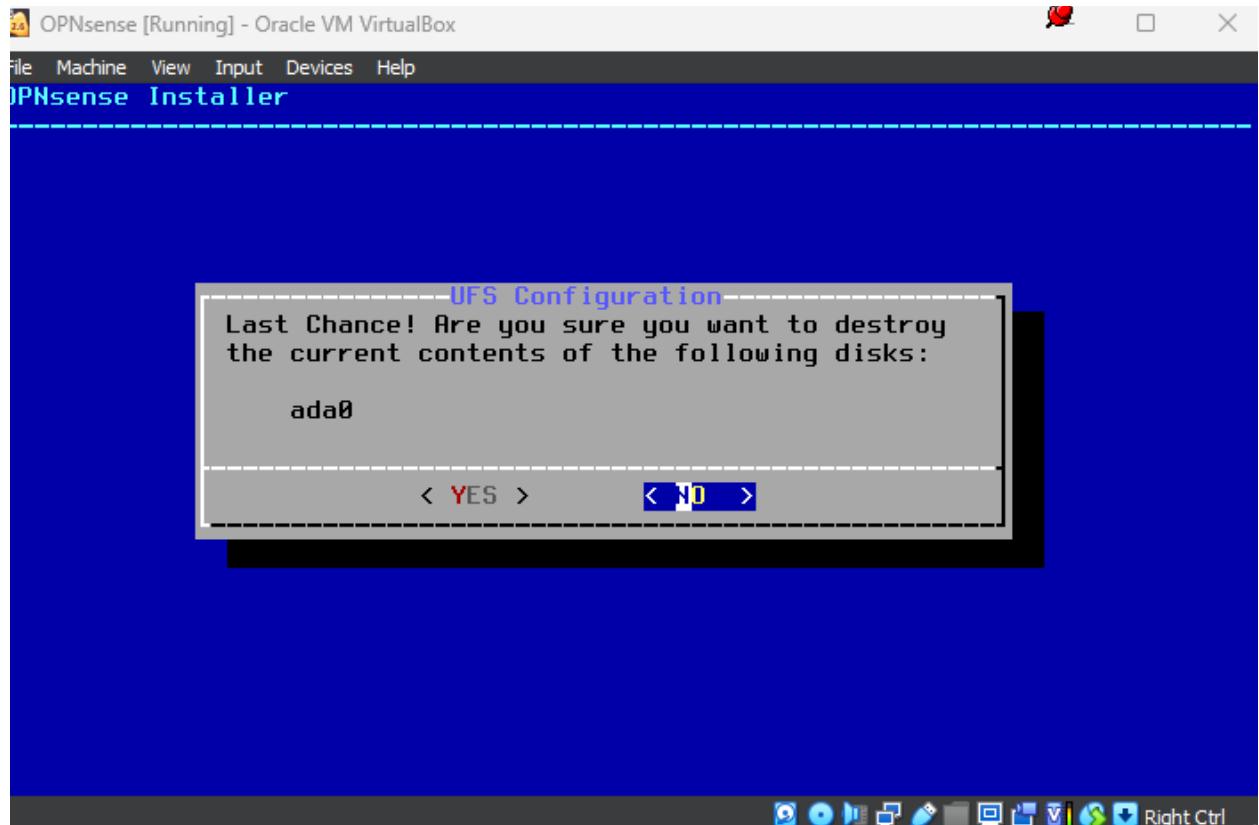
Right arrow and press enter



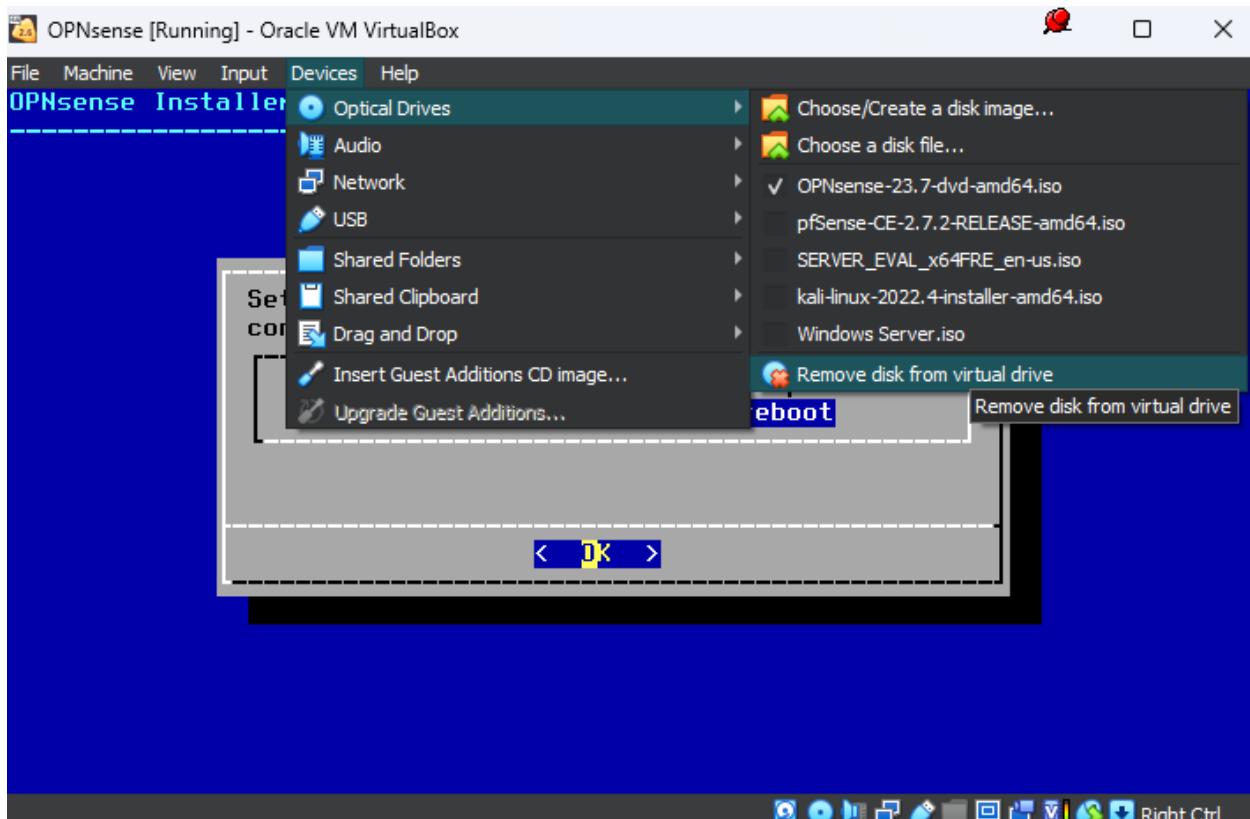
It should now be installing



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

```
File Machine View Input Devices Help
Starting Unbound DNS...done.
enerating RRD graphs...done.
>> Invoking start script 'newwanip'
>> Invoking start script 'freebsd'
>> Invoking start script 'syslog'
>> Invoking start script 'carp'
>> Invoking start script 'cron'
tarting Cron: OK
>> Invoking start script 'openvpn'
>> Invoking start script 'sysctl'
ervice `sysctl` has been restarted.
>> Invoking start script 'beep'
oot file system: /dev/gpt/rootfs
at Jan 6 02:07:12 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

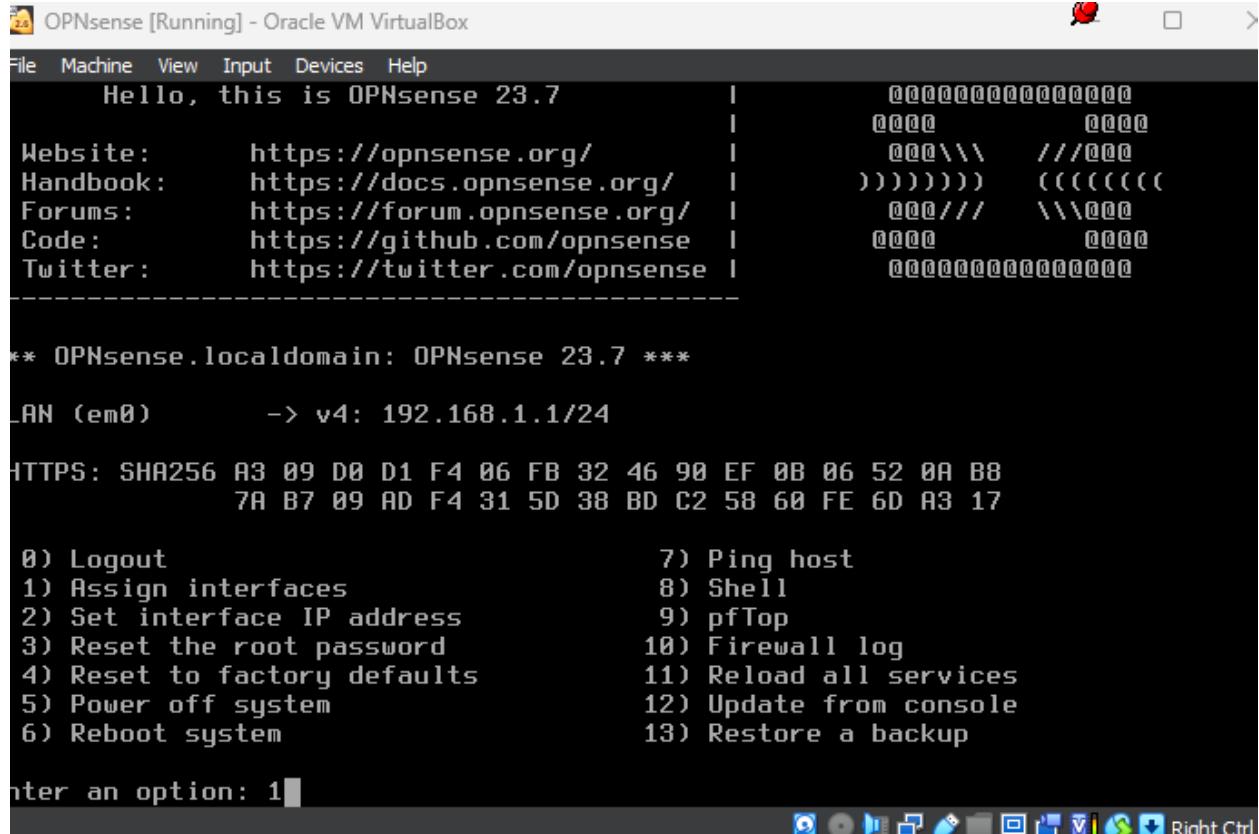
reeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: 
```

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.

OPNsense [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
Handbook: https://docs.opnsense.org/ | )))))))) ((((((
Forums: https://forum.opnsense.org/ | 000/// \\\000
Code: https://github.com/opnsense | 0000 0000
Twitter: https://twitter.com/opnsense | 0000000000000000

** 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

o you want to configure LAGGs now? [y/N]: n
o you want to configure VLANs now? [y/N]: n
```

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  
pressing 'a' to initiate auto detection.  
  
Enter the WAN interface name or 'a' for auto-detection: em0
```

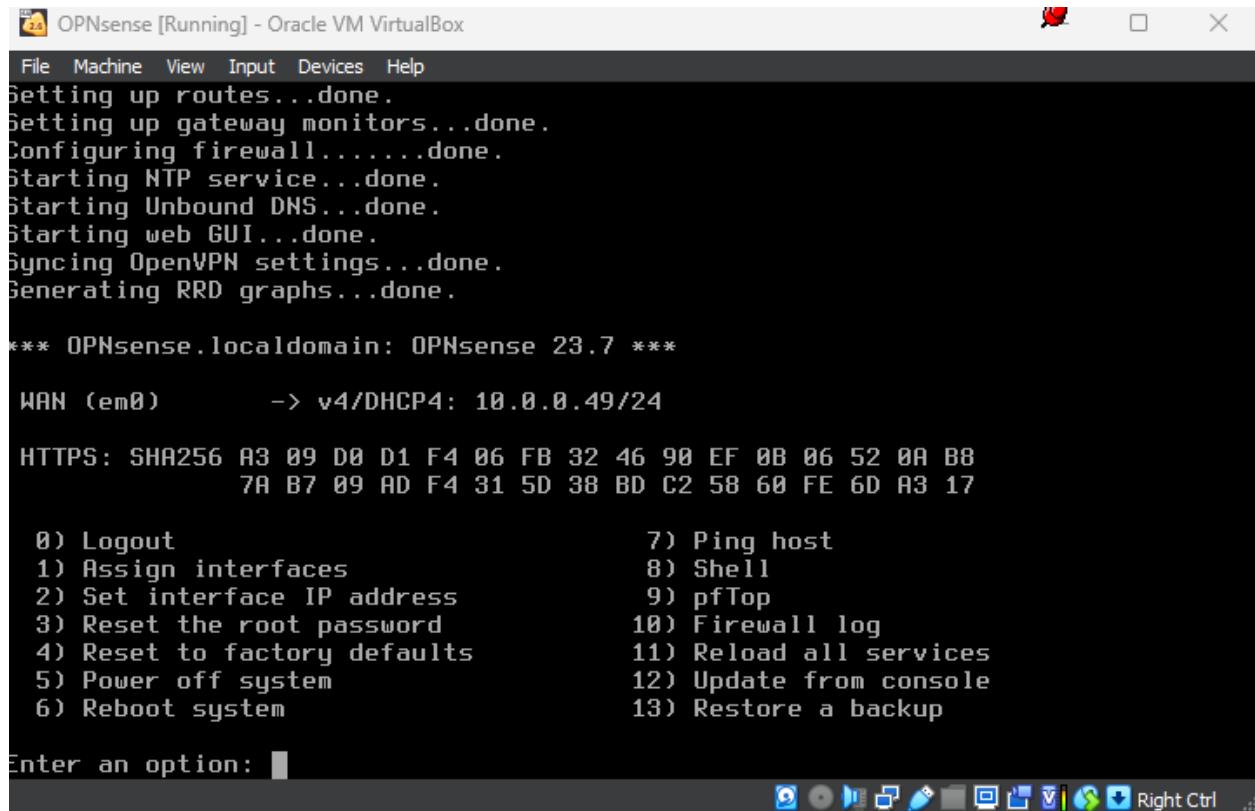
After pressing enter you will be prompted to enter more options. Ignore them as we only need our WAN.

```
OPNsense [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
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  
hitting 'a' to initiate auto detection.  
  
Enter the WAN interface name or 'a' for auto-detection: em0
```

Press y for yes

```
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]:
```

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



The screenshot shows a terminal window titled "OPNsense [Running] - Oracle VM VirtualBox". The window contains the following text:

```
File Machine View Input Devices Help
Setting up routes...done.
Setting 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

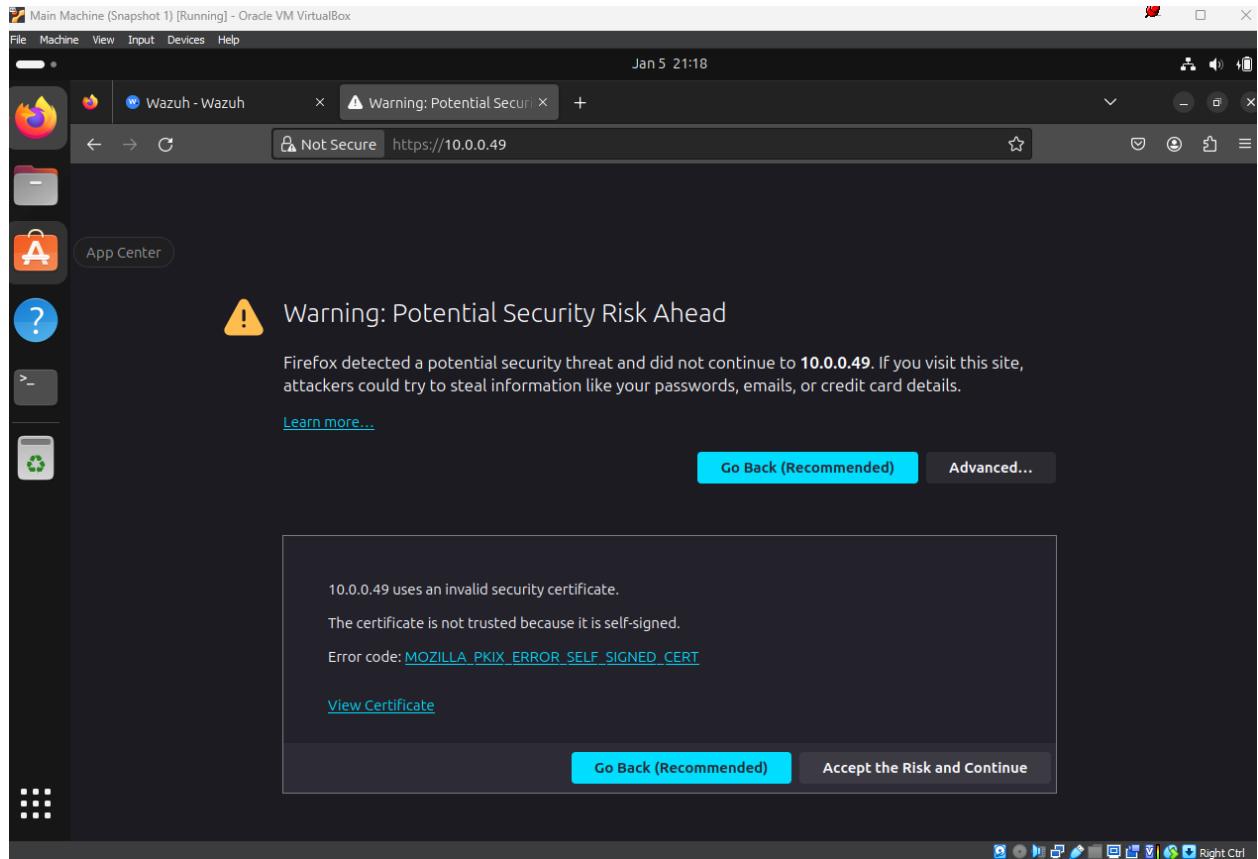
Enter an option: █
```

The terminal window has a standard Linux-style menu bar at the top. Below it, there's a list of system status messages, followed by the IP address assigned via DHCP. At the bottom, a numbered menu provides various administrative options. The prompt "Enter an option: █" is visible at the bottom left, and a set of icons is at the bottom right.

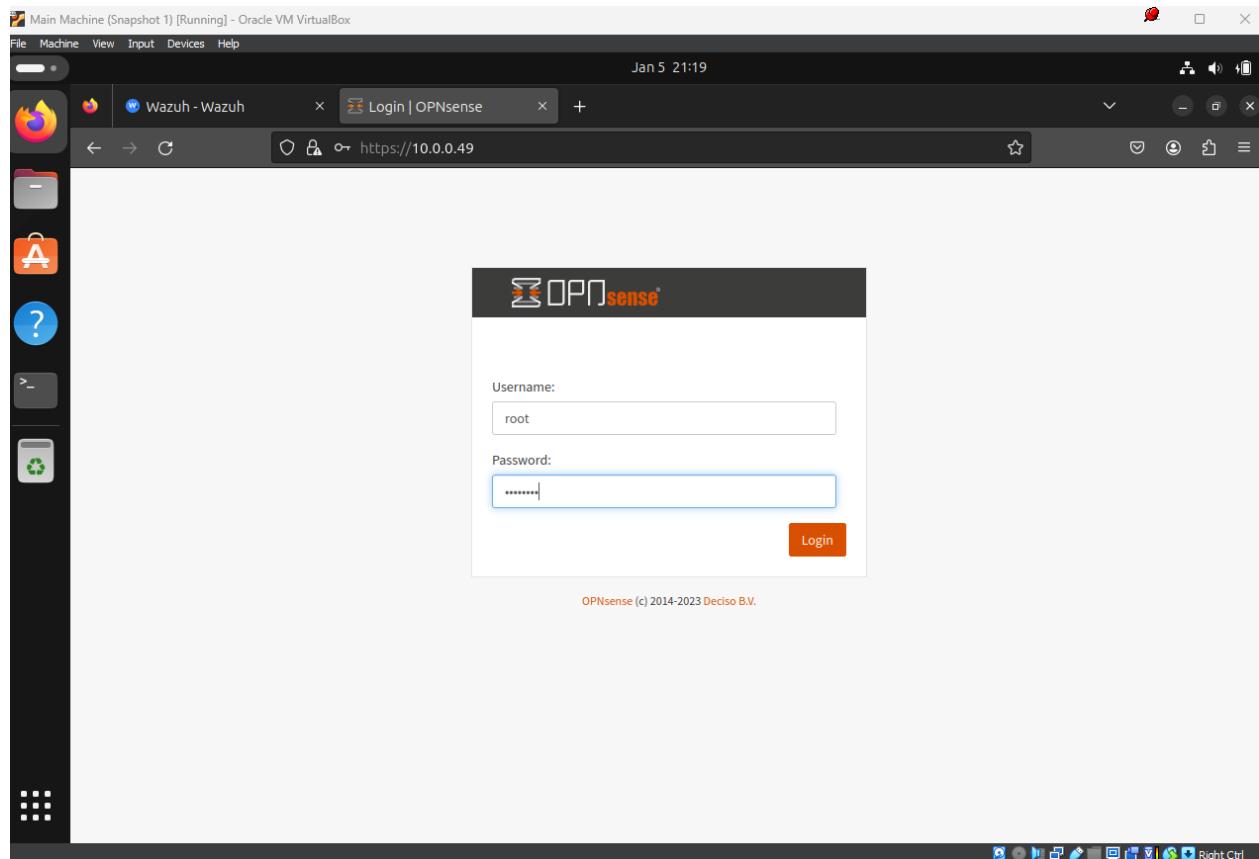
The next steps will now consist of having these machines interact with each other.

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

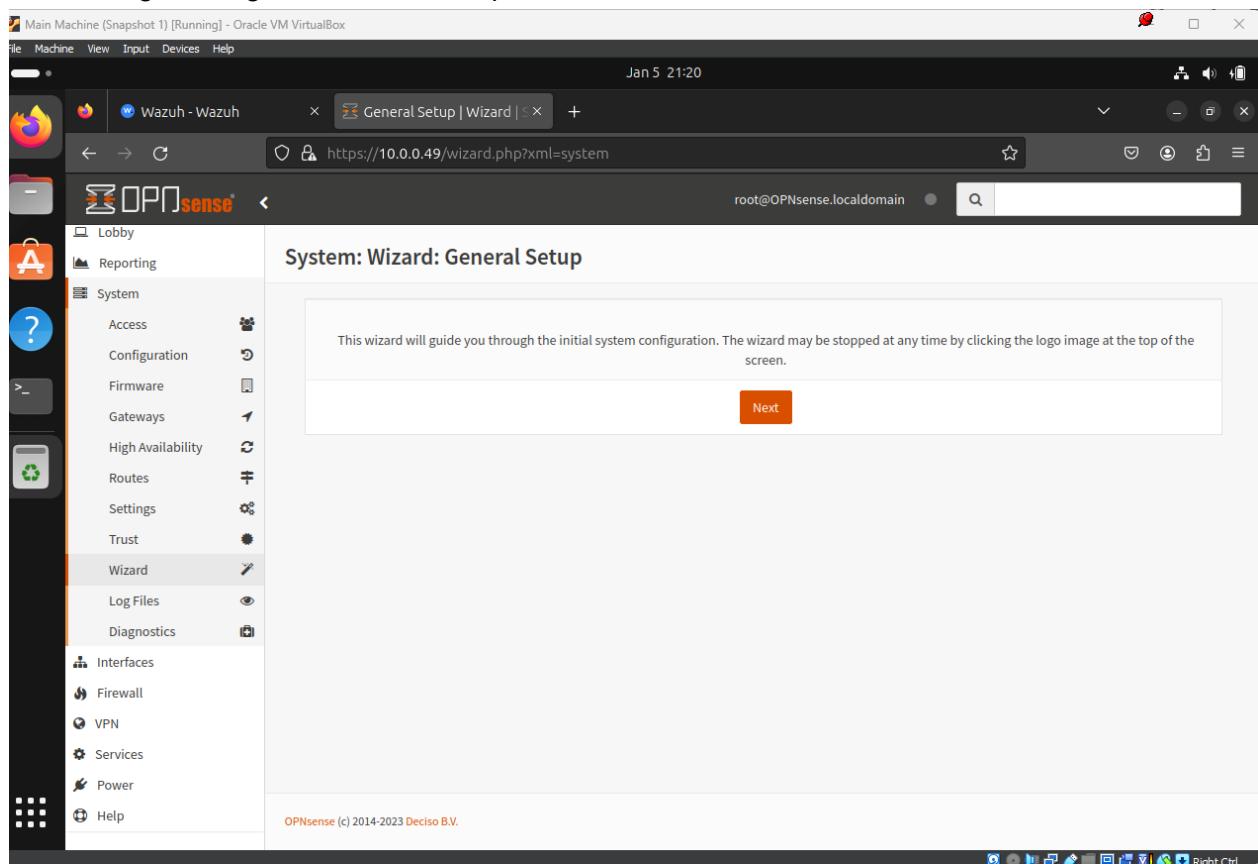
Just like Wazuh, click accept the risks and continue.



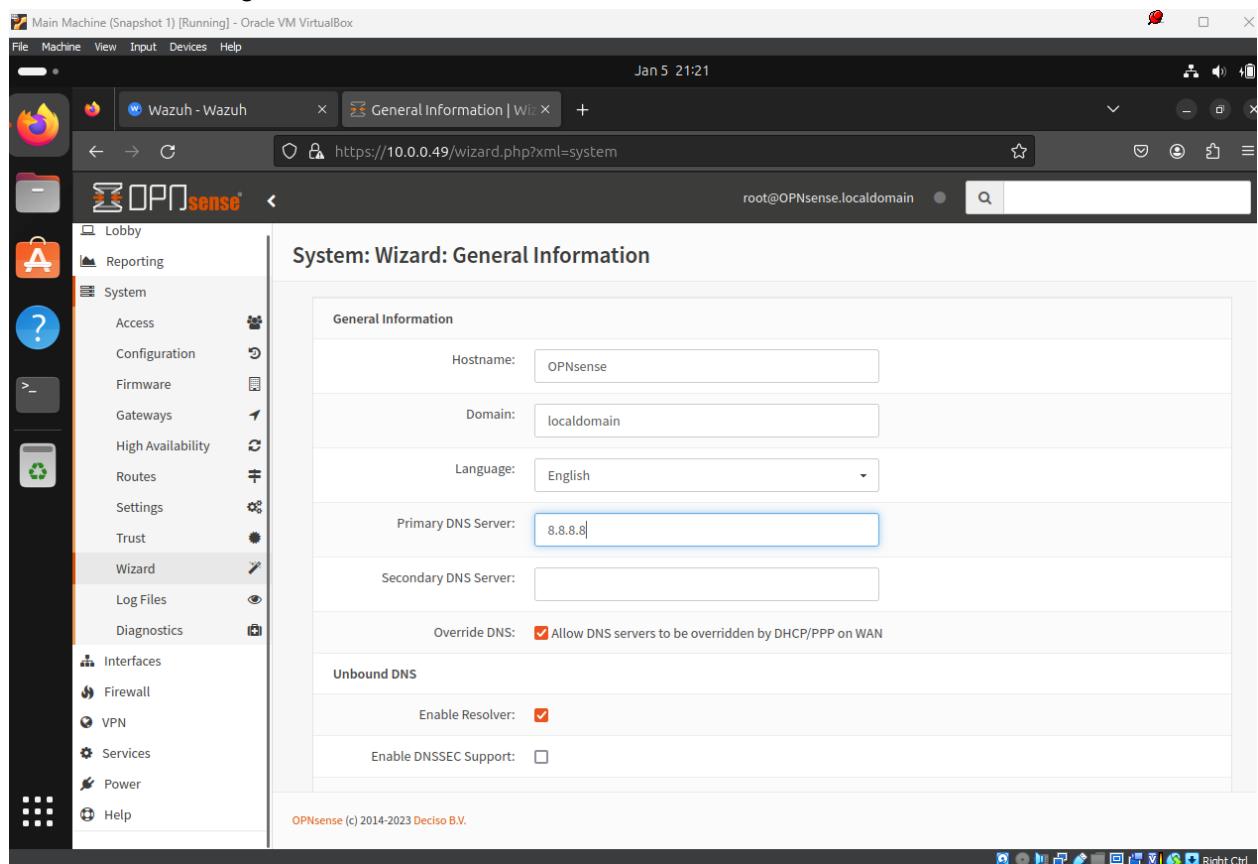
It will use the same password and username as the opnsense server



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



Follow these configurations. Then click next



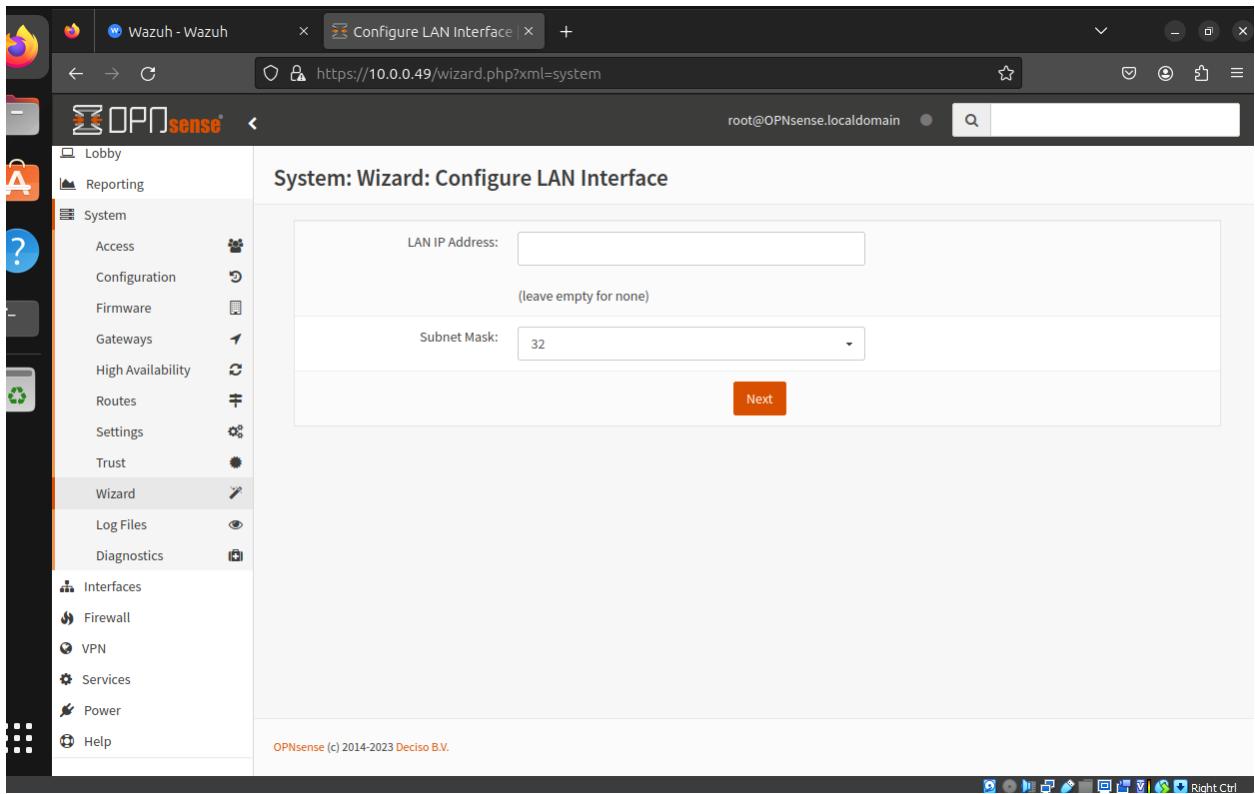
Click next again for time configuration.

We want to change it to static.

The screenshot shows a web browser window titled "Configure WAN Interface" from the URL <https://10.0.0.49/wizard.php?xml=system>. The browser title bar also displays "Wazuh - Wazuh". The page content is the "System: Wizard: Configure WAN Interface" section. On the left, there is a sidebar with various system management icons and links like "Lobby", "Reporting", "System", "Access", "Configuration", etc. The "Wizard" link in the sidebar is highlighted. The main form has a dropdown menu for "IPv4 Configuration Type" set to "Static". Below this, there are fields for "MAC Address" (empty), "MTU" (empty), and "MSS" (empty). A note for "MAC Address" says: "This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank." A note for "MTU" says: "Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed." A note for "MSS" says: "If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases." At the bottom of the form, it says "Static IP Configuration" and "OPNsense (c) 2014-2023 Deciso B.V."

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 your 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.

The screenshot shows the OPNsense web interface on a Linux desktop. The browser window is titled 'Dashboard | Lobby | OPN' and the URL is 'https://10.0.0.49/index.php'. The dashboard displays various system metrics and configuration sections.

Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 23.7-amd64 FreeBSD 13.2-RELEASE-p1 OpenSSL 1.1.1u 30 May 2023
Updates	Click to check for updates.
CPU type	AMD Ryzen 7 4800H with Radeon Graphics (3 cores, 3 threads)
CPU usage	100% (0%)
Load average	0.26, 0.24, 0.17
Uptime	00:21:28
Current date/time	Sat Jan 6 2:28:00 UTC 2024
Last config change	Sat Jan 6 2:27:00 UTC 2024
CPU usage	33%
State table size	0 % (15/233000)
MBUF usage	2 % (3556/145612)

Services

Service	Description
configd	System Configuration Daemon
cron	Cron
login	Users and Groups
ntpd	Network Time Daemon
pf	Packet Filter
routing	System routing
sysctl	System tunables
syslog-ng	Syslog-ng Daemon
unbound	Unbound DNS
webgui	Web GUI

Gateways

Name	RTT	RTTd	Loss	Status
WAN	1ms	1ms	0%	Green

OPNsense (c) 2014-2023 Deciso B.V.

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.

The screenshot shows the OPNsense web interface with the URL <https://10.0.0.49/ui/core/firmware#updates>. The left sidebar has a 'Trash' item selected. The main content area displays a table of updates:

	Package	Current Version	New Version	Action	Source
py39-tzdata	2023.3_1	2023.4	upgrade	OPNsense	
py39-ujson	5.8.0	5.9.0	upgrade	OPNsense	
py39-urllib3	1.26.16.1	1.26.18.1	upgrade	OPNsense	
py39-yaml	6.0	6.0.1	upgrade	OPNsense	
python39	3.9.17	3.9.18	upgrade	OPNsense	
readline	8.2.1	8.2.7	upgrade	OPNsense	
rrdtool	1.8.0_2	1.8.0_2	reinstall	OPNsense	
sqlite3	3.42.0,1	3.44.0_1,1	upgrade	OPNsense	
squid	5.9	6.6	upgrade	OPNsense	
squid-langpack	N/A	7.0.0.20230225	new	OPNsense	
strongswan	5.9.10_2	5.9.13	upgrade	OPNsense	
sudo	1.9.14p3	1.9.15p4	upgrade	OPNsense	
suricata	6.0.13_1	6.0.15	upgrade	OPNsense	
syslog-ng	4.2.0	4.4.0	upgrade	OPNsense	
unbound	1.17.1_3	1.19.0	upgrade	OPNsense	
wpa_supplicant	2.10_6	2.10_10	upgrade	OPNsense	

At the bottom, there are two buttons: a blue 'Update' button and a white 'Cancel' button. A message box states: "There are 102 updates available, total download size is 238.5MB. This update requires a reboot."

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 below.

The screenshot shows a web browser window titled "Firmware | System | OPNsense" with the URL <https://10.0.0.49/ui/core/firmware#plugins>. The page displays the "System: Firmware" section. On the left, a sidebar menu is open under the "Help" category, listing various system management options like Reporting, System, Access, Firmware, Status, Settings, Changelog, Updates, Plugins, Packages, Reporter, Log File, Gateways, High Availability, Routes, Settings, Trust, Wizard, Log Files, and Diagnostics. The main content area has tabs for Status, Settings, Changelog, Updates, Plugins, and Packages, with "Updates" selected. A table lists the "wazuh" plugin, showing its version as 1.0, size as 38.4KiB, tier as 3, repository as OPNsense, and comment as "Agent for the open source security platform Wazuh". A plus icon (+) is visible in the bottom right corner of the table row. At the bottom of the page, a footer note reads "OPNsense (c) 2014-2024 Deciso B.V."

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

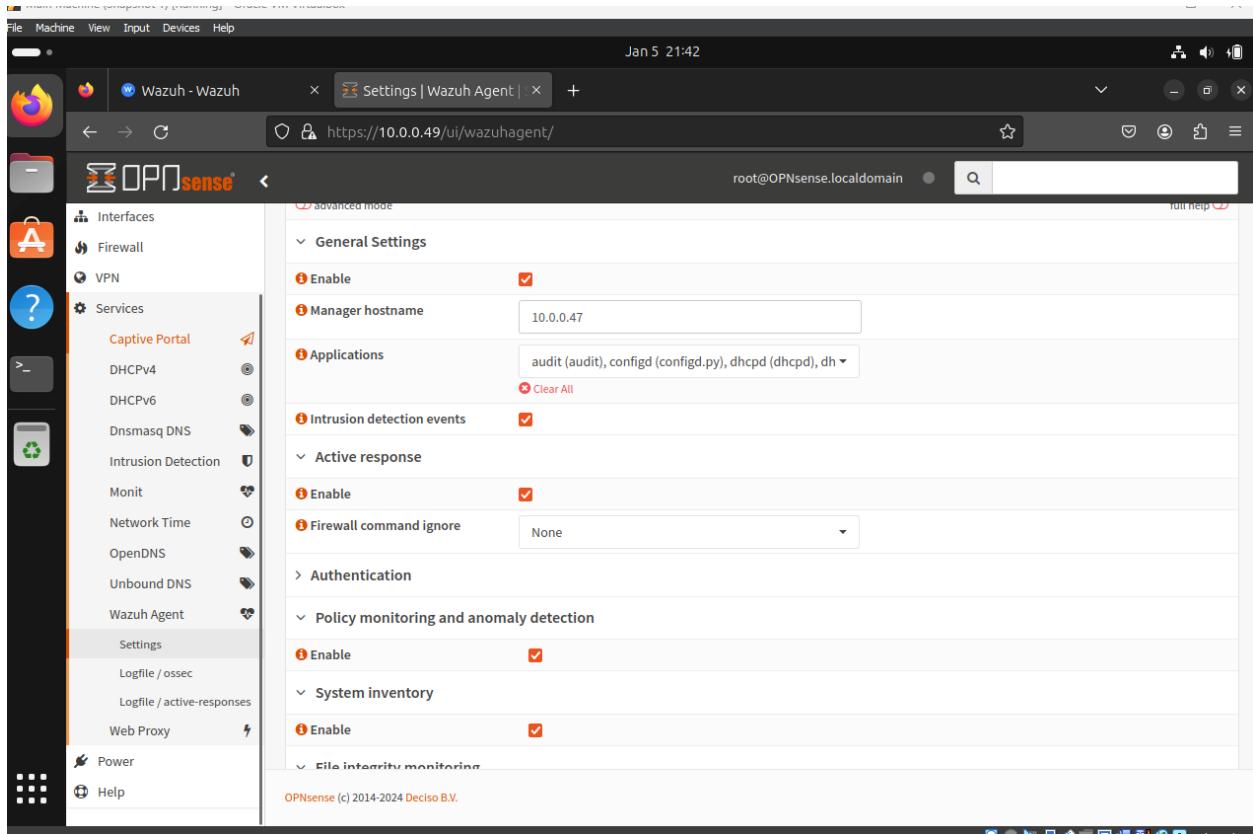
The screenshot shows a web browser window titled "Firmware | System | OPN" with the URL <https://10.0.0.49/ui/core/firmware#updates>. The page is titled "System: Firmware". On the left, there is a sidebar with various system management links: Reporting, System (Access, Configuration, Firmware), Firmware (Status, Settings, Changelog, Updates, Plugins, Packages), Reporter, Log File, Gateways, High Availability, Routes, Settings, Trust, Wizard, Log Files, and Diagnostics. The "Firmware" link under the System section is currently selected. The main content area has tabs for Status, Settings, Changelog, Updates (which is active), Plugins, and Packages. The "Updates" tab contains a numbered list of steps:

- 4) You can find additional useful files installed at
/var/ossec/packages_files/agent_installation_scripts
- 5) Add Wazuh agent to /etc/rc.conf
sysrc wazuh_agent_enable="YES"
or
service wazuh-agent enable
- 6) Start Wazuh agent
service wazuh-agent start
- 7) Enjoy it ;)
Checking integrity... done (0 conflicting)
Nothing to do.
DONE

At the bottom of the content area, there is a note: "Output shown here for diagnostic purposes. There is no general need for manual system intervention. [Click here to copy to clipboard.](#)".

Now 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!

The screenshot shows a browser window titled "Wazuh - Wazuh" with the URL [https://10.0.0.47/app/wazuh#/agents-preview/?_g=\(filters:!\(\),refreshInterval:\(pause:1,value:0\),time:\(from:now-24h,to:now\)\)](https://10.0.0.47/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:1,value:0),time:(from:now-24h,to:now))). The page displays the following information:

- STATUS:** A large teal circle indicating 1 Active agent.
- DETAILS:** Agents coverage is 100.00%. Last registered agent: OPNsense.localdomain. Most active agent: OPNsense.localdomain.
- EVOLUTION:** A line chart showing the count of events over the last 24 hours, with a single point at 1.0.
- Agents (1):** A table listing the single agent: ID 001, Name OPNsense.localdomain, IP address 10.0.0.49, Group(s) default, Operating system BSD 13.2, Cluster node node01, Version v4.7.1, Status active.

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.

The screenshot shows a web browser window titled "Administration | Intrusion" with the URL <https://10.0.0.49/ui/ids>. The browser is running on an OPNsense system, as indicated by the logo in the address bar. The page displays the "Services: Intrusion Detection: Administration" configuration. On the left, a sidebar lists various services: Interfaces, Firewall, VPN, Services (selected), Captive Portal, DHCPv4, DHCPv6, Unbound DNS, Wazuh Agent, Web Proxy, Power, and Help. The "Intrusion Detection" service is also listed under Services. The main content area has tabs for Settings (selected), Download, Rules, User defined, Alerts, and Schedule. Under Settings, there are several configuration options:

- Enabled: A checkbox is unchecked.
- IPS mode: A checkbox is unchecked.
- Promiscuous mode: A checkbox is unchecked.
- Enable syslog alerts: A checkbox is unchecked.
- Enable eve syslog output: A checkbox is unchecked.
- Pattern matcher: A dropdown menu set to "Aho-Corasick".
- Interfaces: A dropdown menu set to "WAN".
- Rotate log: A dropdown menu set to "Weekly".
- Save logs: An input field containing the value "4".

An "Apply" button is located at the bottom of the settings section. The footer of the page includes the text "OPNsense (c) 2014-2024 Deciso B.V." and a series of small icons.

Now follow these configurations.

The screenshot shows the OPNsense web interface with the URL <https://10.0.0.49/ui/ids>. The left sidebar contains navigation links for various services like Interfaces, Firewall, VPN, Services, and Intrusion Detection. The main content area is titled "Services: Intrusion Detection: Administration". It has tabs for Settings, Download, Rules, User defined, Alerts, and Schedule. Under Settings, several options are checked: Enabled, IPS mode, Promiscuous mode, Enable syslog alerts, and Enable eve syslog output. Other settings include Pattern matcher (Hyperscan), Interfaces (WAN), Rotate log (Weekly), and Save logs (4). An "Apply" button is at the bottom. The footer credits OPNsense (c) 2014-2024 Deciso B.V.

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.

Description	Last updated	Enabled	Edit
abuse.ch/Feodo Tracker	not installed	✗	<input type="button" value="Edit"/>
abuse.ch/SSL Fingerprint Blacklist	not installed	✗	<input type="button" value="Edit"/>
abuse.ch/SSL IP Blacklist	not installed	✗	<input type="button" value="Edit"/>
abuse.ch/ThreatFox	not installed	✗	<input type="button" value="Edit"/>
abuse.ch/URLhaus	not installed	✗	<input type="button" value="Edit"/>
ET open/botcc	not installed	✗	<input type="button" value="Edit"/>
ET open/botcc.portgrouped	not installed	✗	<input type="button" value="Edit"/>
ET open/ciarmy	not installed	✗	<input type="button" value="Edit"/>
ET open/compromised	not installed	✗	<input type="button" value="Edit"/>
ET open/drop	not installed	✗	<input type="button" value="Edit"/>
ET open/dshield	not installed	✗	<input type="button" value="Edit"/>

Then click download and update rules

Description	Last updated	Enabled	Edit
ET open/ciarmy	not installed	✓	<input type="button" value="Edit"/>
ET open/compromised	not installed	✓	<input type="button" value="Edit"/>
ET open/drop	not installed	✓	<input type="button" value="Edit"/>
ET open/dshield	not installed	✓	<input type="button" value="Edit"/>

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!

The screenshot shows the OPNsense Administration interface with the 'Intrusion' tab selected. The left sidebar has 'Services' expanded, with 'Intrusion Detection' selected. The main area displays a table of intrusion detection rules. The columns are: sid, Action, Source, ClassType, Message, and Info / Enabled. The table lists 16 rules, with the last one (sid 2000016) having 'Alert' and 'Drop' checked under 'Action'. The message for this rule is 'ET P2P Phatbot Control C...'. A checkbox at the bottom of the table is also checked. The footer shows 'OPNsense (c) 2014-2024 Deciso B.V.'

sid	Action	Source	ClassType	Message	Info / Enabled
2000005	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Cisco Telnet B...	<input type="checkbox"/>
2000006	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco Router HTTP...	<input type="checkbox"/>
2000007	alert	emerging-exploit.rules	attempted-dos	ET EXPLOIT Catalyst SSH p...	<input type="checkbox"/>
2000009	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HT...	<input type="checkbox"/>
2000010	alert	emerging-dos.rules	attempted-dos	ET DOS Cisco 514 UDP flo...	<input type="checkbox"/>
2000011	alert	emerging-dos.rules	attempted-dos	ET DOS Catalyst memory l...	<input type="checkbox"/>
2000012	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco %u IDS ...	<input type="checkbox"/>
2000013	alert	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HT...	<input type="checkbox"/>
2000015	alert	emerging-p2p.rules	trojan-activity	ET P2P Phatbot Control C...	<input checked="" type="checkbox"/>
2000016	Alert Drop	emerging-deleted.rules	attempted-dos	ET DELETED SSL Bomb Do...	<input type="checkbox"/>

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.

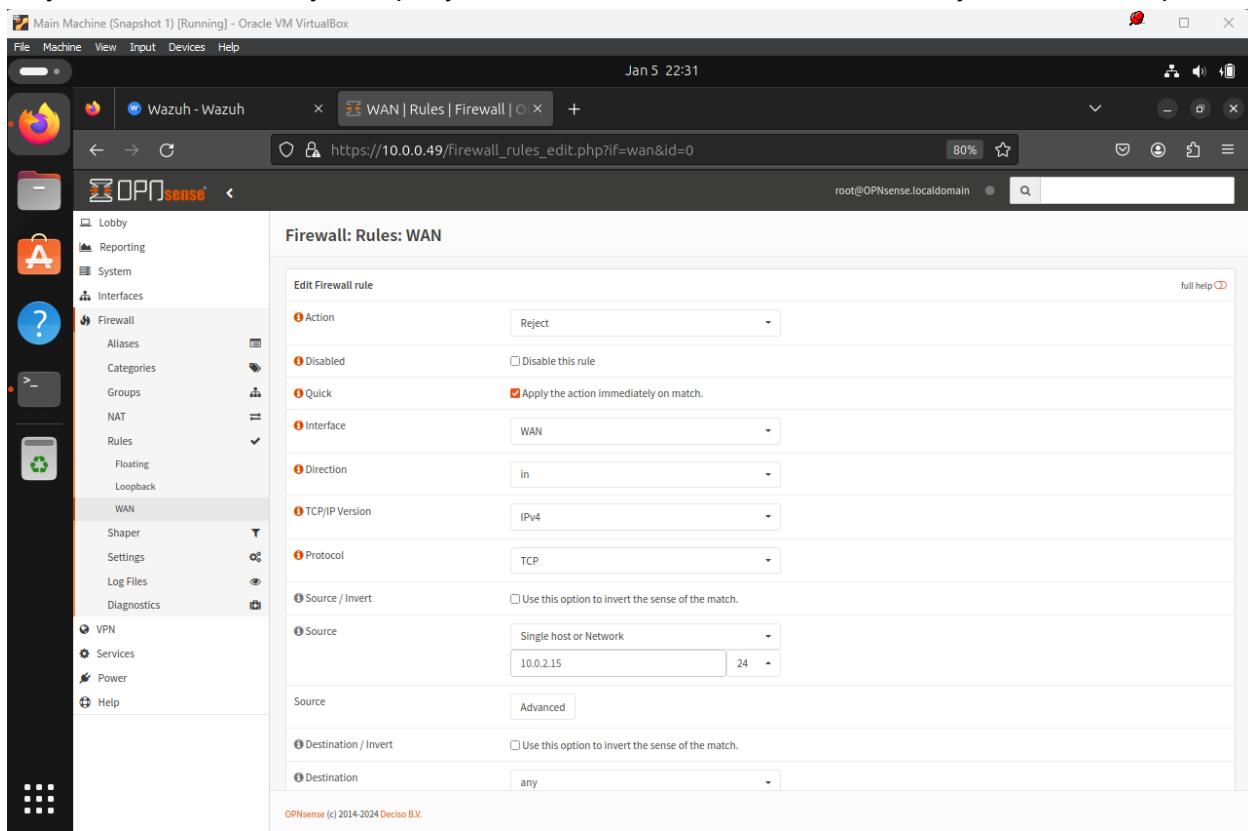
The screenshot shows the OPNsense web interface. The left sidebar has a dark theme with orange icons. The 'Wazuh - Wazuh' tab is open in the top bar. The main content area is titled 'Firewall: Rules: WAN'. A table lists firewall rules:

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action Buttons
	IPv4 TCP	10.0.2.15/24	*	*	*	*	*	Kali Rule	+ Add Edit Delete Check Uncheck
	pass	x block	x reject	log	→ in	first match			
	pass (disabled)	x block (disabled)	x reject (disabled)	log (disabled)	← out	last match			

Below the table, a note states: "WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default."

At the bottom, it says "OPNsense (c) 2014-2024 Deciso B.V." and shows a toolbar with various icons.

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



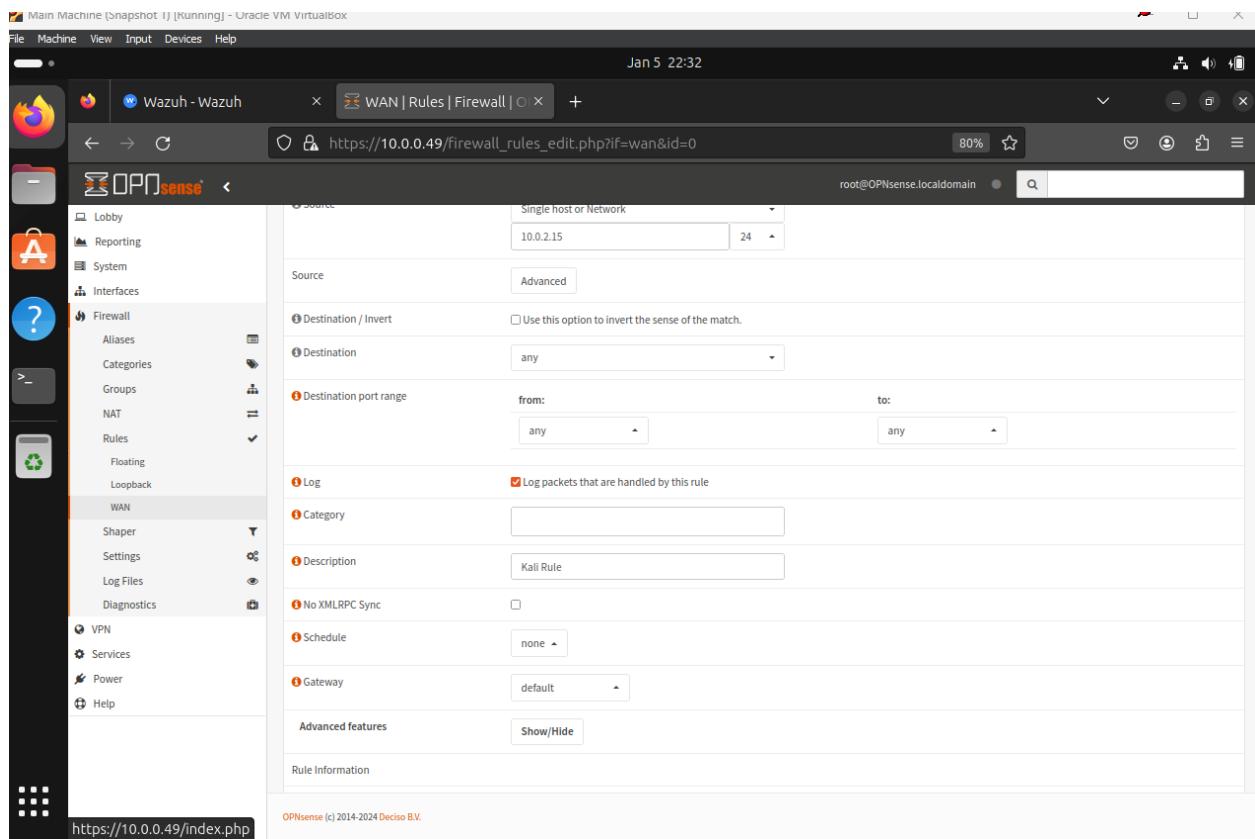
The screenshot shows the OPNsense web interface for managing firewall rules. The left sidebar has a 'WAN' section selected under 'Firewall'. The main content area is titled 'Firewall: Rules: WAN' and shows a form for editing a rule:

- Action:** Reject
- Disabled:** Disable this rule
- Quick:** Apply the action immediately on match.
- Interface:** WAN
- Direction:** in
- TCP/IP Version:** IPv4
- Protocol:** TCP
- Source / Invert:** Use this option to invert the sense of the match.
Source: Single host or Network
10.0.2.15 24
- Destination / Invert:** Use this option to invert the sense of the match.
Destination: any

At the bottom, it says 'OPNsense (c) 2014-2024 Deciso B.V.'

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.



The screenshot shows the OPNsense web interface for editing firewall rules. The URL is https://10.0.0.49/firewall_rules_edit.php?if=wan&id=0. The left sidebar is collapsed, and the main content area is titled "WAN | Rules | Firewall". The configuration form for a rule is displayed:

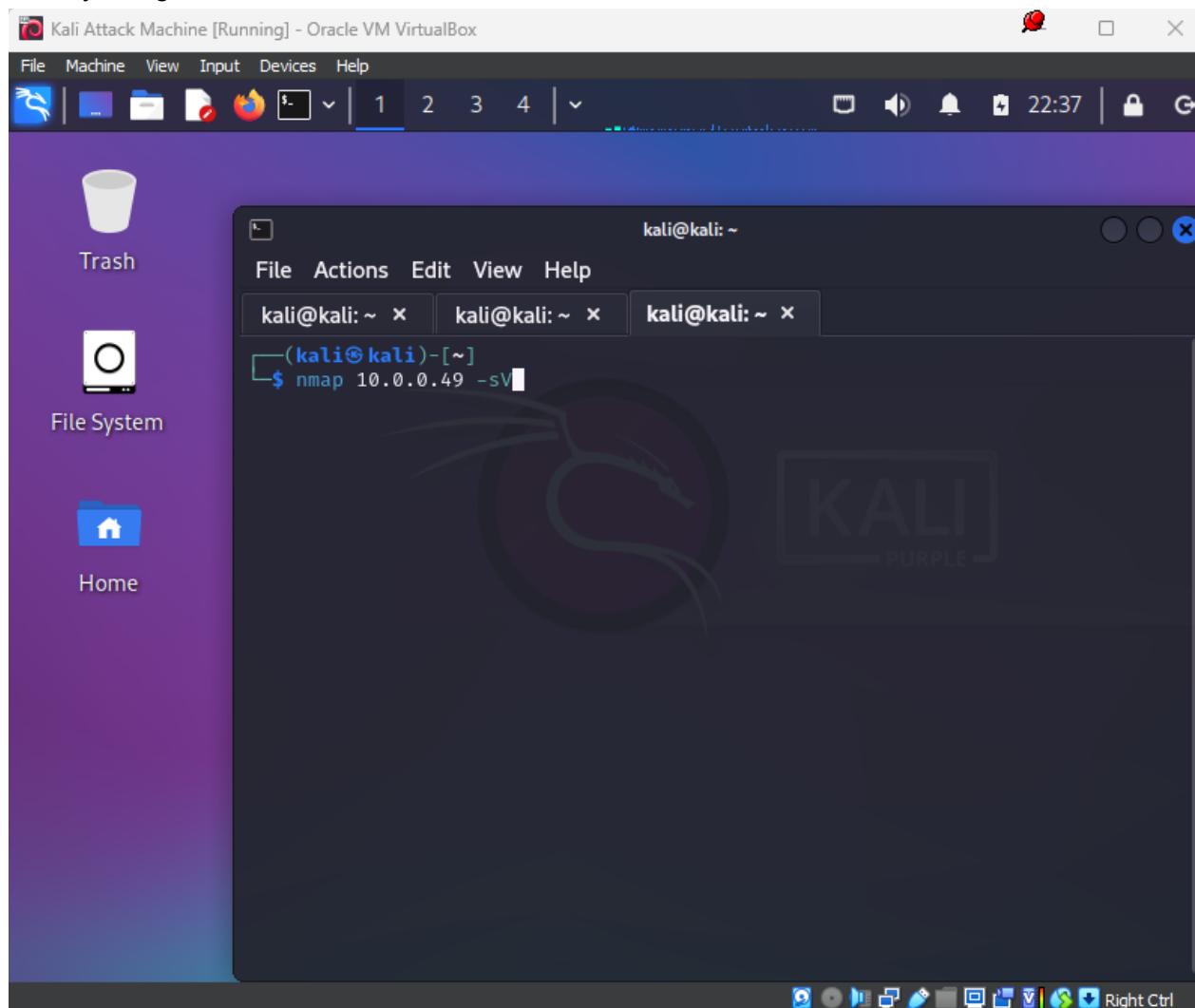
- Source:** Single host or Network, IP: 10.0.2.15, Port: 24
- Destination / Invert:** Destination is set to "any".
Invert checkbox is unchecked.
- Destination port range:** From: any, To: any
- Log:** Log packets that are handled by this rule is checked.
- Category:** Category field is empty.
- Description:** Description field contains "Kali Rule".
- No XMLRPC Sync:** No XMLRPC Sync checkbox is unchecked.
- Schedule:** Schedule dropdown is set to "none".
- Gateway:** Gateway dropdown is set to "default".
- Advanced features:** Show/Hide button is present.

At the bottom of the form, there is a blue button labeled "Apply changes".

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.



And here are the results,

The screenshot shows a Kali Linux desktop environment. On the left, there's a purple sidebar with icons for Trash, File System, and Home. The main window has a dark blue header bar with standard system icons like battery, signal, and volume. Below the header is a dock with several application icons. A central terminal window titled 'kali@kali: ~' is open, showing the results of an 'nmap -sV' scan against host 10.0.0.49. The output indicates the host is up with 0.0022s latency, and it lists two services: http (Open) and https (Open). It also prompts for service fingerprints submission. The bottom of the screen features a dock with various application icons.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 22:22 EST
Nmap scan report for 10.0.0.49
Host is up (0.0022s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    OPNsense
443/tcp   open  ssl/https  OPNsense

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

===== NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY) =====
```

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

OPNsense

Lobby Reporting System Interfaces Firewall VPN Services Terminal 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 7

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.

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

OPNsense

Lobby App Center System Interfaces Firewall VPN Services Captive Portal 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

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	<input checked="" type="checkbox"/> Enabled
	Alert

Info

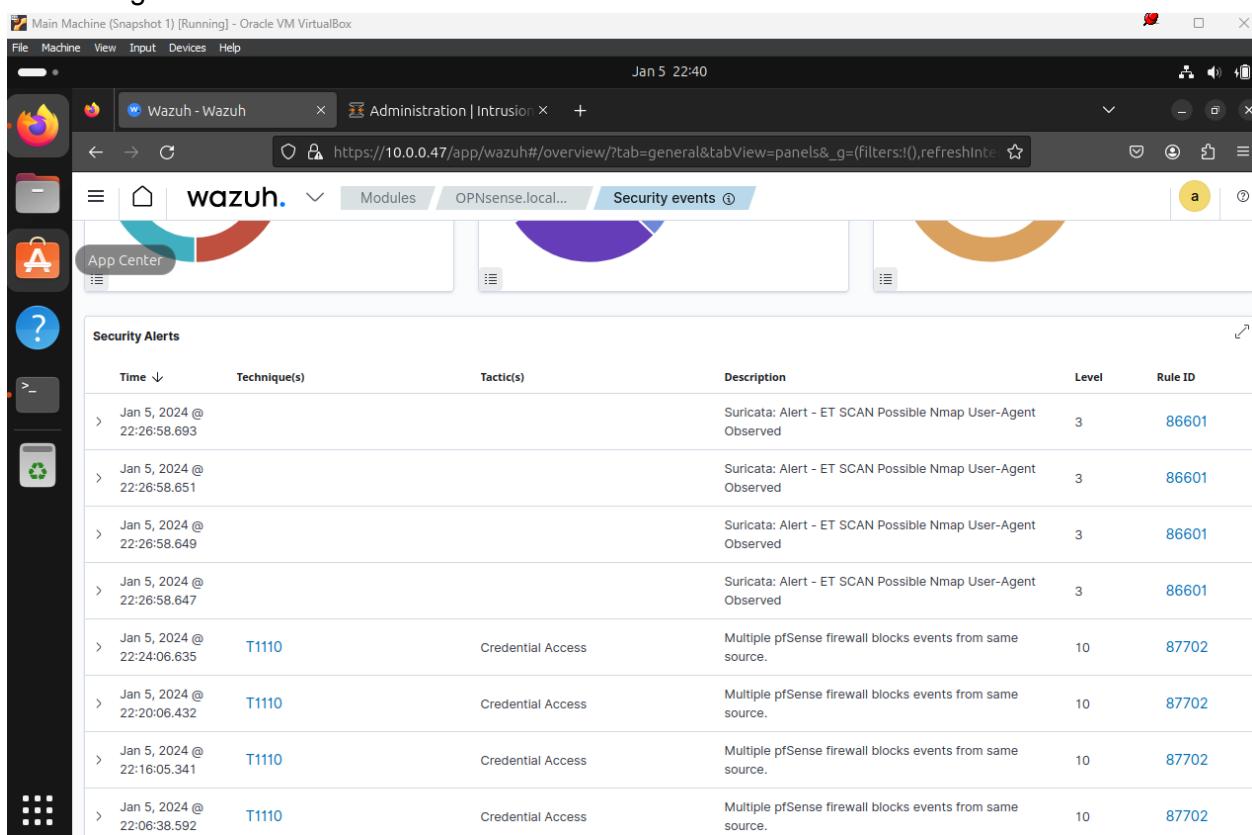
er-Agent ...
er-Agent ...

Showing 1 to 4

Close

OPNsense (c) 2014-2024 Deciso B.V.

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:!(),refreshInterval:<none>)

wazuh. Modules OPNsense.local... Security events

Terminal

@timestamp	2024-01-06T03:26:58.693Z
_id	szHP3lwBdpd4Vq3MVI_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:!(),refreshInterval:<none>)

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.firetimes	4
rule.groups	ids, suricata

As you can see, the attack was detected.