

Jared Lowe

3/8/25

Midterm Project Report

Professor Wimmer

## Virtual Lab With Threat Detection

As most projects this was exciting, frustrating and challenging. My objectives were to build a fully virtual cyber security lab and gain experience in networking, detection, and attack simulations. For the midterm and halfway through my goals were to build the virtual machines and connect them through pfSense. I first used Virtual Workstation Pro and designed a multi-tiered network with pfSense as the primary firewall. I then found Security Onion and added it for traffic monitoring. I then added the multiple machines Windows, Ubuntu, and Kali Linux that will be used for different responsibilities like networking, attacking, and vulnerability assessing. I had thought this would have been a straightforward connection and downloading project that would be done in a couple weeks but this quickly turned into more. I had to reset and redownload more than I thought, had to reconnect and debug more than I had thought, and troubleshooted and patiently waited more than I had thought. Though there were many hiccups that cost me days, I gained a lot of experience in firewall configuration, network segmentation, virtual networking, and security monitoring.

One of the more known and relaxed parts of the project is working with pfSense as many of the classes we have learned and worked with firewall connections. I learned a lot more about network adapters and how firewalls operate in a n enterprise environment. I encountered many challenges such as ensuring proper connections and setting correct configurations. Also a more relaxed part was the Kali setup which with their download allowed for an easy virtual machine environment already. I didn't have much trouble but did see why some would choose Linux over Windows.

To continue, setting up Windows and Ubuntu to function with the network infrastructure was an intriguing and fun part of the project. These helped with connectivity, segmentation, and showed me how a virtual machine can interact within the network I built. It was at times tricky and hard to configure but I came out with a more impactful knowledge of these operating systems and their attributes.

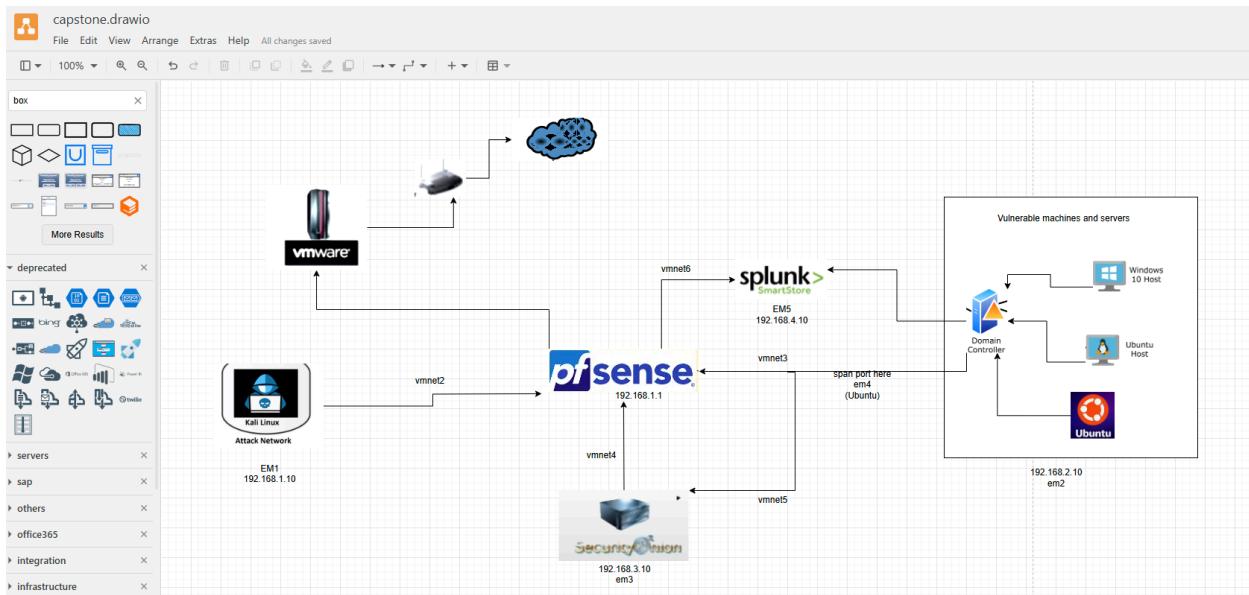
Most frustrating part was Security Onion as when I learned about it, it sounded great to add to my workstation but doing so I had to rest/reboot/redownload close to 20 times and it took two downloads that are both around 30-60 minutes and this was aggravating. I did learn about the tools it brings and was able to mess around with it. Similarly was the longing configuration of pfSense through Kali which was fun as it helped me gain a larger sense of firewall rules and configurations. I got to see how my built network was used and segmented. I got to understand the power and future use of the pfSense and anticipate the next steps.

The images below serve as my evidence of work completed. I tried to make as many screenshots and tried to be thorough as possible without being too long. There were many times where I had to delete images to add a newer and better image. Hopefully my screenshots are clear and coincide to show you my work and effort in this portion of the project.

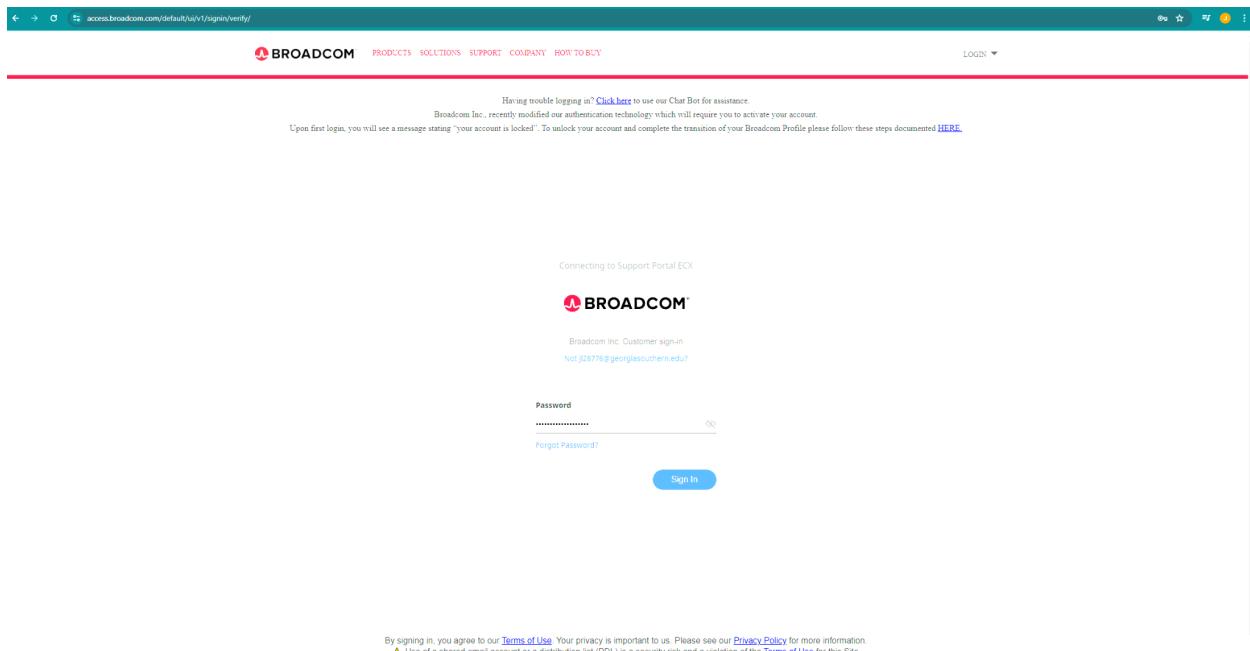
All in all this project was both rewarding and exhausting but through it all this has been a great experience and I can't wait to add it to my resume and GitHub. Here I was able to get hands-on experience and see my networking come to life. This strengthened all my skills and gave me insight into cyber security roles. I now feel more confident in my abilities

# TOC

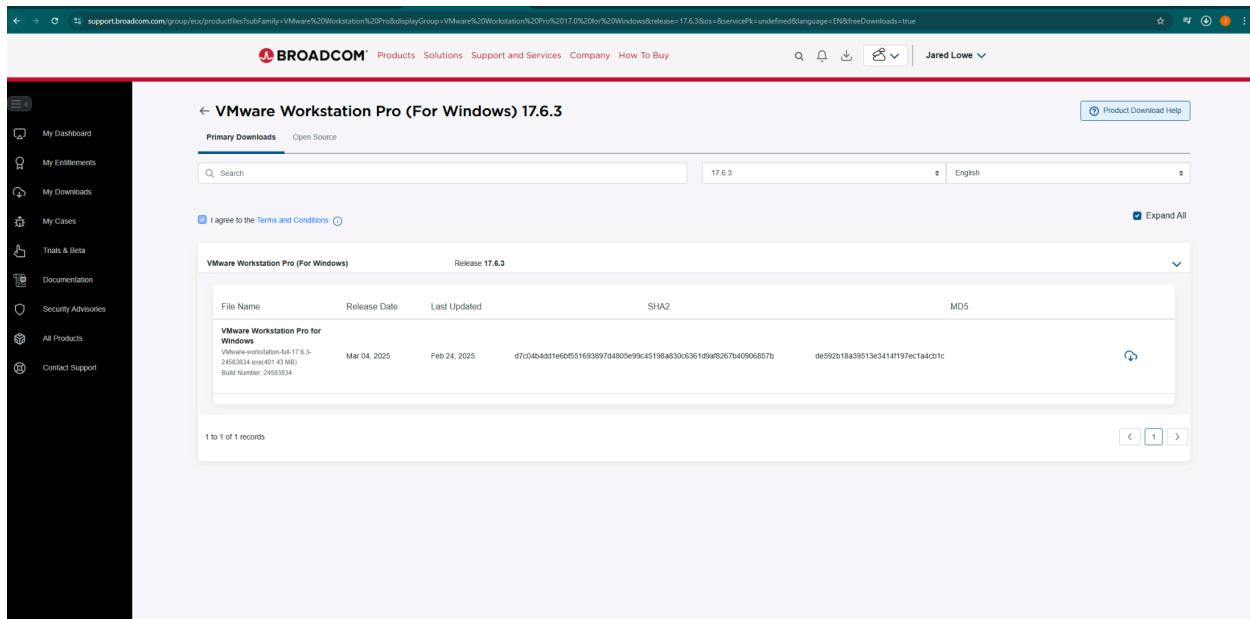
<b>Topology.....</b>	<b>4</b>
<b>VMware Workstation.....</b>	<b>5-6</b>
<b>Pfsense VM.....</b>	<b>7-15</b>
<b>Security Onion &amp; Ubuntu VMs.....</b>	<b>16-30</b>
<b>Linux VM.....</b>	<b>31-35</b>
<b>Windows Server Vm.....</b>	<b>36-45</b>
<b>Pfsense Firewall Configuration/Rules.....</b>	<b>46-</b>
<b>Resources.....</b>	



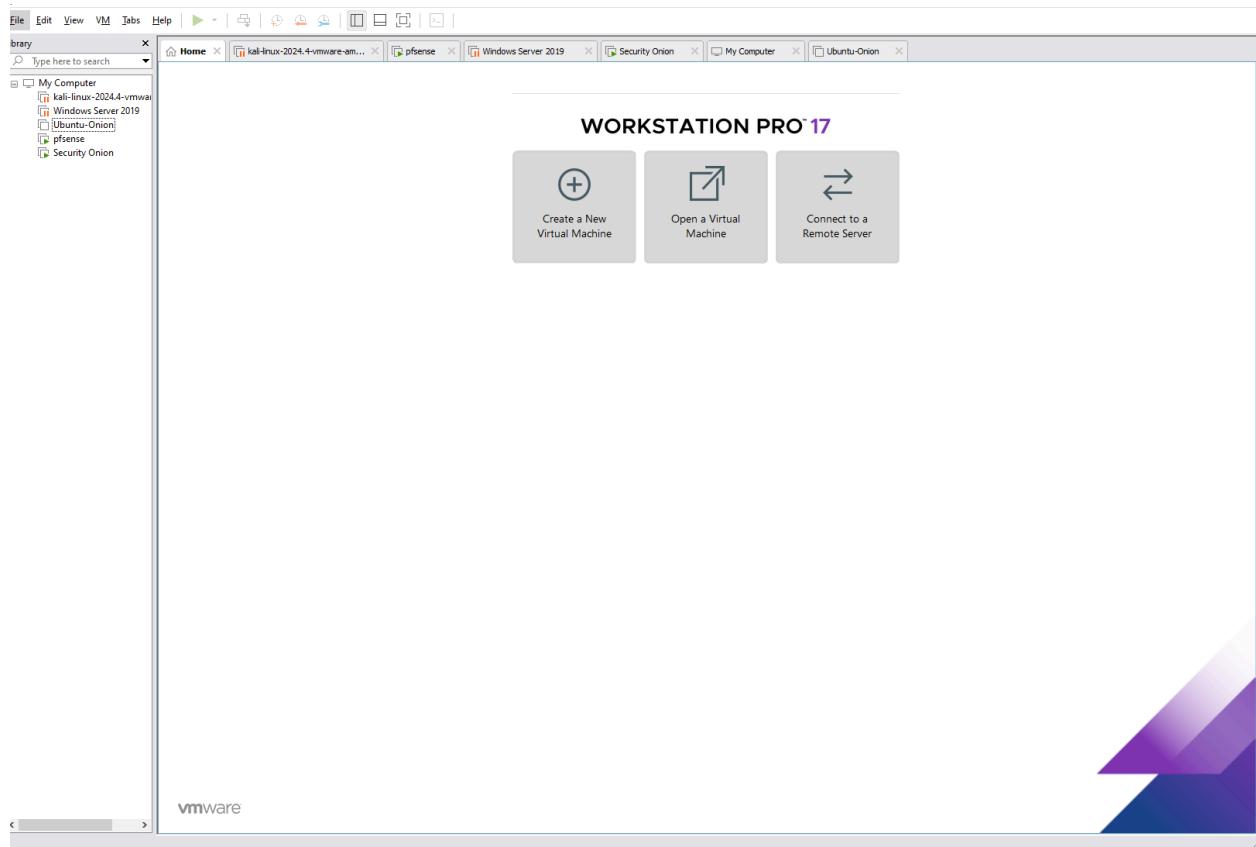
## -Logging into Broadcom to acquire VMware Workstation Pro



## -VMware download



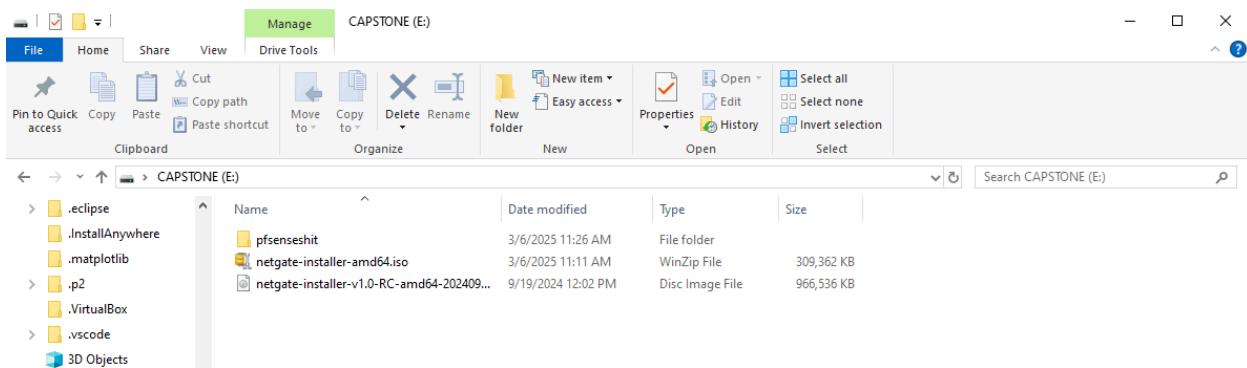
## -The Workstation program



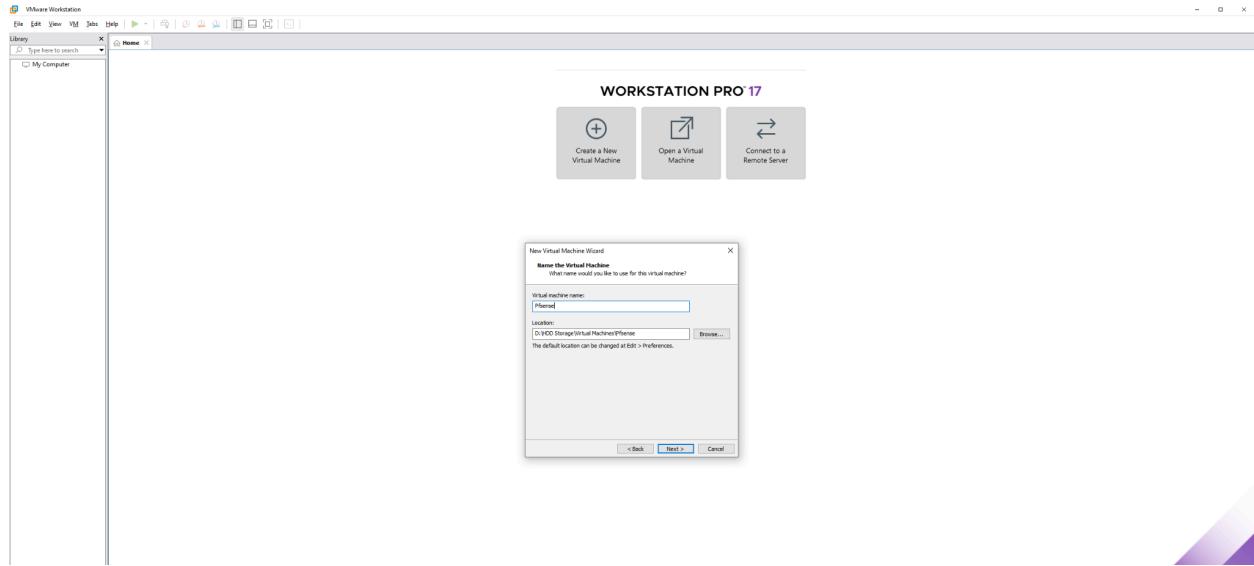
## -Downloading pfSense

The screenshot shows the pfSense.org download page. At the top, there's a navigation bar with links for Get Started, Cloud, Products, Services, Support, Training, Community, and Download. Below the navigation is a main content area titled "Latest Stable Version". It features a "Version: 2.7.2" section with a "RELEASE NOTES" button, a "SOURCE CODE" button, and a prominent blue "DOWNLOAD" button. To the right of this is a "Supported by netgate" logo. Further down, there's a "Subscribe To The Netgate Newsletter" section with fields for "Email\*", "I understand I am signing up to receive the newsletter, software announcements, and special offers. See our [newsletter archive](#) for past announcements.", and "I'm interested in...". There are checkboxes for "pfSense Plus Appliances" and "TNSR Appliances", followed by a "Subscribe" button and a link to the "privacy policy". Below this, there's a "Daily Snapshots Available" section with a "DAILY SNAPSHOTS" button and a "DISCUSSION FORUM" button. A note says "You can determine the files needed for your install by reading the rest of this page for guidance."

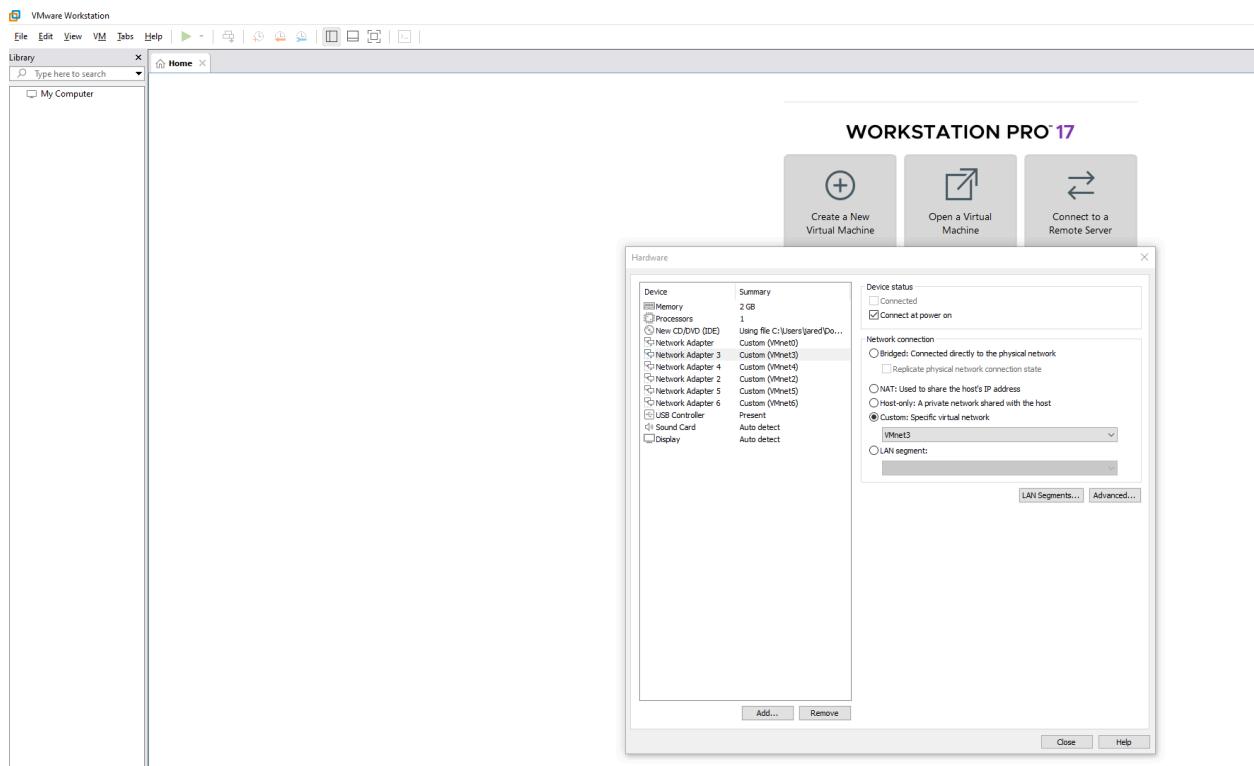
## -Unzipping the pfSense file with 7-zip to extract the iso file



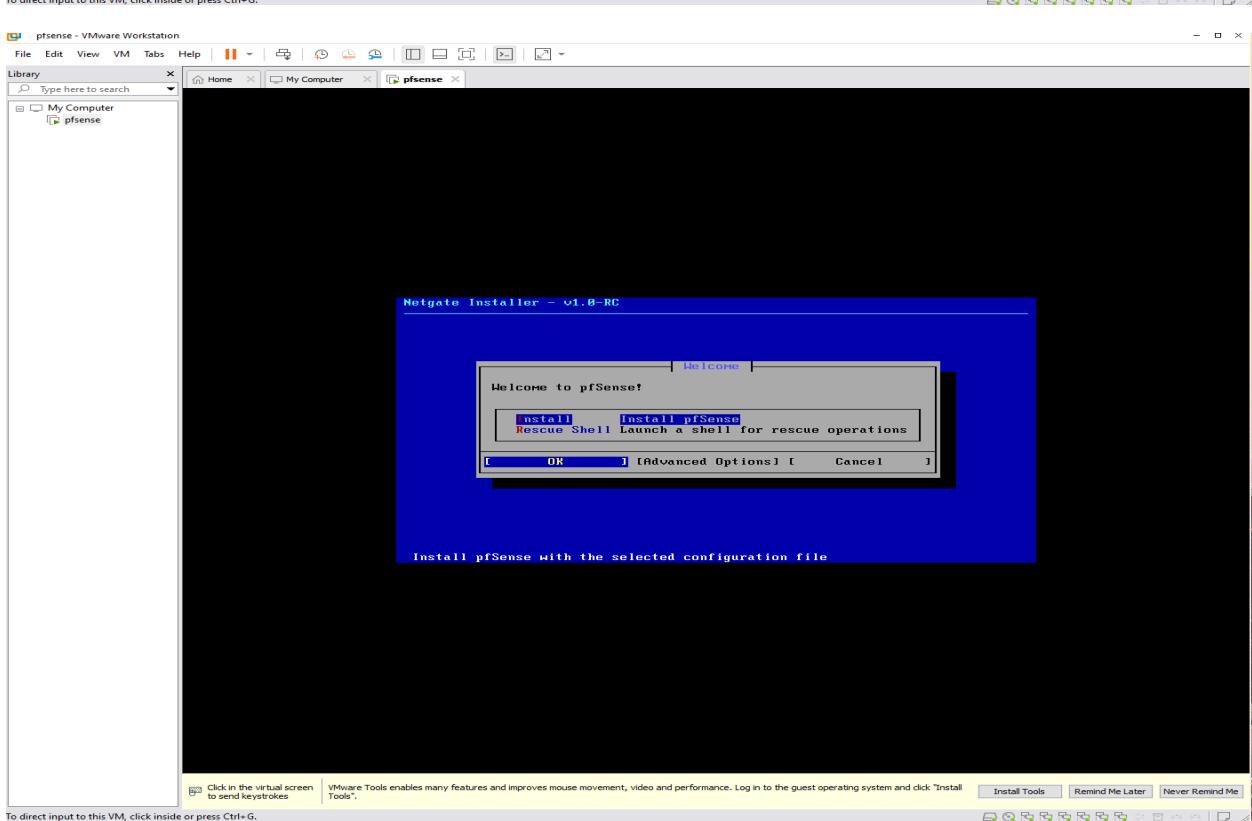
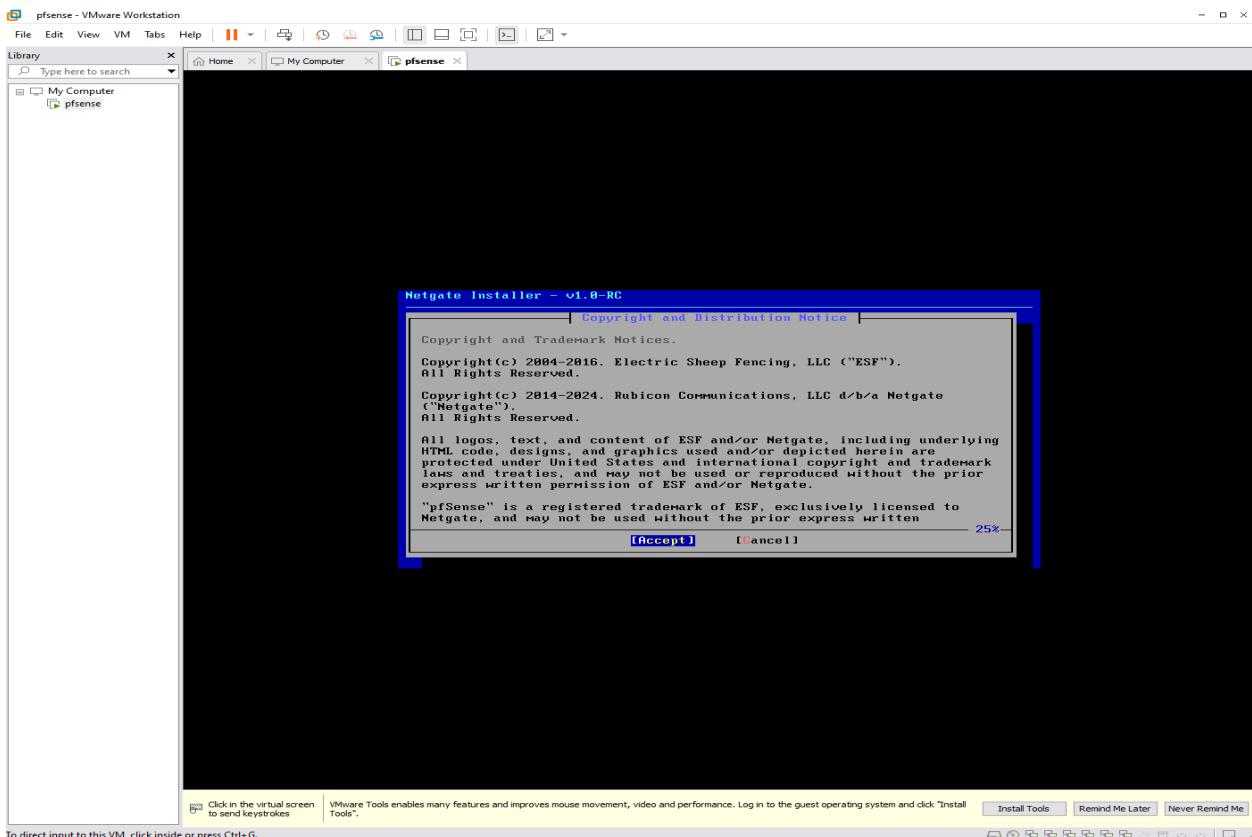
-Adding pfSense as a virtual machine

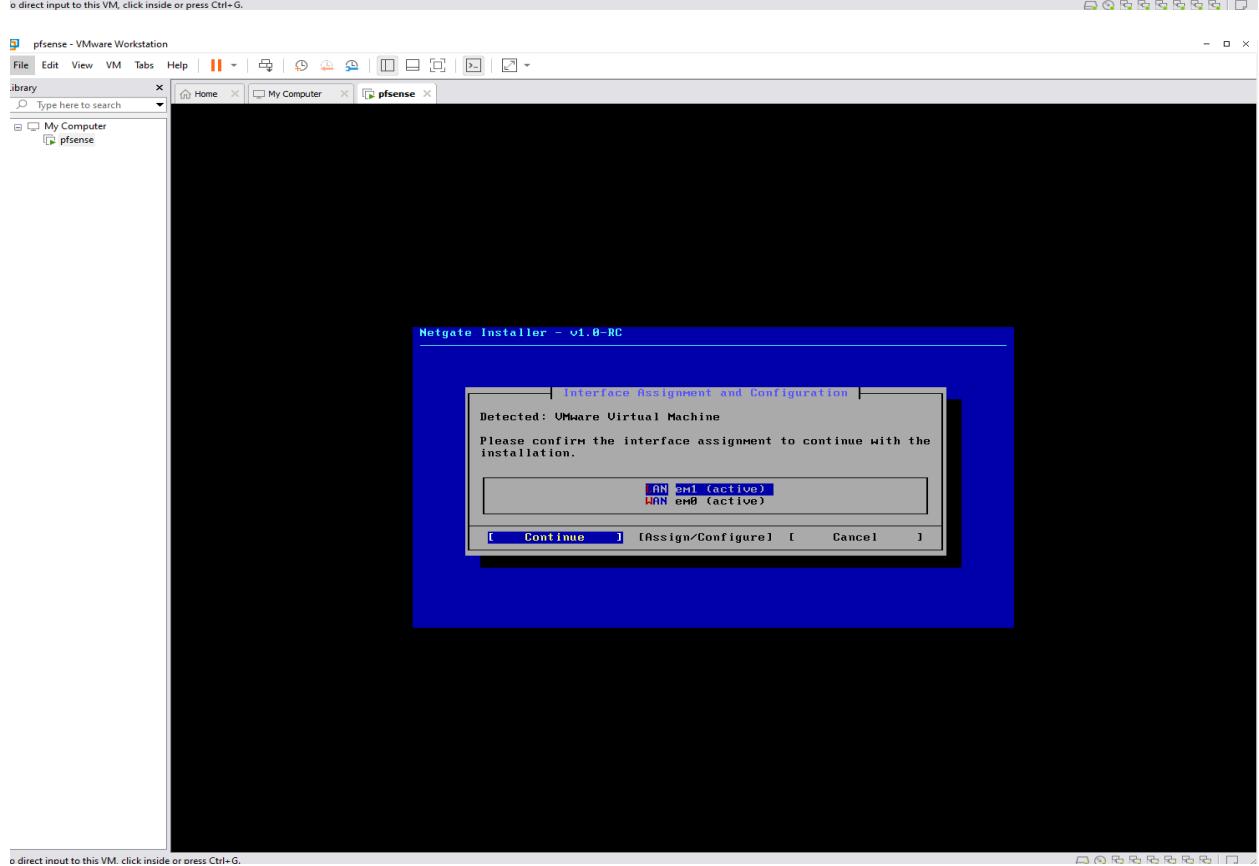
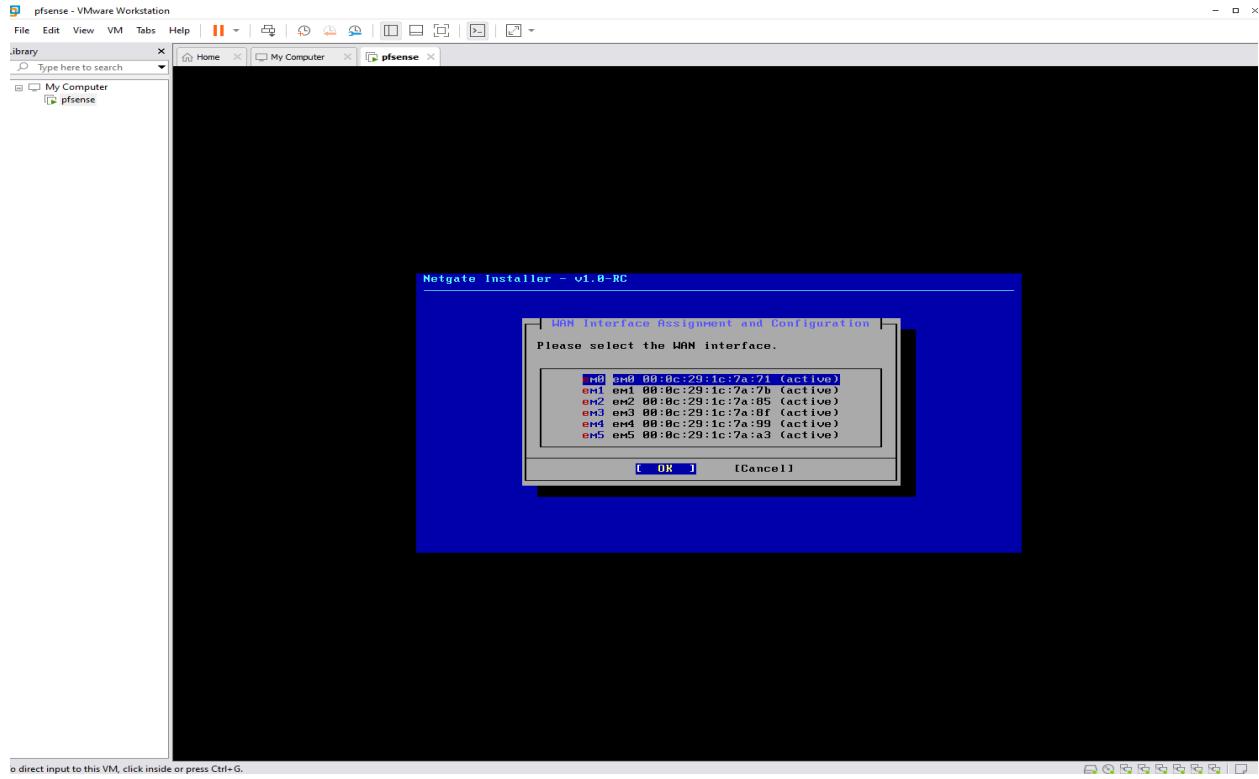


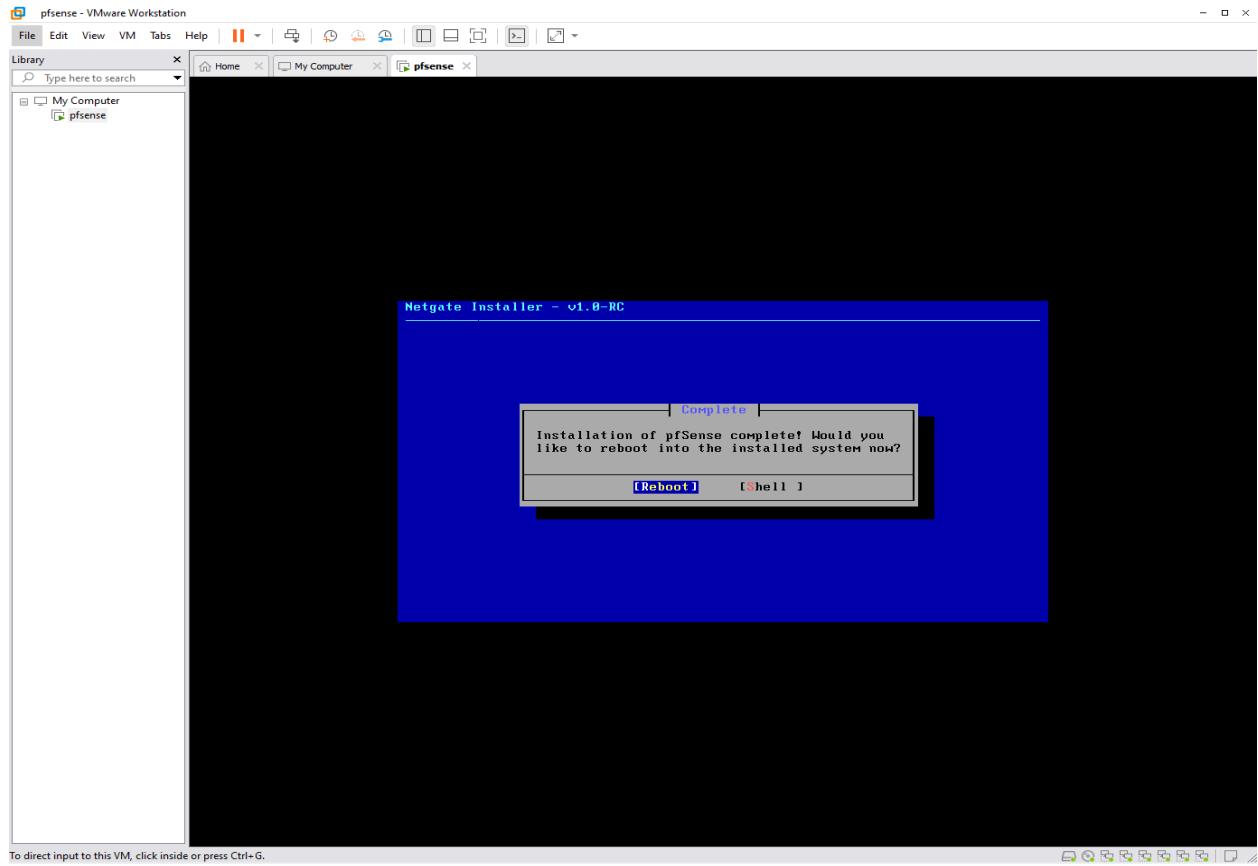
-configuring pfSense and adding 5 new network adapter with own specific virtual network



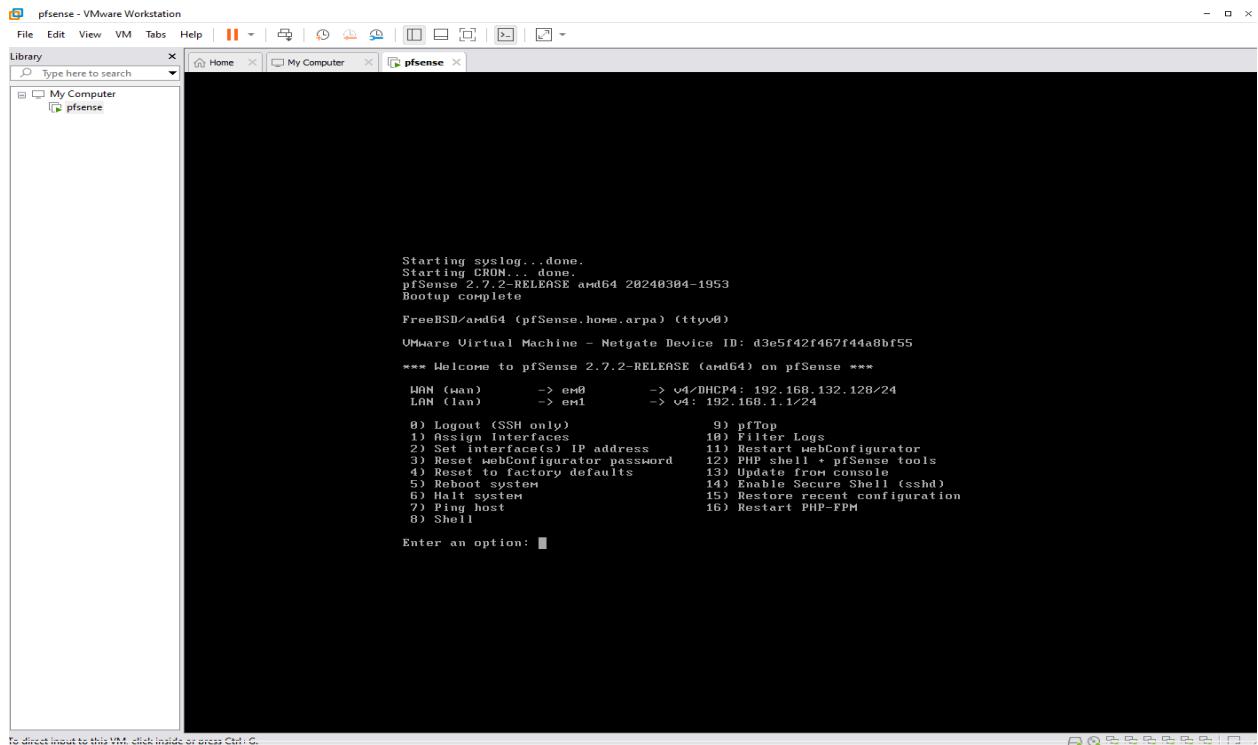
-The following images show entering the pfSense and enabling it inside the VM(5 images)







-after rebooting now we can set up the connections



-the following images will show the connections into the interfaces(3 images)

```

Enter an option: 1

Valid interfaces are:
em0    00:0c:29:1c:7a:71  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1    00:0c:29:1c:7a:70  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2    00:0c:29:1c:7a:69  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3    00:0c:29:1c:7a:68  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4    00:0c:29:1c:7a:67  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5    00:0c:29:1c:7a:63  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 or a): em0

```

To direct input to this VM, click inside or press Ctrl+G.

```

NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished): em4

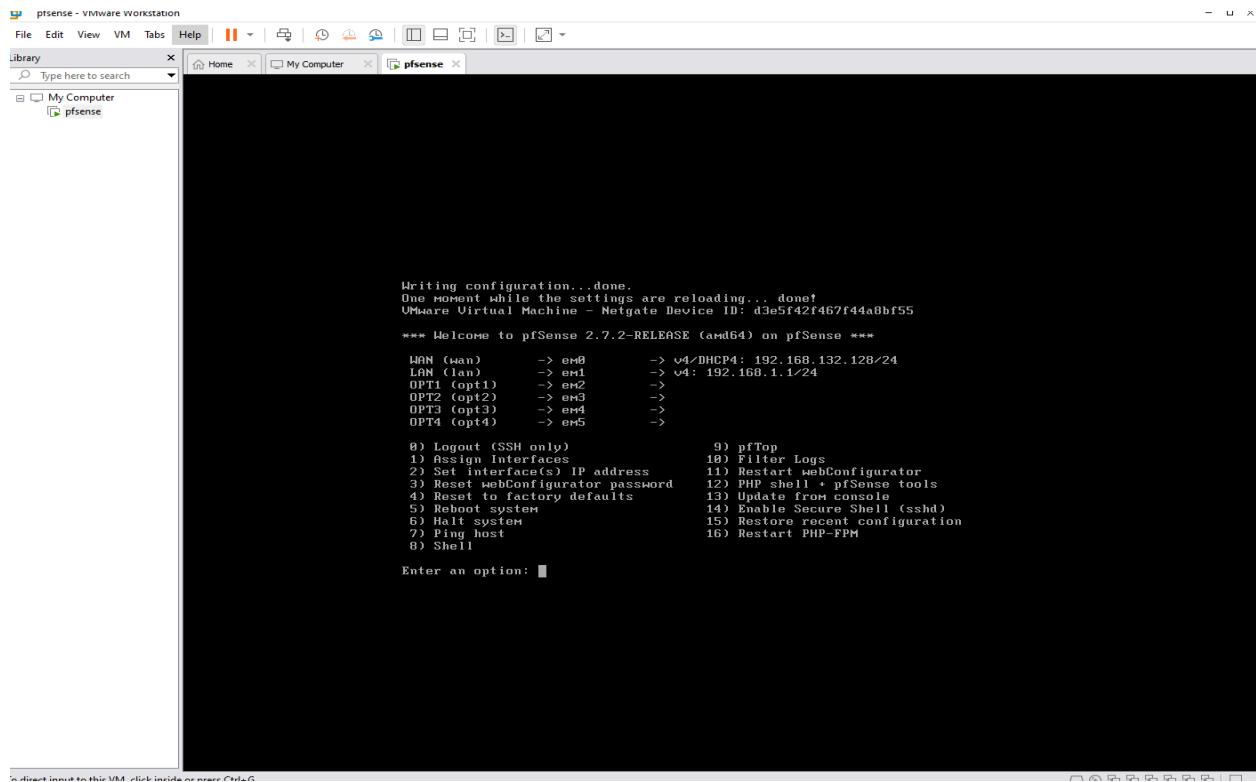
Enter the Optional 4 interface name or 'a' for auto-detection
(em5 a or nothing if finished): em5

The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4
OPT4 -> em5

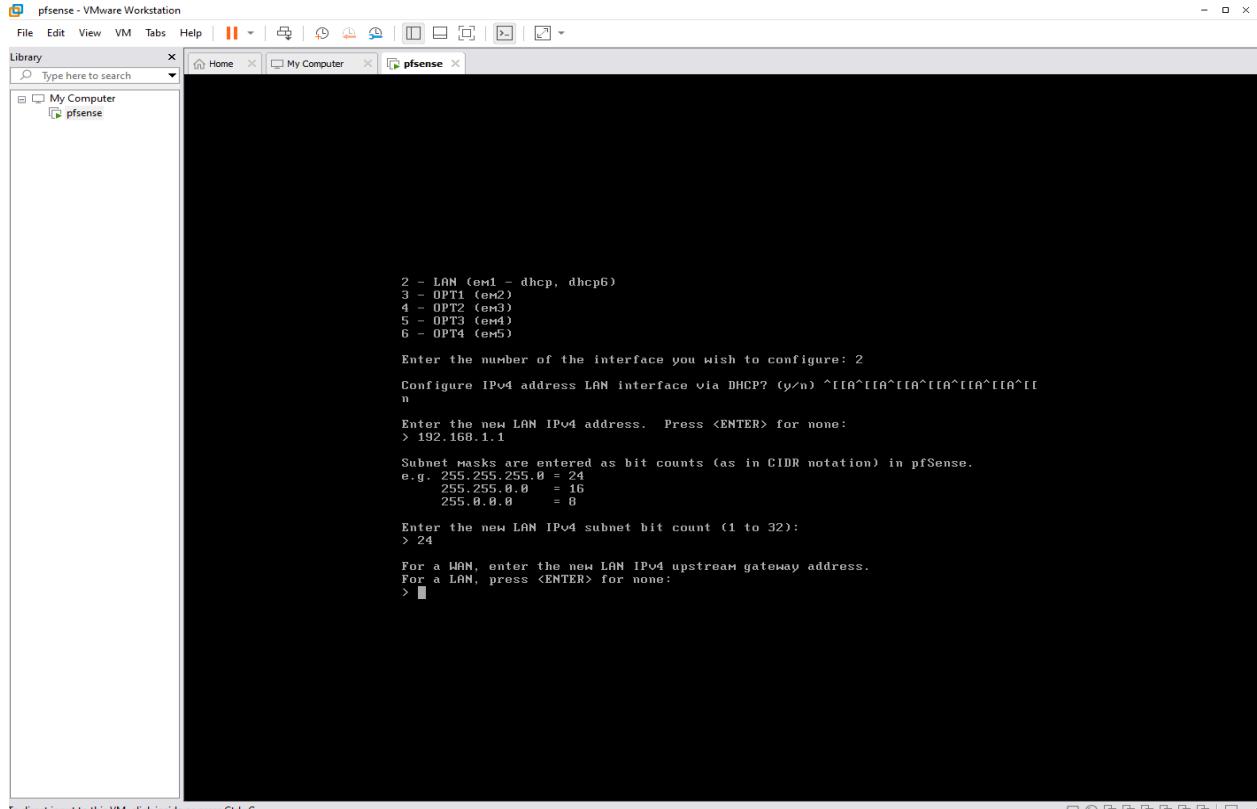
Do you want to proceed [y/n]? n

```

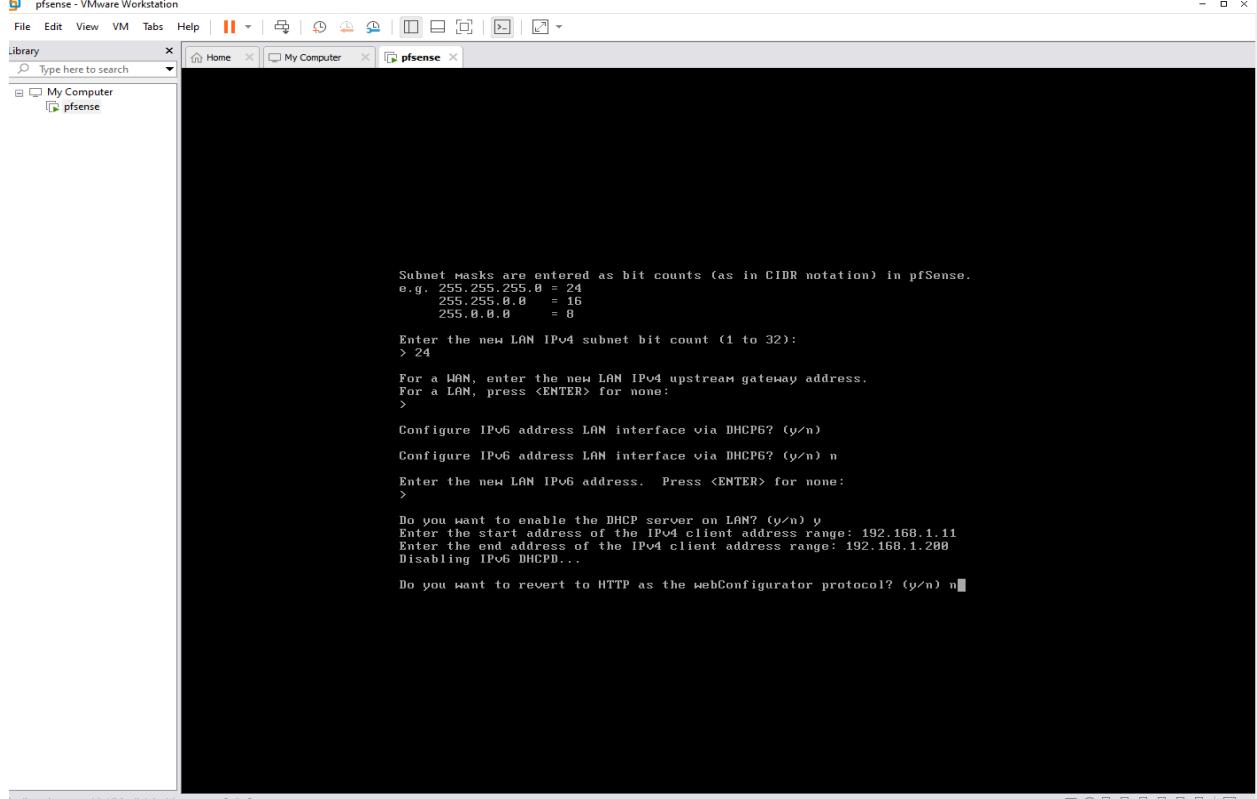
To direct input to this VM, click inside or press Ctrl+G.



-now the following will be the interface IP addresses set up(2 images)

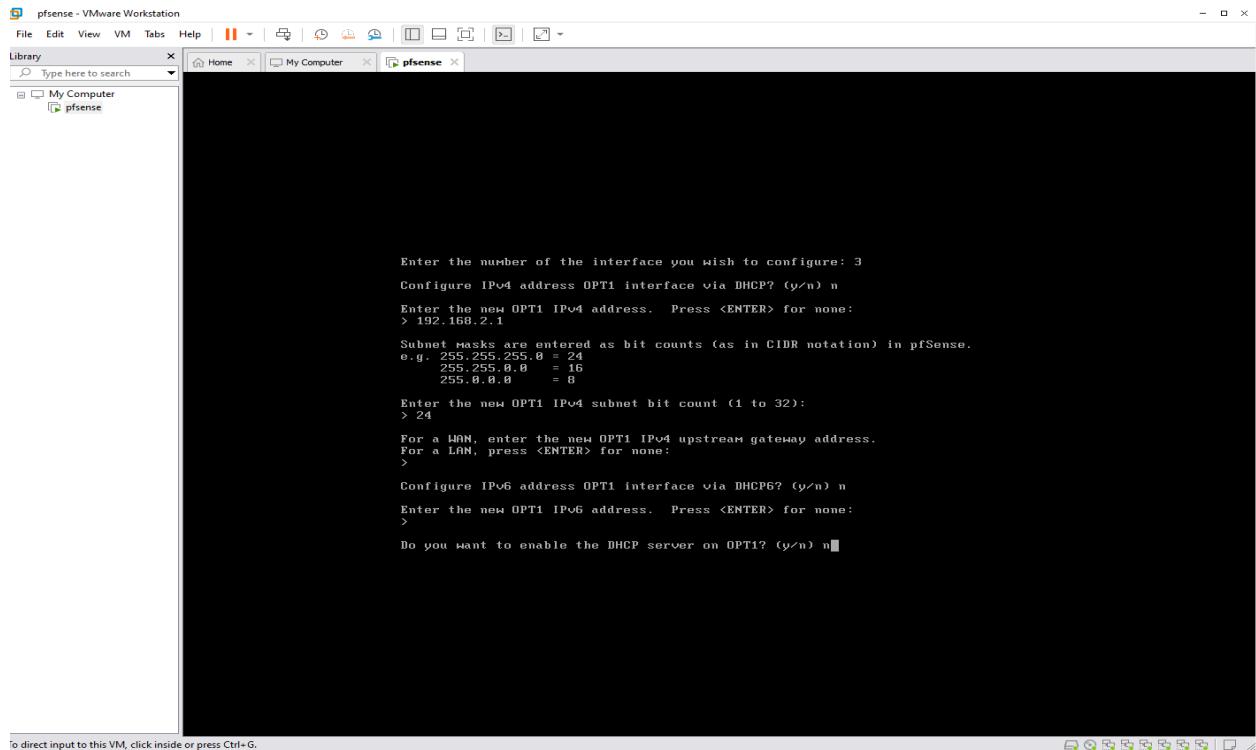


To direct input to this VM, click inside or press **Ctrl+G**.

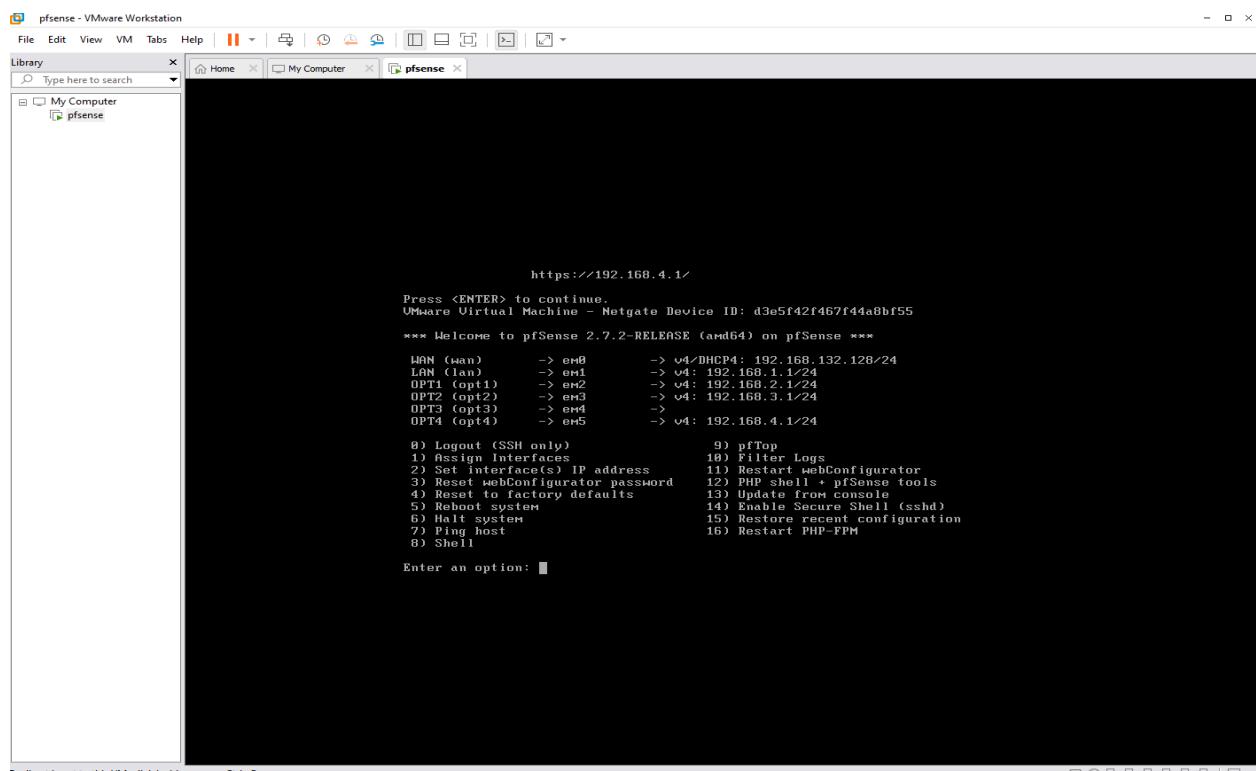


'o direct input to this VM. click inside or press Ctrl+G.

-To minimize the amount of images I set opt1, opt2, and opt4 to these settings and leaving opt3 blank so it can have pinpoint traffic that security onion can monitor



-This is the finished interface setup



- Now I will add on security onion as a new Vm to monitor traffic:
- This is the downloads page I found on a github with the latest version

[Preview](#) [Code](#) [Blame](#) 52 lines (88 loc) • 1.95 KB

**2.3.300-20240401 ISO image built on 2024/04/01**

**Download and Verify**

2.3.300-20240401 ISO image:  
<https://download.securityonion.net/file/securityonion/securityonion-2.3.300-20240401.iso>

MDS: 5CBDA8012D773C5EC362D21C4E3B7FB  
SHA1: T3A4FAA0E11F09F529FF38EC239211CD87CB1A7  
SHA256: 123066DAFBF6F2AA0E1924296CFEE1213002D7760E8797AB74F1FC1D683C6D7

Signature for ISO image:  
<https://github.com/Security-Onion-Solutions/securityonion/raw/master/sigs/securityonion-2.3.300-20240401.iso.sig>

Signing key:  
<https://raw.githubusercontent.com/Security-Onion-Solutions/securityonion/master/KEYS>

For example, here are the steps you can use on most Linux distributions to download and verify our Security Onion ISO image.

Download and import the signing key:

```
wget https://raw.githubusercontent.com/Security-Onion-Solutions/securityonion/master/KEYS -O - | gpg --import -
```

Download the signature file for the ISO:

```
wget https://github.com/Security-Onion-Solutions/securityonion/raw/master/sigs/securityonion-2.3.300-20240401.iso.sig
```

Download the ISO image:

```
wget https://download.securityonion.net/file/securityonion/securityonion-2.3.300-20240401.iso
```

Verify the downloaded ISO image using the signature file:

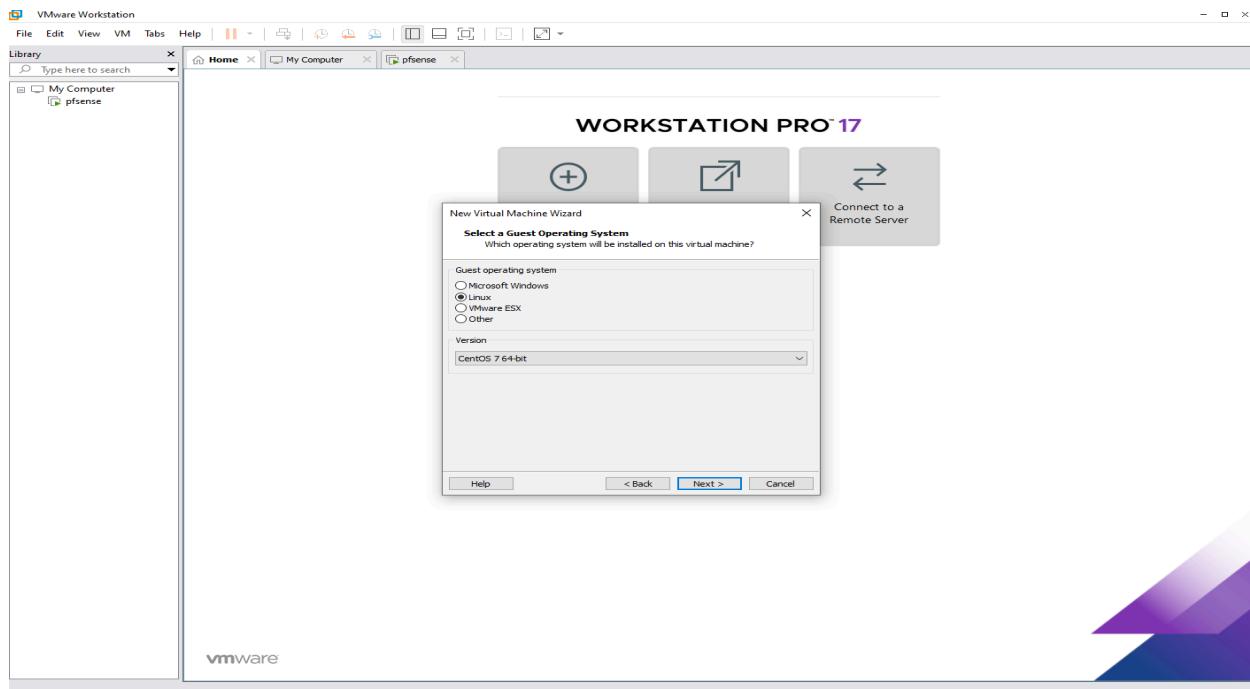
```
gpg --verify securityonion-2.3.300-20240401.iso.sig securityonion-2.3.300-20240401.iso
```

The output should show "Good signature" and the Primary key fingerprint should match what's shown below:

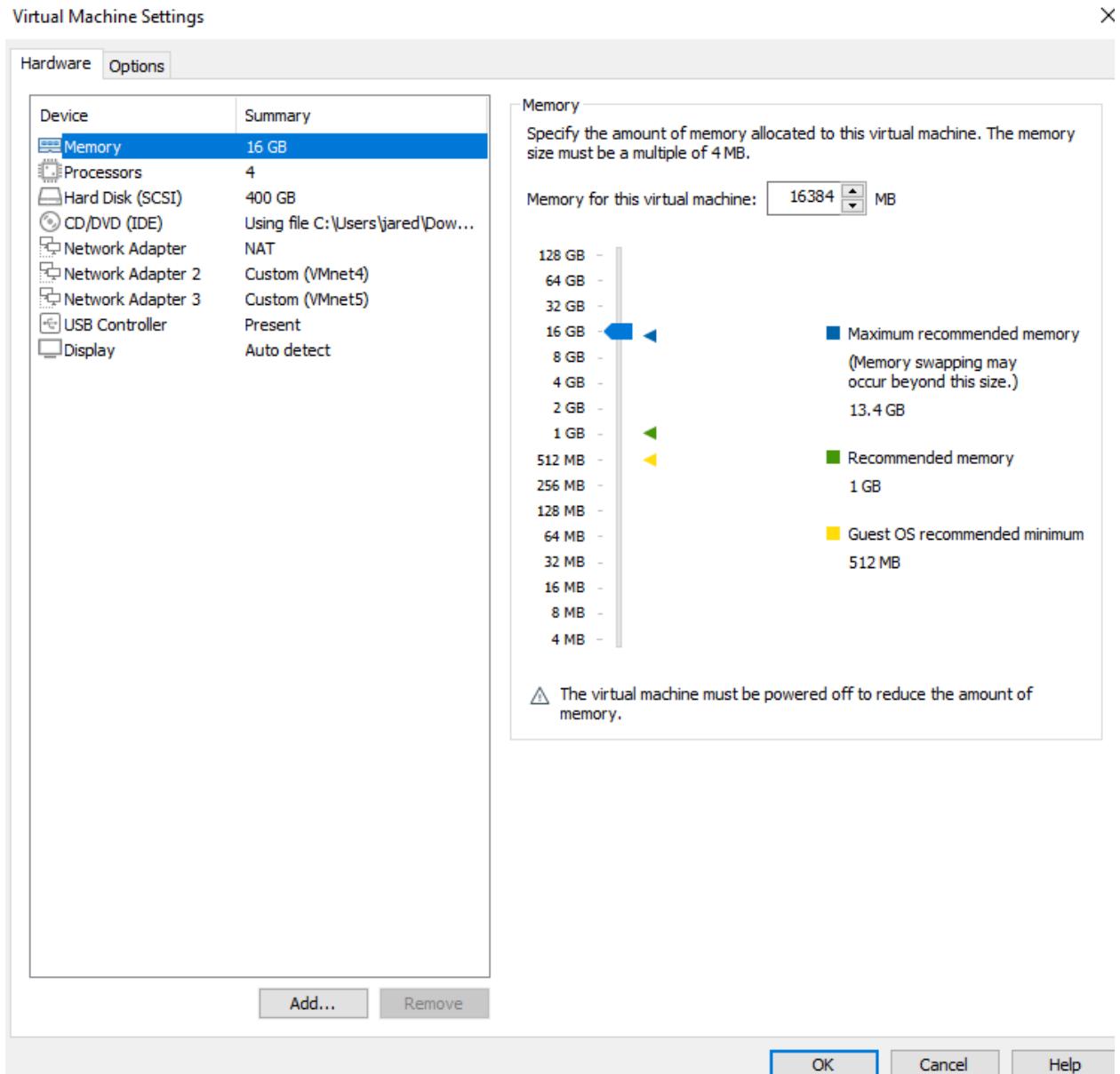
```
gpg: Signature made Wed 27 Mar 2024 05:09:33 PM EDT using RSA key ID FEE507013
gpg: Good signature from "Security Onion Solutions, LLC <info@securityonionsolutions.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C804 A93D 36BE 0C73 3EA1 9644 7C10 60B7 FEE50 7013
```

Once you've verified the ISO image, you're ready to proceed to our Installation guide:  
<https://docs.securityonion.net/en/2.3/installation.html>

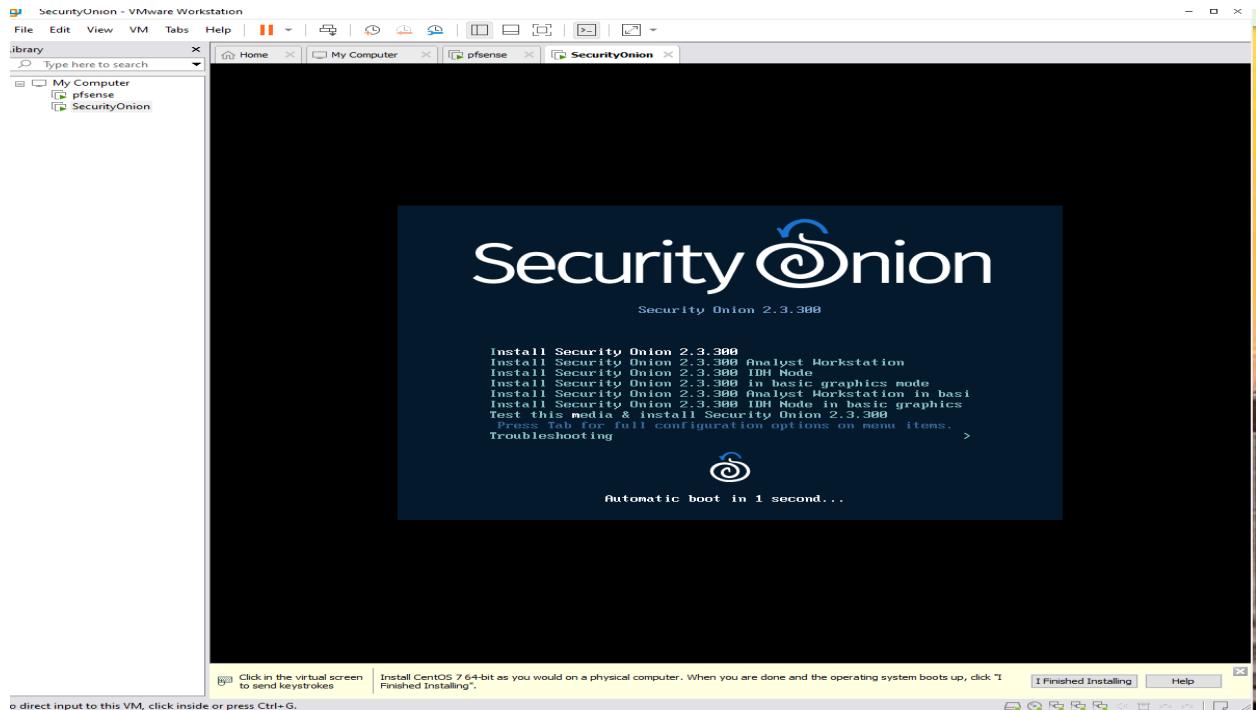
## -Setting the OS and version for security Onion



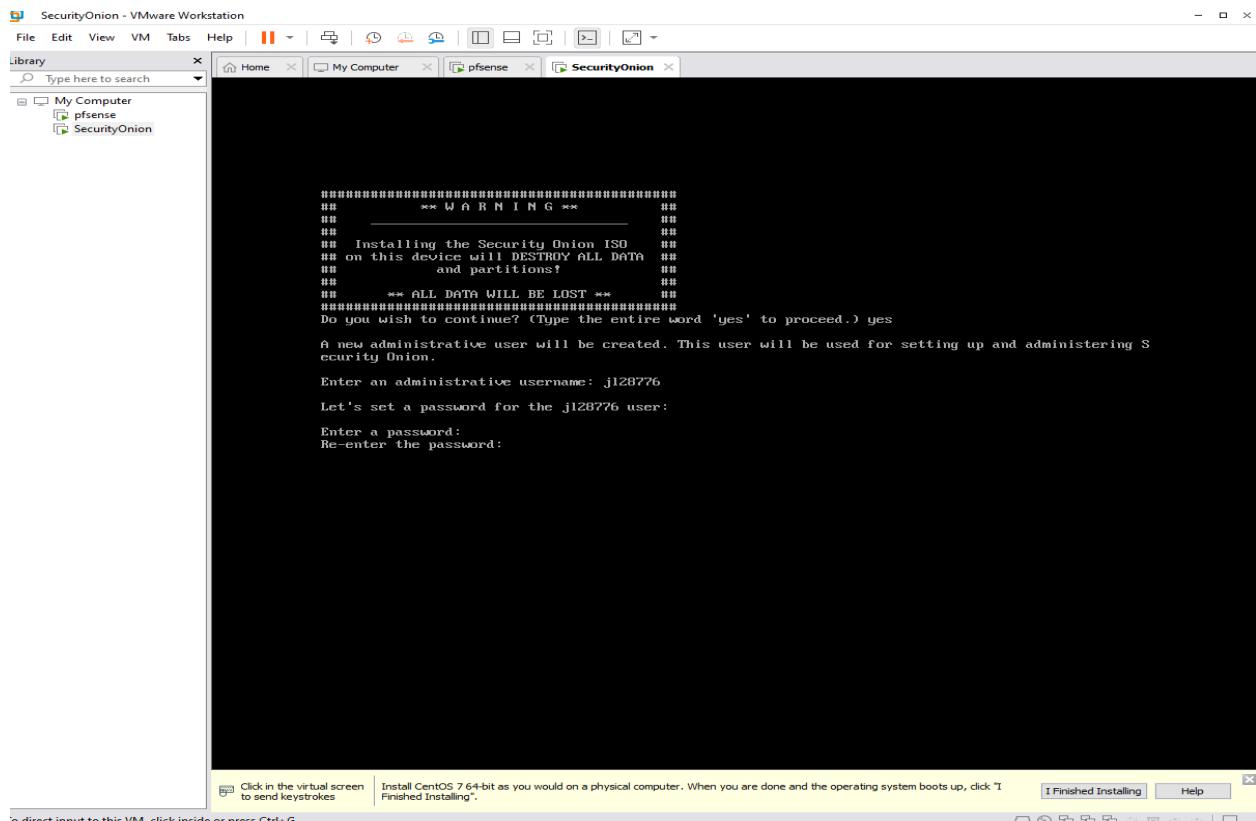
-setting up the hardware. Setting the memory and processors to the minimum it recommends for security Onion. Adding 2 network adapters where we match one to vmnet4 tp pair with pfSense and vmnet5 to port.



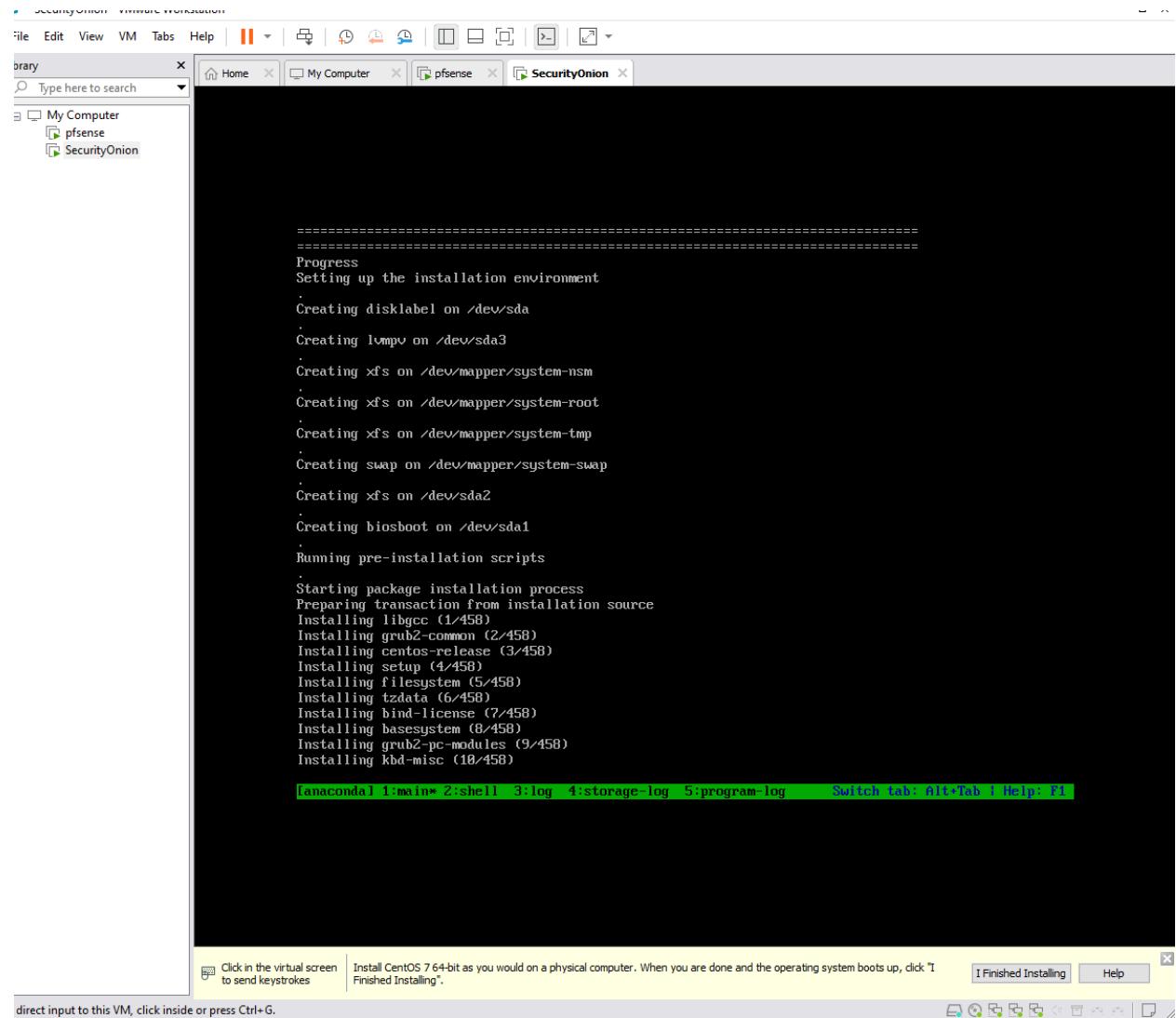
-now we can enter the security onion



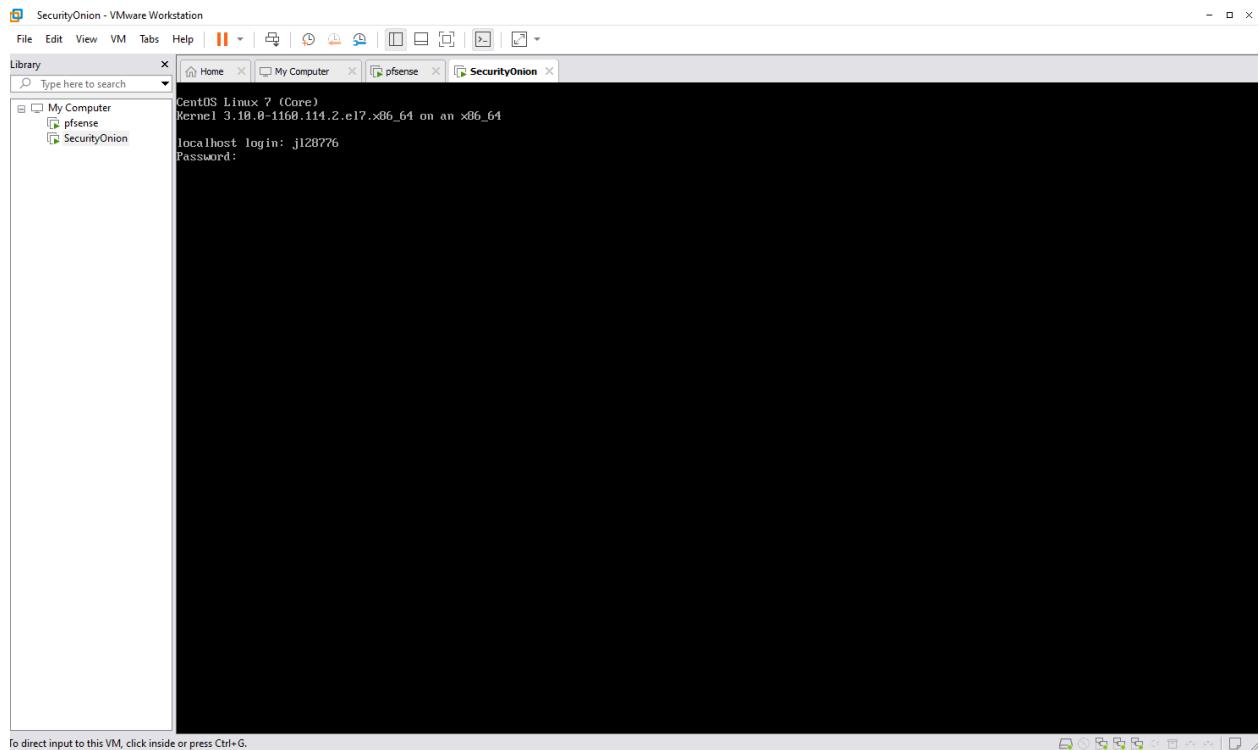
-now we can create a username and password for security onion where i used my GSU username for this username and just onion as the password



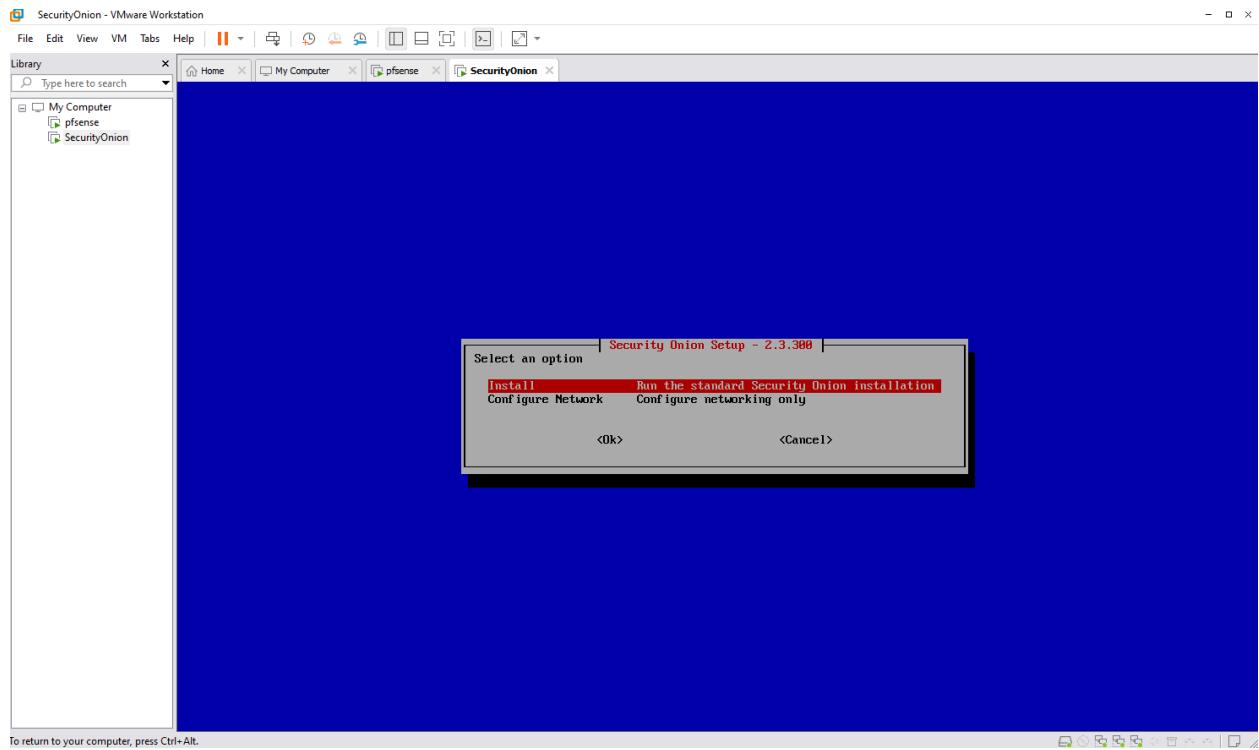
-Long installation process(30 min)

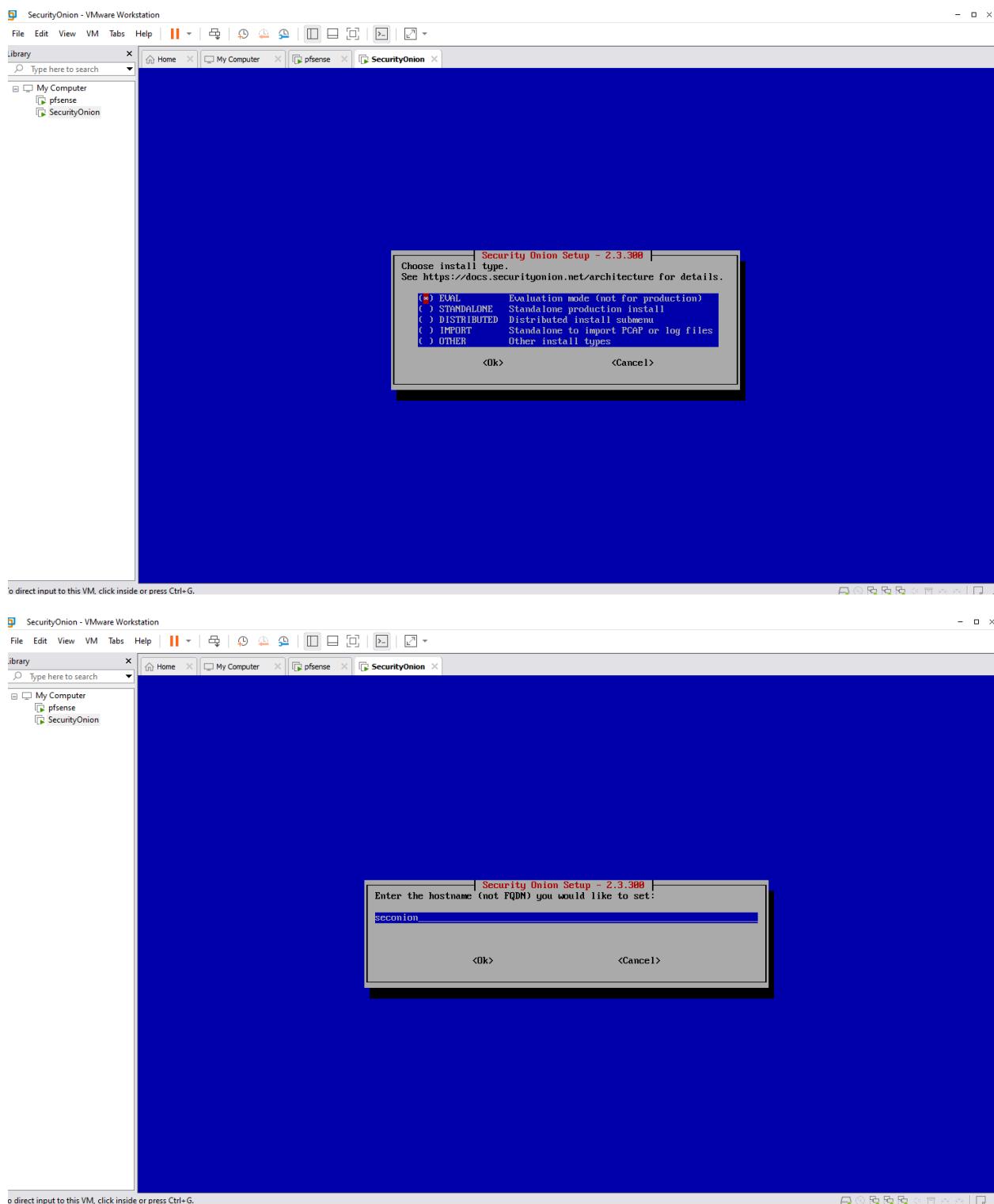


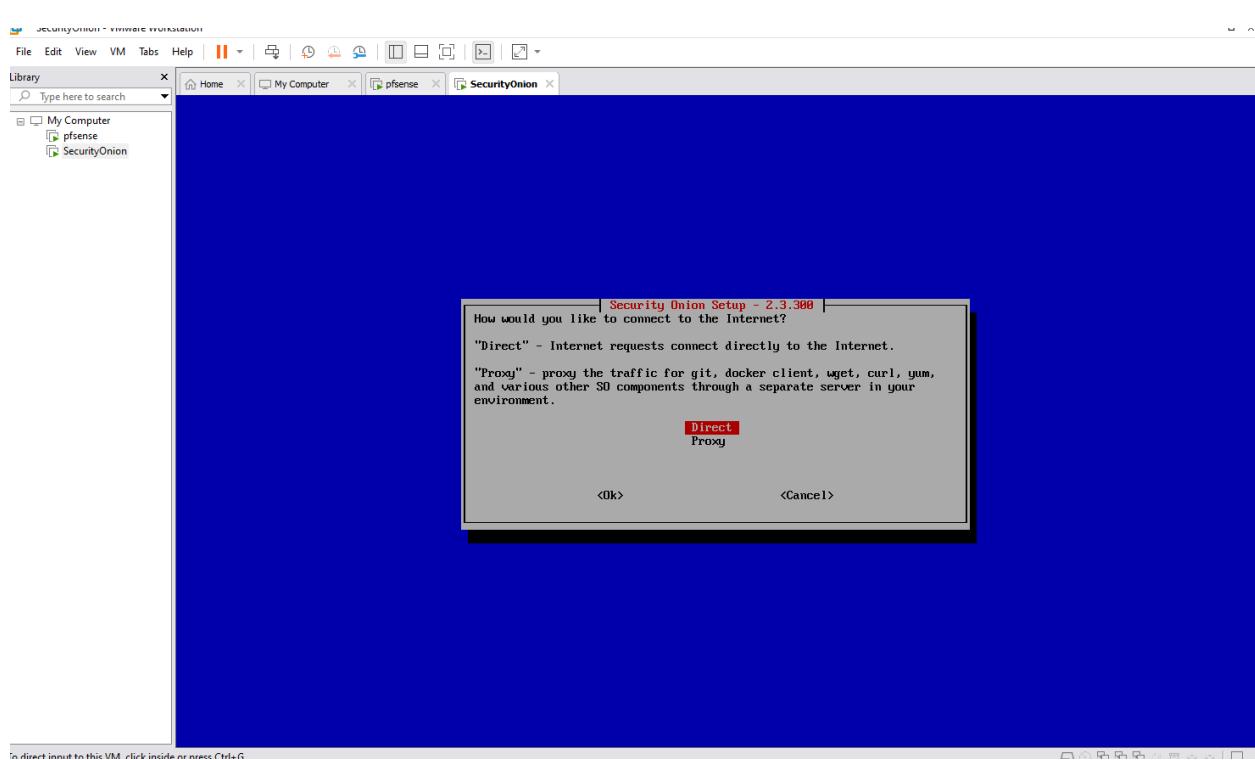
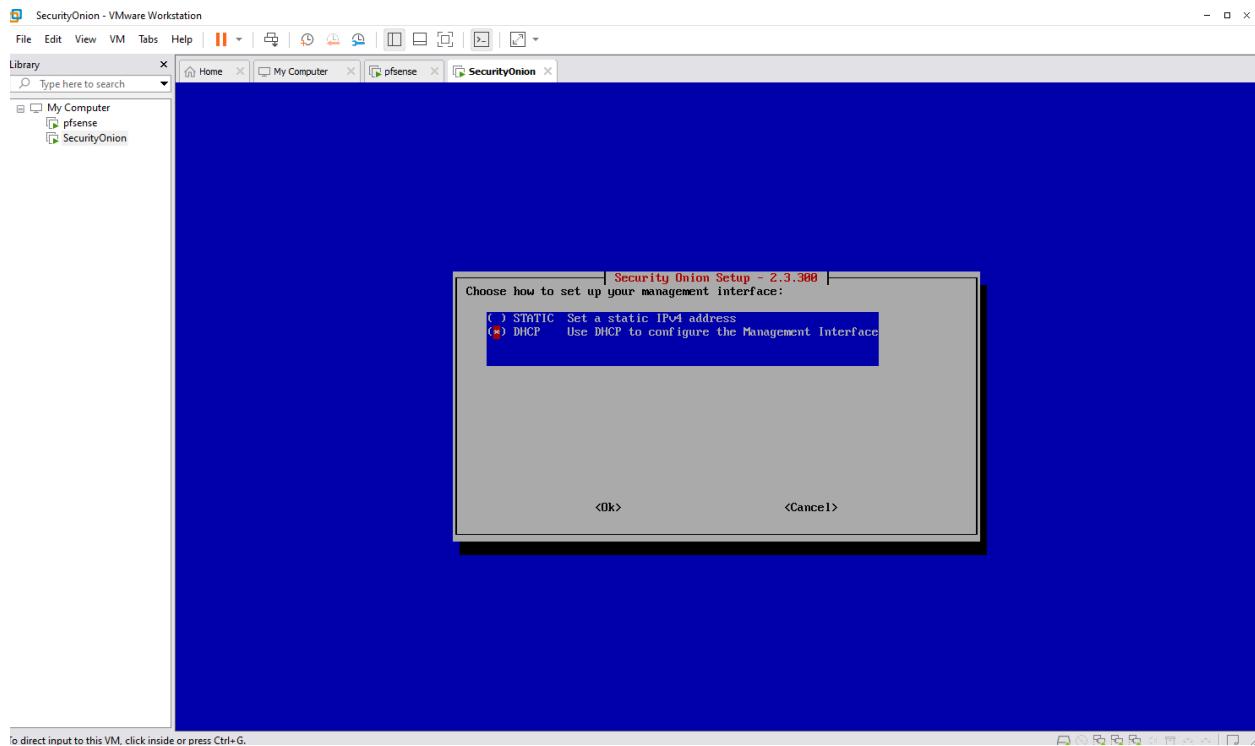
-After installation and reboot we sign into the onion

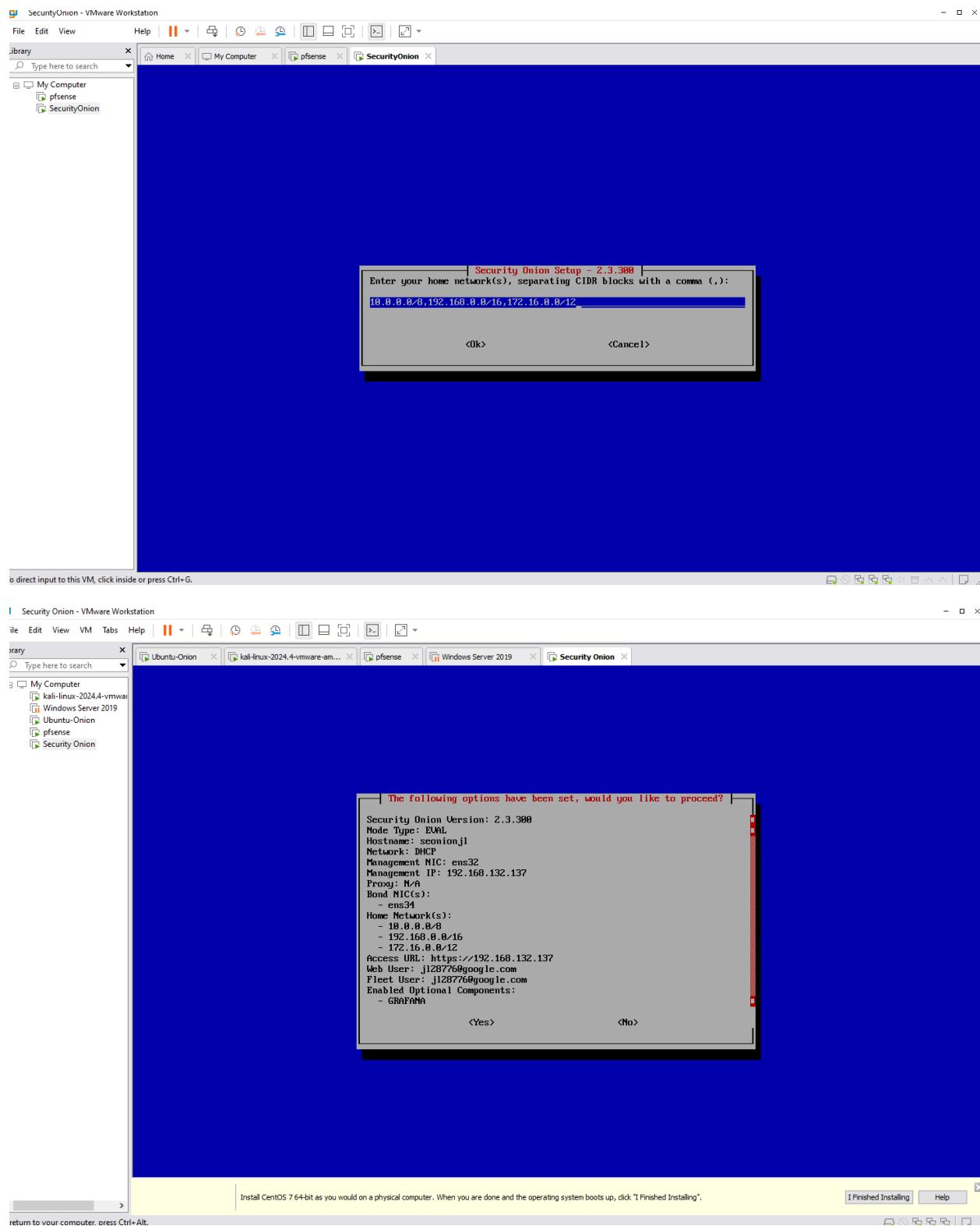


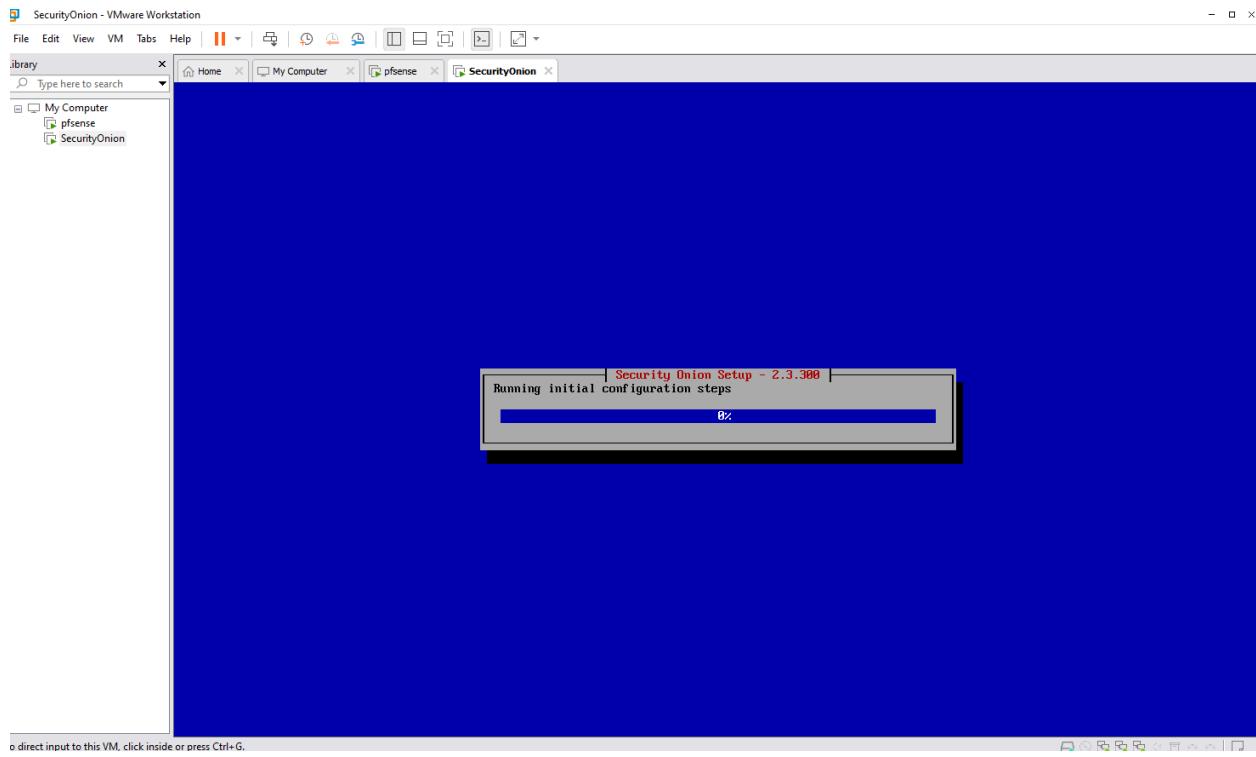
-The following is the installation progress(9 images)



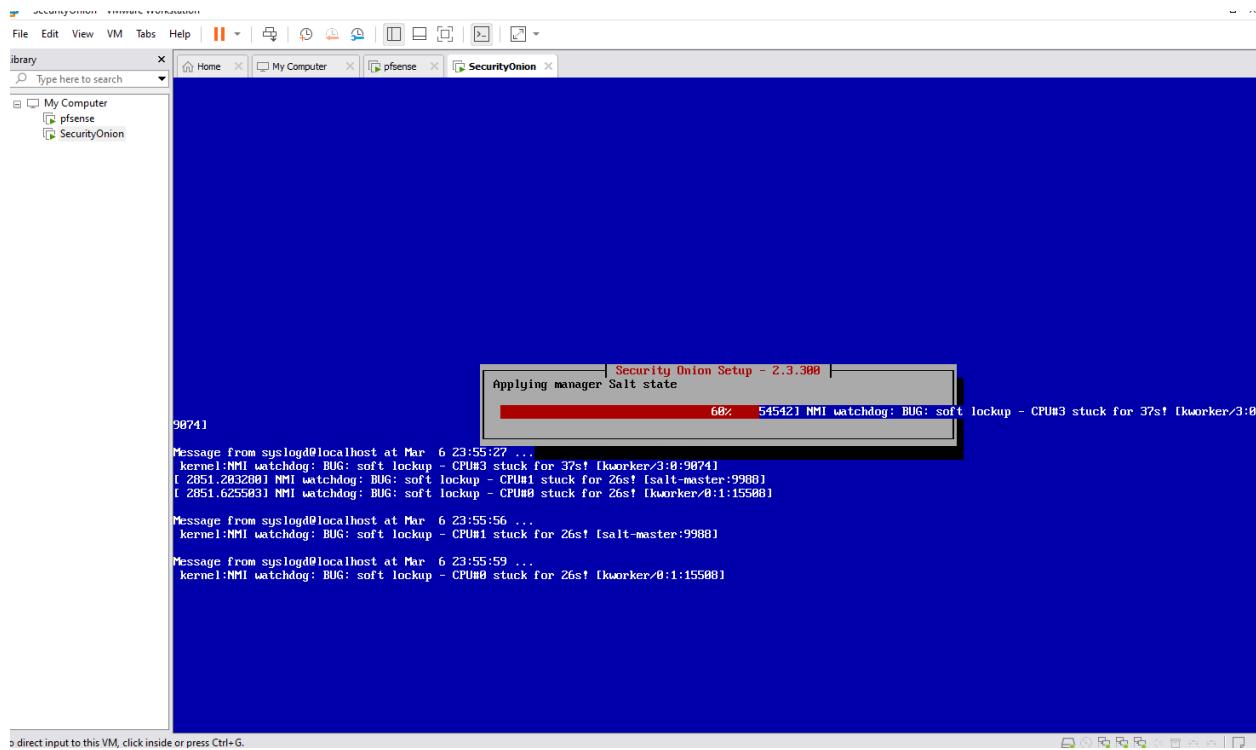




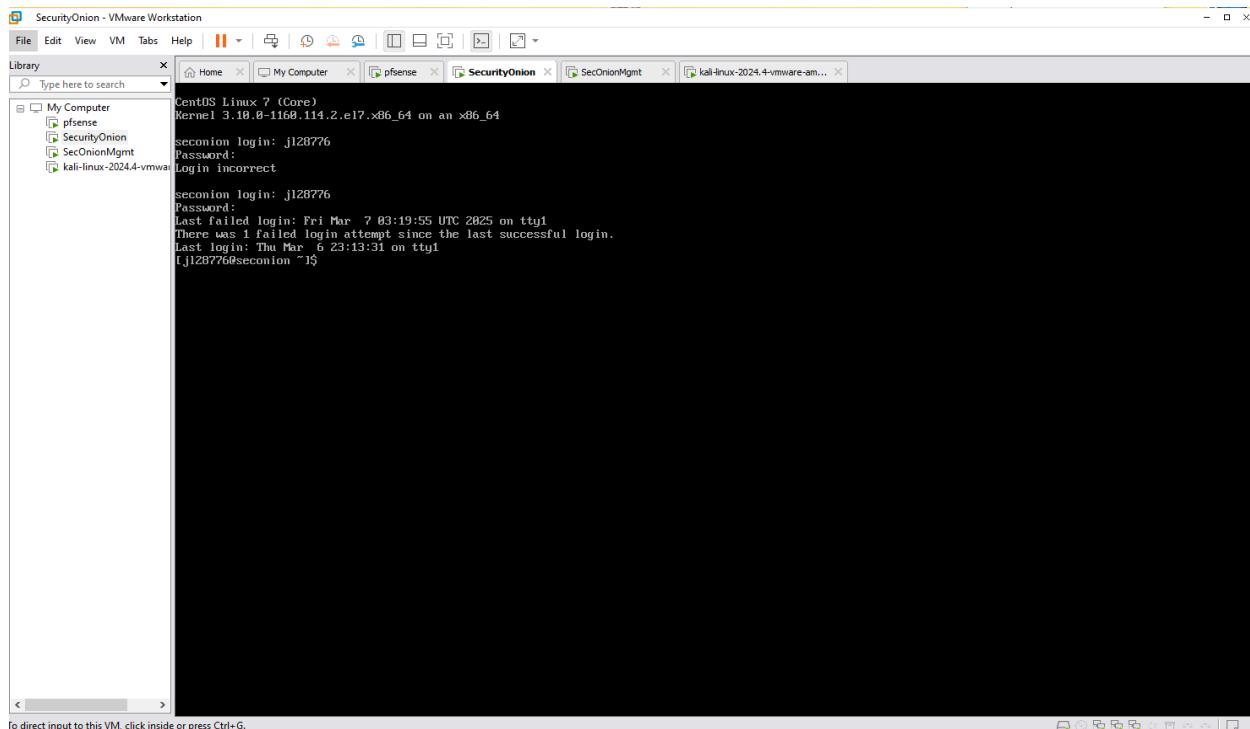




-This took around 1 hour



-After installation and rebooting we can login into seconion. Now we will need to configure ubuntu to allow the connection together and grab it's ip address



-Now we will add ubuntu as a VM host

ubuntu.com/download/desktop/thank-you?version=24.04.2&architecture=amd64&its=true

Canonical Ubuntu Products Use cases Support Community Download Ubuntu All Canonical Sign in

Downloads Desktop Server Core Cloud

# Thank you for downloading Ubuntu Desktop 24.04.2 LTS

Your download should start automatically. If it doesn't, [download now](#). You can [verify your download](#), or get help on [installing](#).

Sign up for our newsletter

Get the latest Ubuntu news and updates in your inbox.

Email\*:

How do you plan to use Ubuntu Desktop?

Work  Education  Personal use

I agree to receive information about Canonical's products and services.

By submitting this form, I confirm that I have read and agree to [Canonical's Privacy Notice](#) and [Privacy Policy](#).

[Subscribe now](#)

---

**RESOURCES**

[Install Ubuntu Desktop](#)  
Follow this tutorial to install Ubuntu Desktop on your laptop or PC.  
You can also run Ubuntu from a USB to try it without installing.

[How to run Ubuntu Desktop on a virtual machine using VirtualBox](#)  
Run Ubuntu Desktop using VirtualBox. A quick start guide that will work across any operating system.

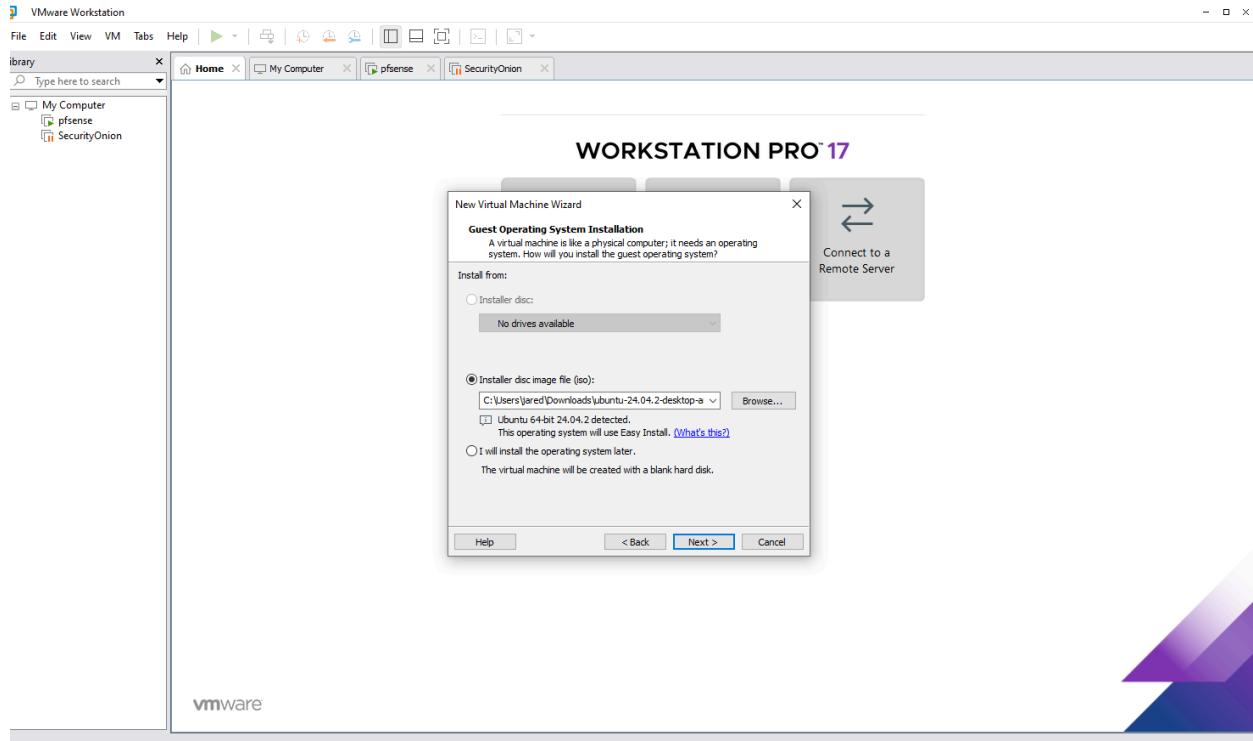
[Install Ubuntu Desktop on Raspberry Pi](#)  
Use the Raspberry Pi Imager or install Ubuntu manually. Ubuntu LTS releases are certified on select Raspberry Pi hardware.

---

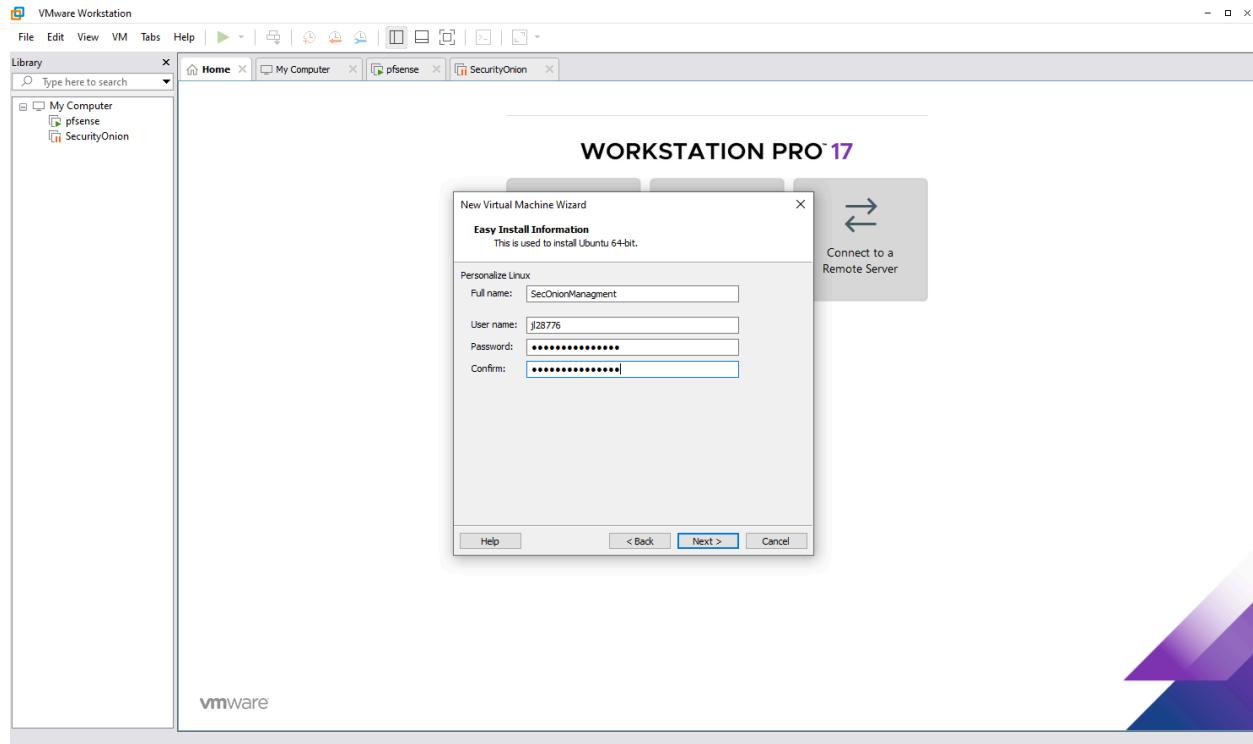
**HELP IS ALWAYS AT HAND**

[Ubuntu documentation](#)  
[Ubuntu Discourse](#)  
[Ask Ubuntu](#)  
[Launchpad Answers](#)

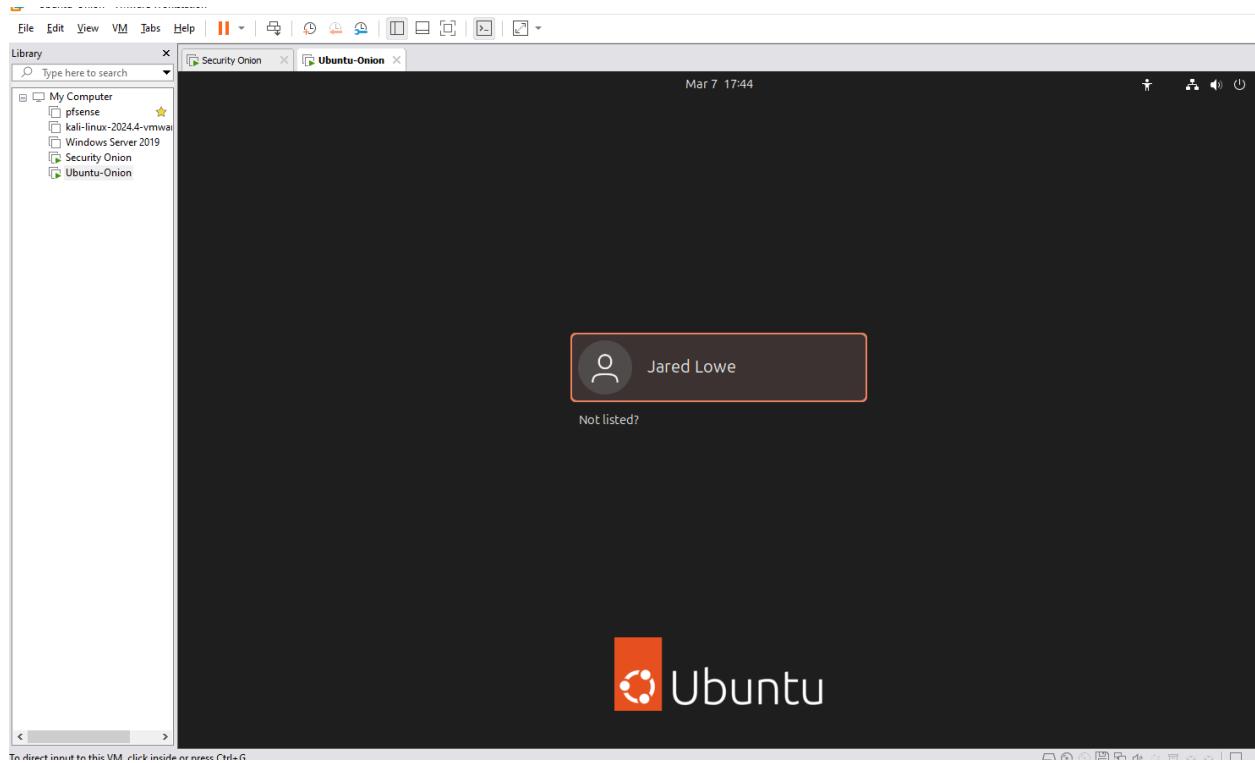
-Installing the disc image file (iso)



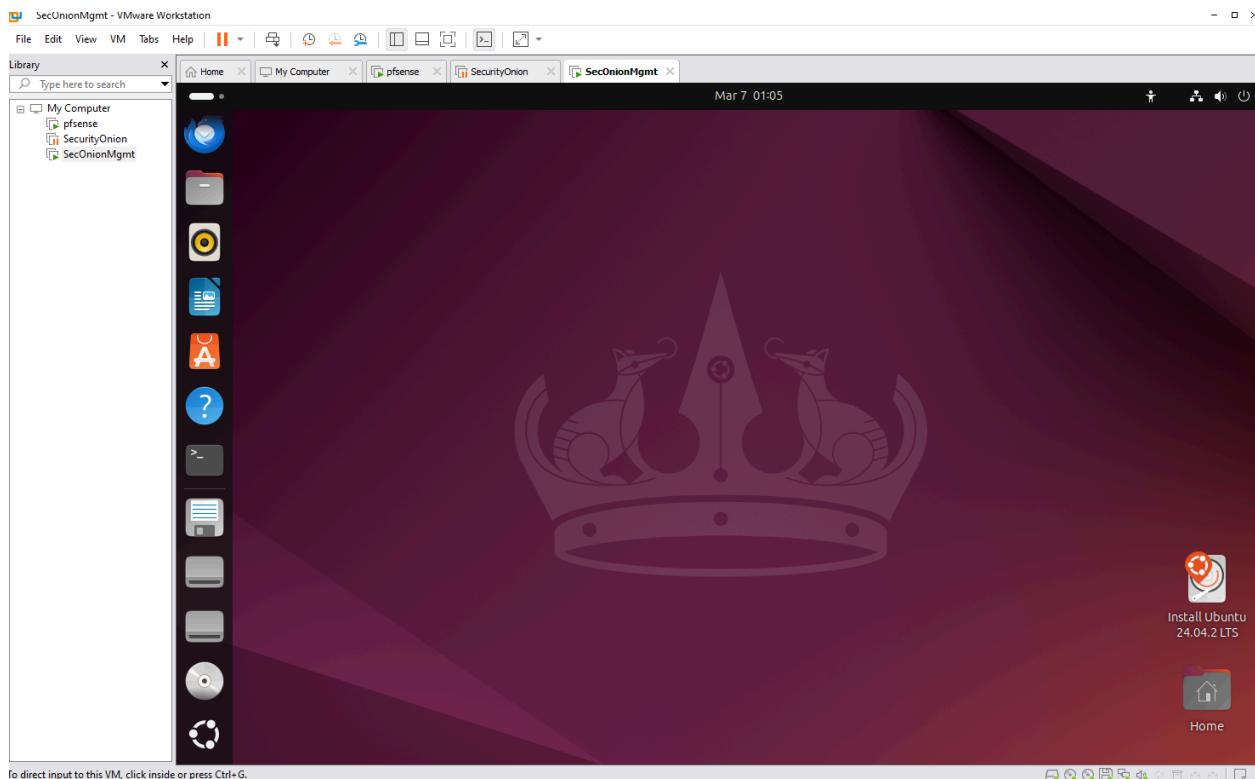
-Going to initialize it with the security onion so I named it SecOnionManagement and gave it a username and password. Also why we do not add any other configurations



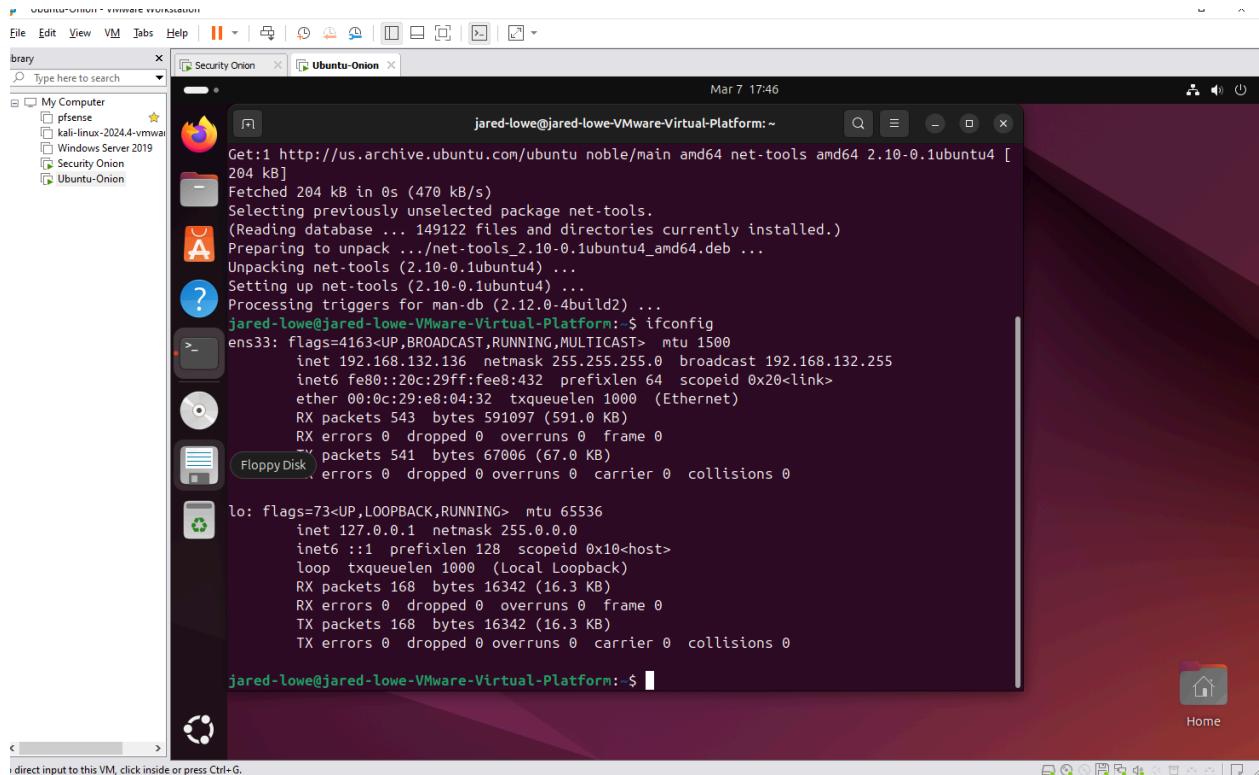
-after default set up we get access to the ubuntu login



-Now entering the Ubuntu VM



-I used install net tool to be able to use ifconfig and get the ip address for future use



-After 2nd attempt we added the ubuntu vm to the analyst role

SecurityOnion - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

Home My Computer pfSense SecurityOnion SecOnionMgmt kali-linux-2024-4-vmware-am...

ji120776@seconion ~ \$ sudo so-allow

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

##1) Respect the privacy of others.  
##2) Think before you type.  
##3) With great power comes great responsibility.

[sudo] password for ji120776:

Choose the role for the IP or Range you would like to allow

(a) - Analyst - 80/tcp, 443/tcp  
(b) - Logstash Beat - 5444/tcp  
(c) - Elasticsearch REST API - 9200/tcp  
(f1) - Strelka frontend - 57314/tcp  
(o) - Osquery endpoint - 8090/tcp  
(s1) - Syslog device - 514/tcp/udp  
(w) - Wazuh agent - 1514/tcp/udp  
(p1) - Wazuh API - 55000/tcp  
(r) - Wazuh registration service - 1515/tcp

Please enter your selection: a

Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.132.131

Adding 192.168.132.131 to the analyst role. This can take a few seconds...

Failed to add whitelist entry for 192.168.132.131 from /nsm/wazuh/etc/ossec.conf

[Errno 2] No such file or directory: '/nsm/wazuh/etc/ossec.conf'

ji120776@seconion ~ \$ sudo so-allow

[sudo] password for ji120776:

Choose the role for the IP or Range you would like to allow

(a) - Analyst - 80/tcp, 443/tcp  
(b) - Logstash Beat - 5444/tcp  
(c) - Elasticsearch REST API - 9200/tcp  
(f1) - Strelka frontend - 57314/tcp  
(o) - Osquery endpoint - 8090/tcp  
(s1) - Syslog device - 514/tcp/udp  
(w) - Wazuh agent - 1514/tcp/udp  
(p1) - Wazuh API - 55000/tcp  
(r) - Wazuh registration service - 1515/tcp

Please enter your selection: a

Enter a single ip address or range to allow (ex: 10.10.10.10 or 10.10.0.0/16): 192.168.132.131

Adding 192.168.132.131 to the analyst role. This can take a few seconds...

Already exists

ji120776@seconion ~ \$

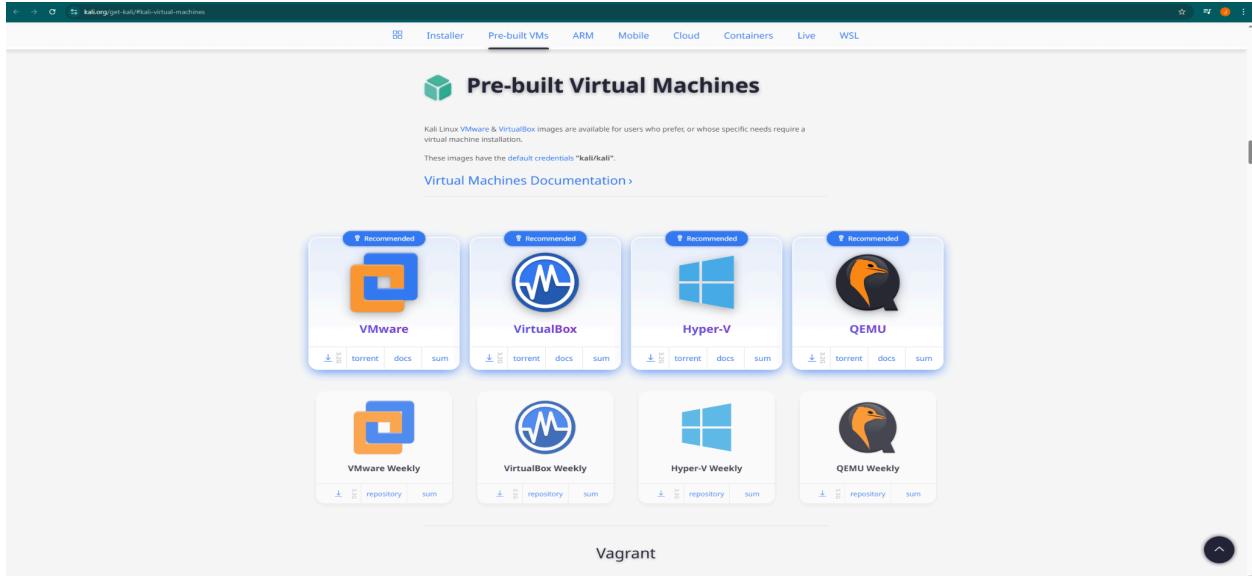
To direct input to this VM, click inside or press **Ctrl+G**.

NOTE:I WAS UNABLE TO ACCESS THE UBUNTU THROUGH <http://192.168.132.137> ON UBUNTU BUT SET PINGS FROM BOTH THE ONION AND UBUNTU SO IT CAN BE REACHED BUT AFTER A WEEK TRYING TO FIGURE IT OUT I GOT THIS AND THEN I WILL EVENTUALLY FIX IT(2 IMAGES SHOWING PING)

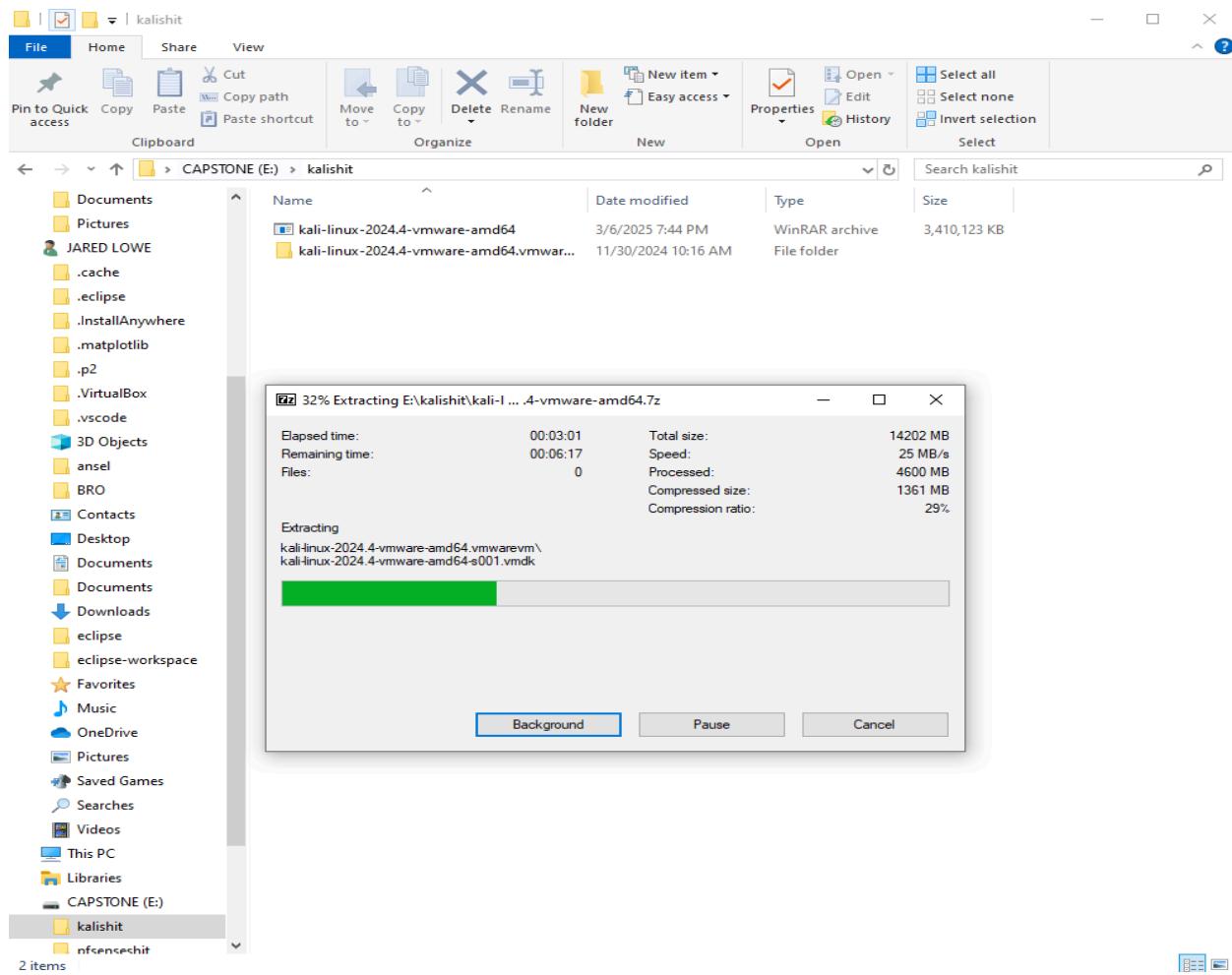
```
jared-lowe@jared-lowे-VMware-Virtual-Platform:~$ ping 192.168.132.137
PING 192.168.132.137 (192.168.132.137) 56(84) bytes of data.
64 bytes from 192.168.132.137: icmp_seq=1 ttl=64 time=0.289 ms
64 bytes from 192.168.132.137: icmp_seq=2 ttl=64 time=0.284 ms
64 bytes from 192.168.132.137: icmp_seq=3 ttl=64 time=0.278 ms
64 bytes from 192.168.132.137: icmp_seq=4 ttl=64 time=0.295 ms
64 bytes from 192.168.132.137: icmp_seq=5 ttl=64 time=0.288 ms
64 bytes from 192.168.132.137: icmp_seq=6 ttl=64 time=0.279 ms
64 bytes from 192.168.132.137: icmp_seq=7 ttl=64 time=0.287 ms
64 bytes from 192.168.132.137: icmp_seq=8 ttl=64 time=0.303 ms
64 bytes from 192.168.132.137: icmp_seq=9 ttl=64 time=1.03 ms
64 bytes from 192.168.132.137: icmp_seq=10 ttl=64 time=0.297 ms
64 bytes from 192.168.132.137: icmp_seq=11 ttl=64 time=0.288 ms
^C
--- 192.168.132.137 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10221ms
rtt min/avg/max/mdev = 0.278/0.356/1.032/0.213 ms
jared-lowe@jared-lowे-VMware-Virtual-Platform:~$
```

```
[j128776@secononj1 ~]$ ping 192.168.132.136
PING 192.168.132.136 (192.168.132.136) 56(84) bytes of data.
64 bytes from 192.168.132.136: icmp_seq=1 ttl=64 time=593 ms
64 bytes from 192.168.132.136: icmp_seq=2 ttl=64 time=1258 ms
64 bytes from 192.168.132.136: icmp_seq=3 ttl=64 time=251 ms
64 bytes from 192.168.132.136: icmp_seq=4 ttl=64 time=1956 ms
64 bytes from 192.168.132.136: icmp_seq=5 ttl=64 time=955 ms
64 bytes from 192.168.132.136: icmp_seq=6 ttl=64 time=674 ms
^64 bytes from 192.168.132.136: icmp_seq=7 ttl=64 time=3117 ms
64 bytes from 192.168.132.136: icmp_seq=8 ttl=64 time=2117 ms
64 bytes from 192.168.132.136: icmp_seq=9 ttl=64 time=1117 ms
64 bytes from 192.168.132.136: icmp_seq=10 ttl=64 time=117 ms
^64 bytes from 192.168.132.136: icmp_seq=11 ttl=64 time=366 ms
stop
64 bytes from 192.168.132.136: icmp_seq=12 ttl=64 time=1988 ms
64 bytes from 192.168.132.136: icmp_seq=13 ttl=64 time=980 ms
quit
64 bytes from 192.168.132.136: icmp_seq=14 ttl=64 time=887 ms
64 bytes from 192.168.132.136: icmp_seq=15 ttl=64 time=877 ms
64 bytes from 192.168.132.136: icmp_seq=16 ttl=64 time=887 ms
64 bytes from 192.168.132.136: icmp_seq=17 ttl=64 time=5979 ms
64 bytes from 192.168.132.136: icmp_seq=18 ttl=64 time=4879 ms
64 bytes from 192.168.132.136: icmp_seq=19 ttl=64 time=3878 ms
64 bytes from 192.168.132.136: icmp_seq=20 ttl=64 time=2871 ms
64 bytes from 192.168.132.136: icmp_seq=21 ttl=64 time=1878 ms
64 bytes from 192.168.132.136: icmp_seq=22 ttl=64 time=78.9 ms
64 bytes from 192.168.132.136: icmp_seq=23 ttl=64 time=304 ms
64 bytes from 192.168.132.136: icmp_seq=24 ttl=64 time=306 ms
64 bytes from 192.168.132.136: icmp_seq=25 ttl=64 time=1083 ms
64 bytes from 192.168.132.136: icmp_seq=26 ttl=64 time=83.0 ms
64 bytes from 192.168.132.136: icmp_seq=27 ttl=64 time=530 ms
64 bytes from 192.168.132.136: icmp_seq=28 ttl=64 time=3839 ms
64 bytes from 192.168.132.136: icmp_seq=29 ttl=64 time=2848 ms
64 bytes from 192.168.132.136: icmp_seq=30 ttl=64 time=1040 ms
64 bytes from 192.168.132.136: icmp_seq=31 ttl=64 time=48.0 ms
^C
--- 192.168.132.136 ping statistics ---
36 packets transmitted, 31 received, 13% packet loss, time 35013ms
rtt min/avg/max/mdev = 48.034/2181.724/8870.020/2845.465 ms, pipe 9
[j128776@secononj1 ~]$
```

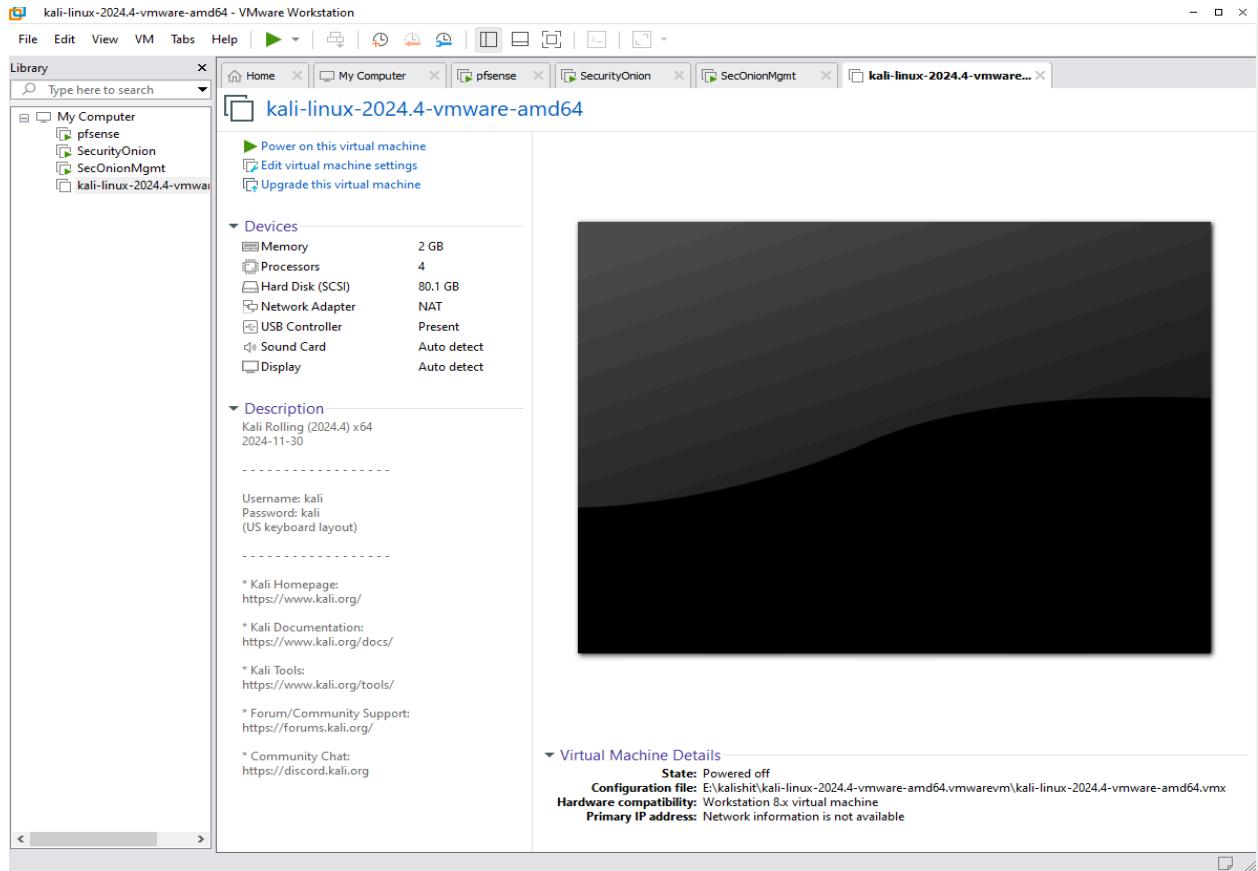
-Now we are going to add the attack machine which is Linux



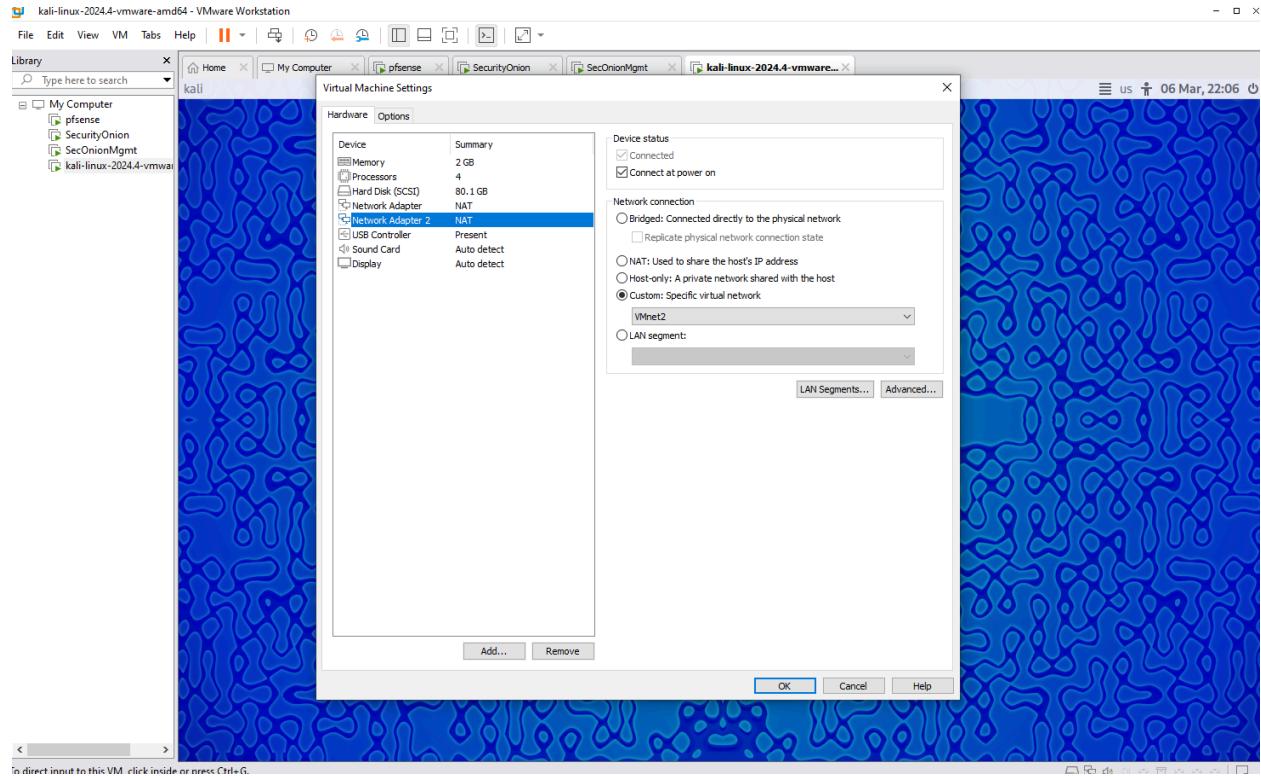
### -Unzipping the file



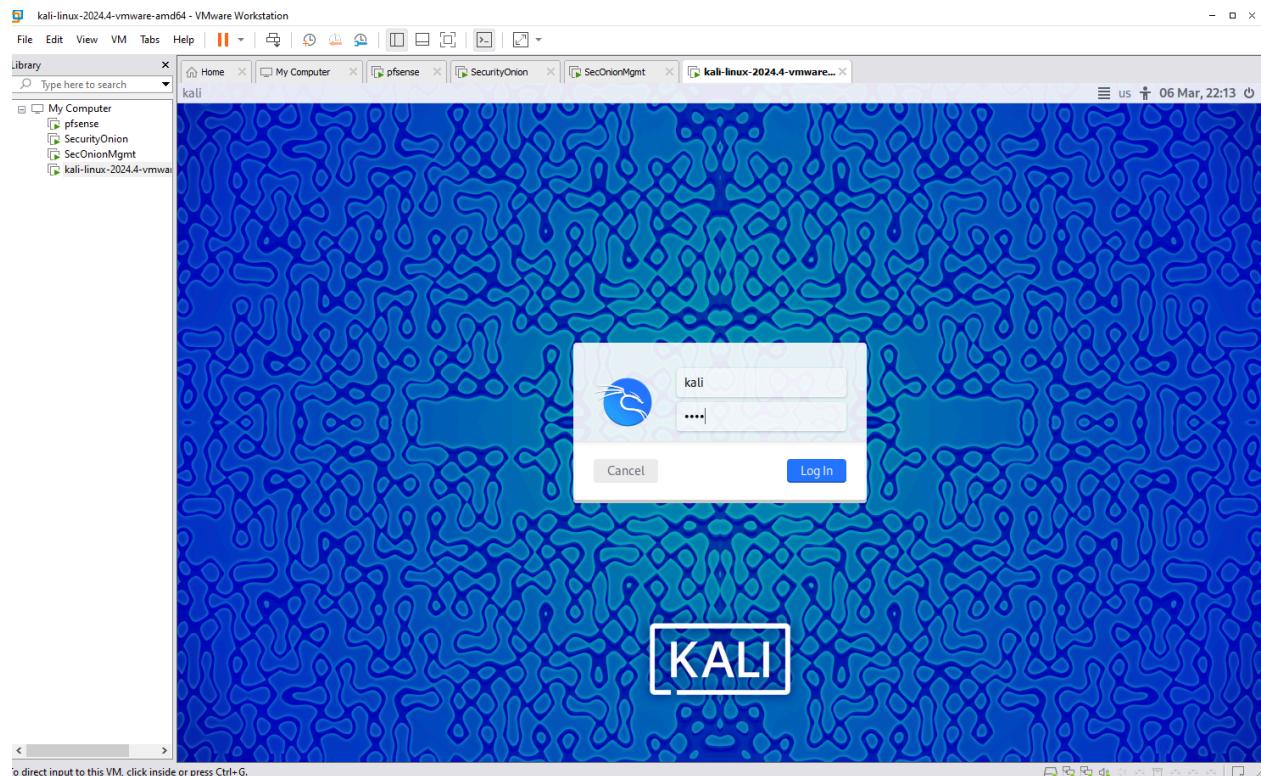
-Instead I used open a virtual machine and find the Kali-Linux disc file and open to immediately get the VM



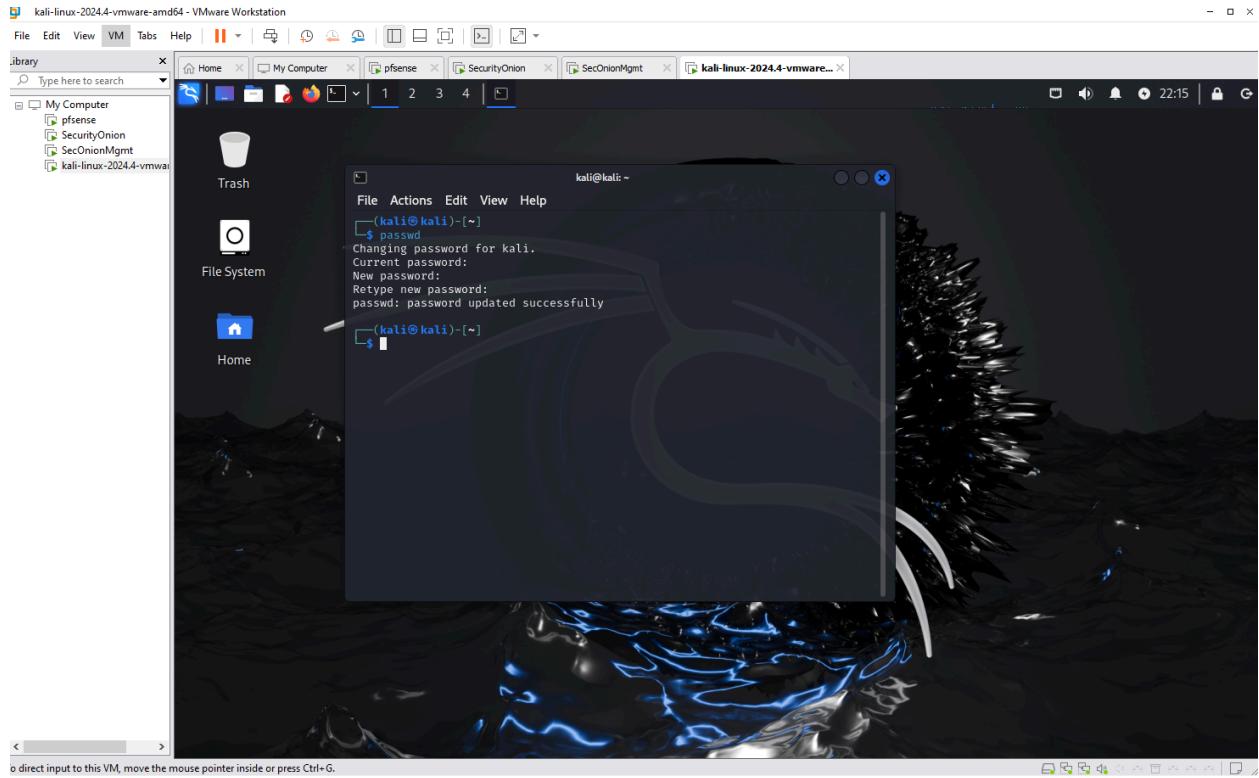
-Adding a new network adapter that has vmnet2 network



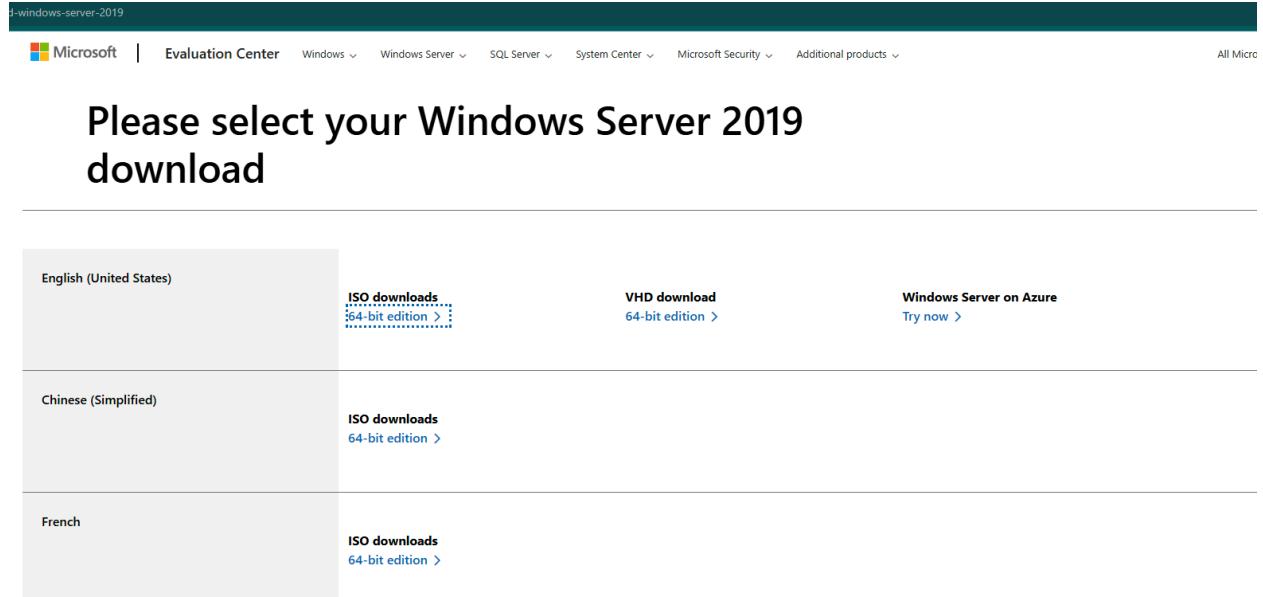
-Now can access it



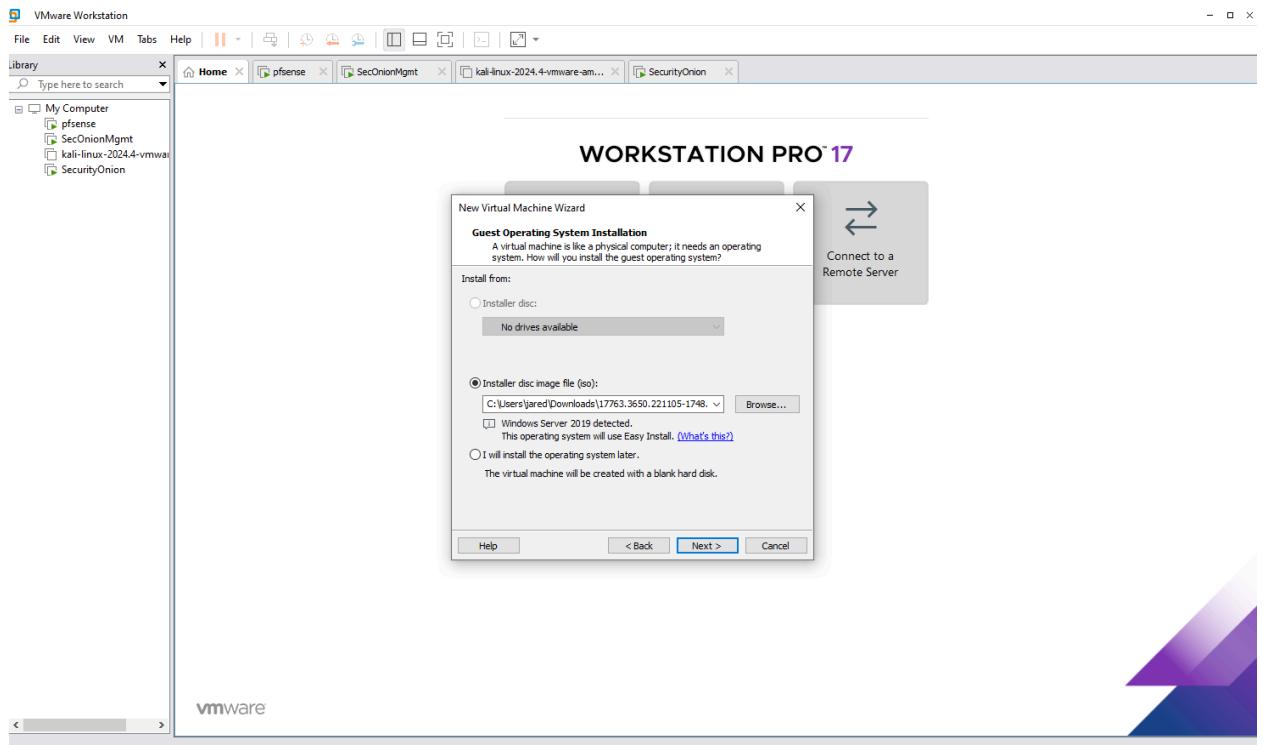
-Now creating a unique password. This is all for this installation because we will soon use this to attack systems and also change pfSense settings.



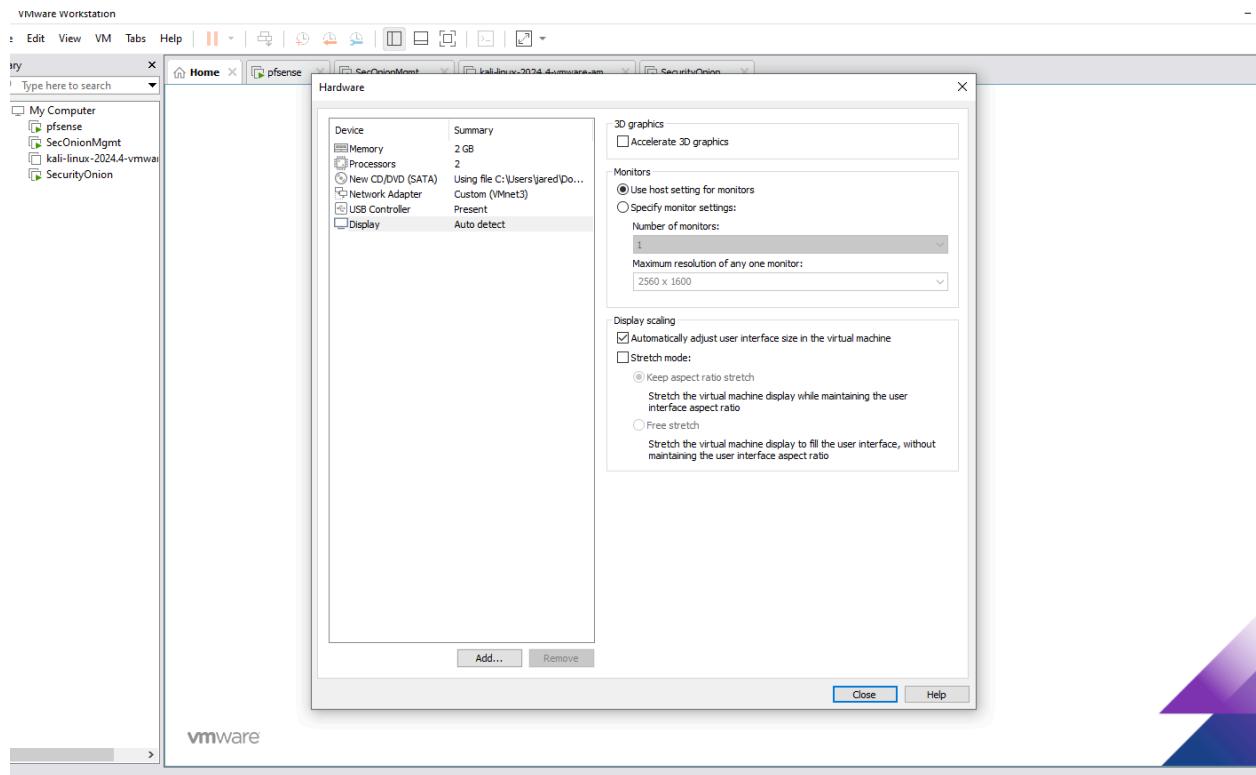
-Now we are going to add a windows VM



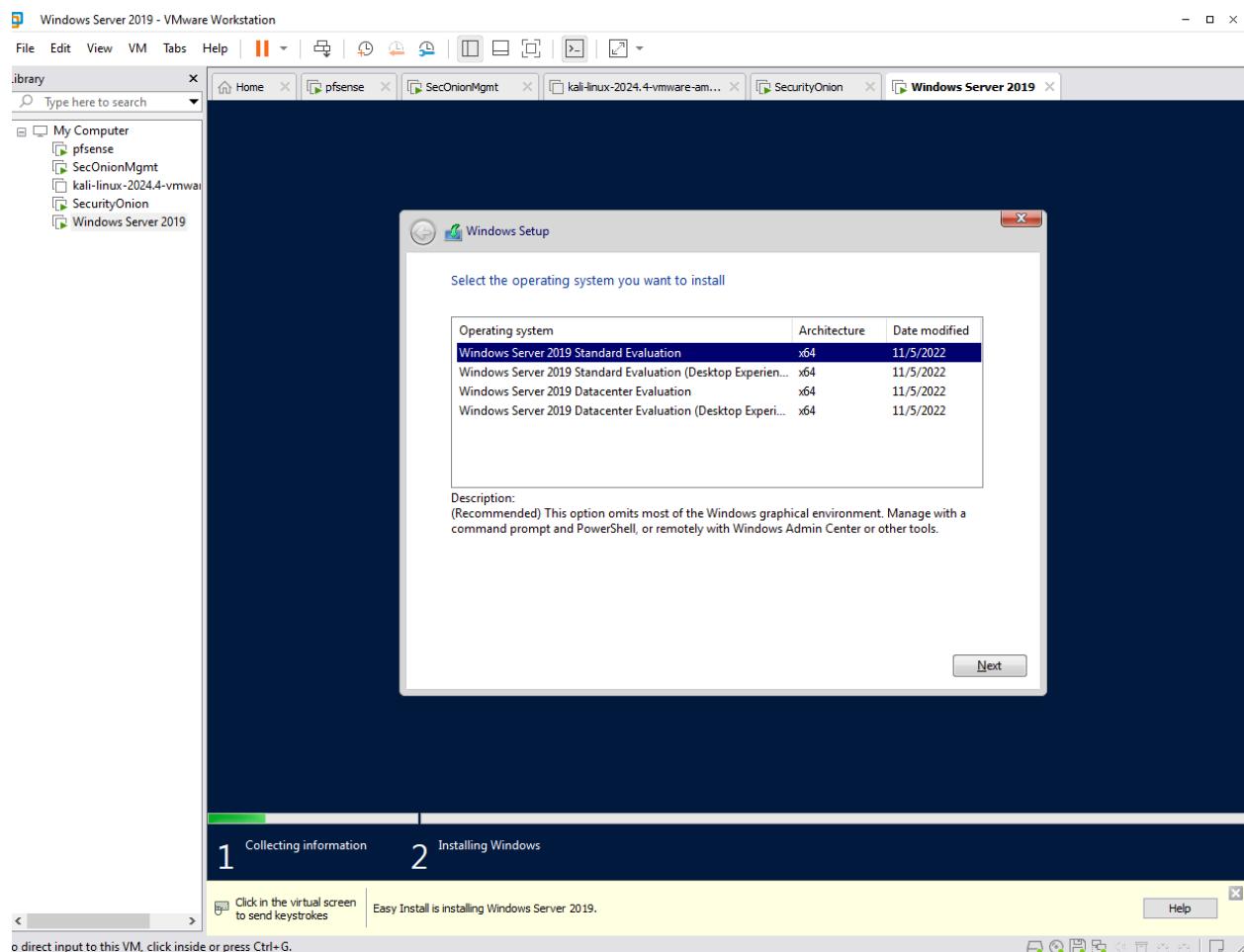
-Adding the windows server as a VM



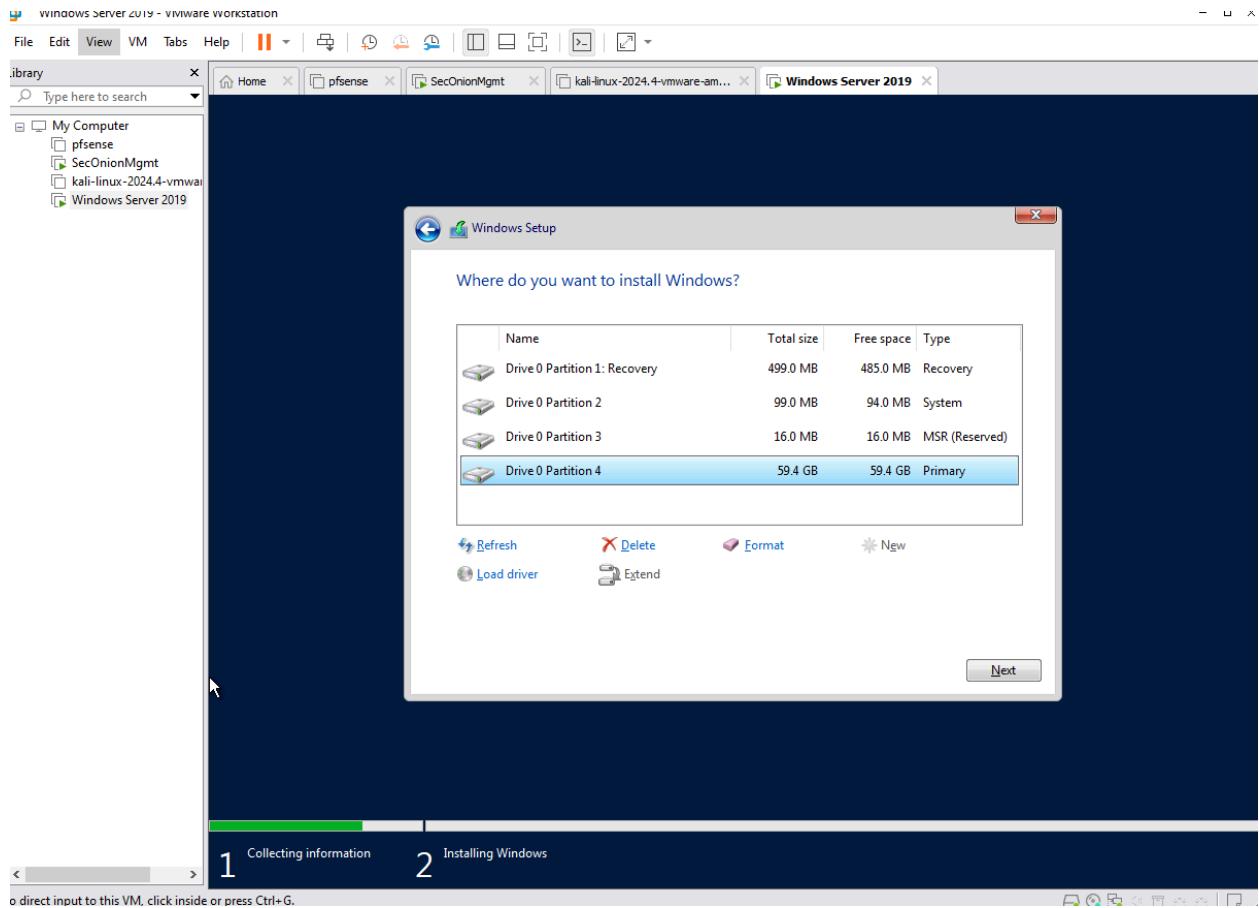
-Keeping default expect changing the network adapter to our vmnet3



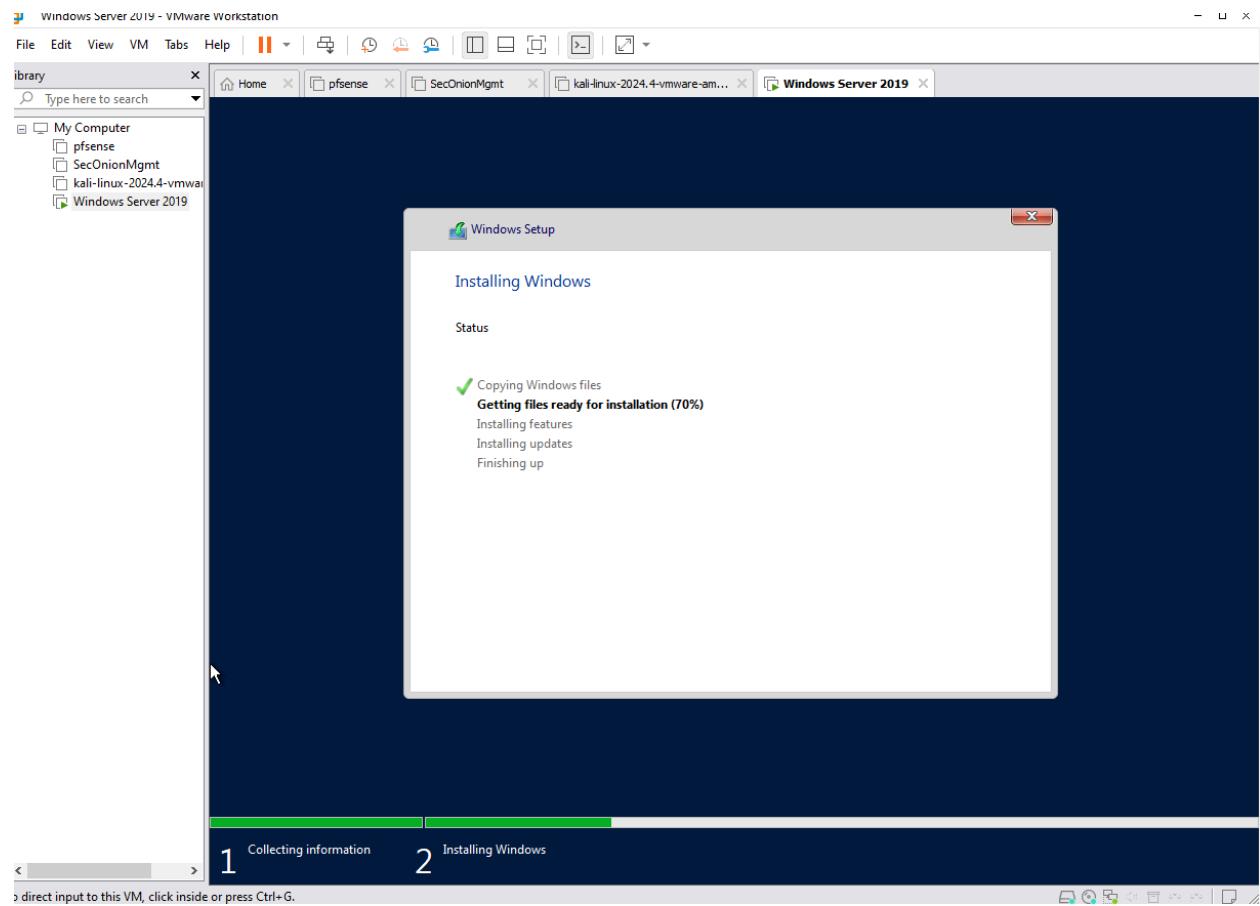
-Entering the windows server selecting the second option



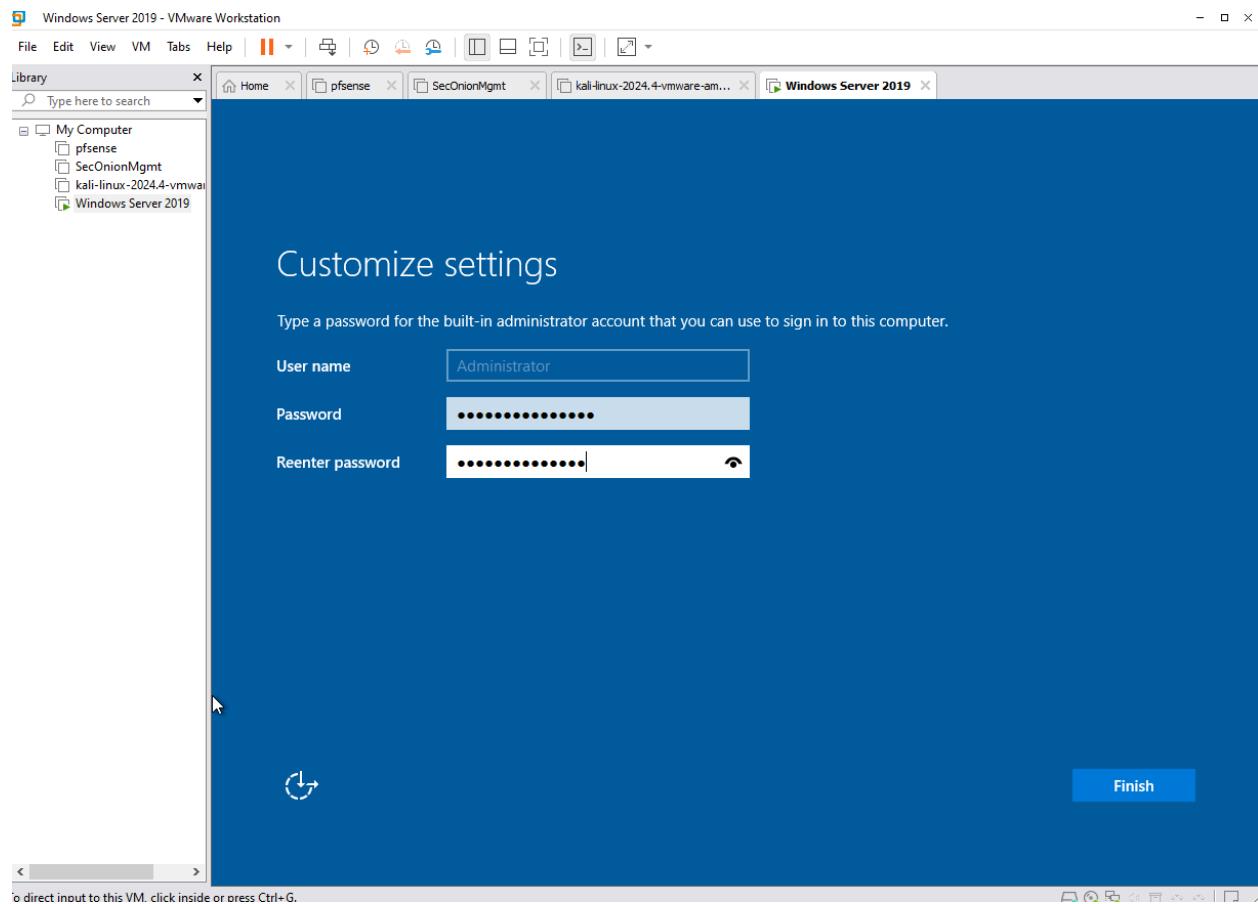
-Now we have created a new custom installation



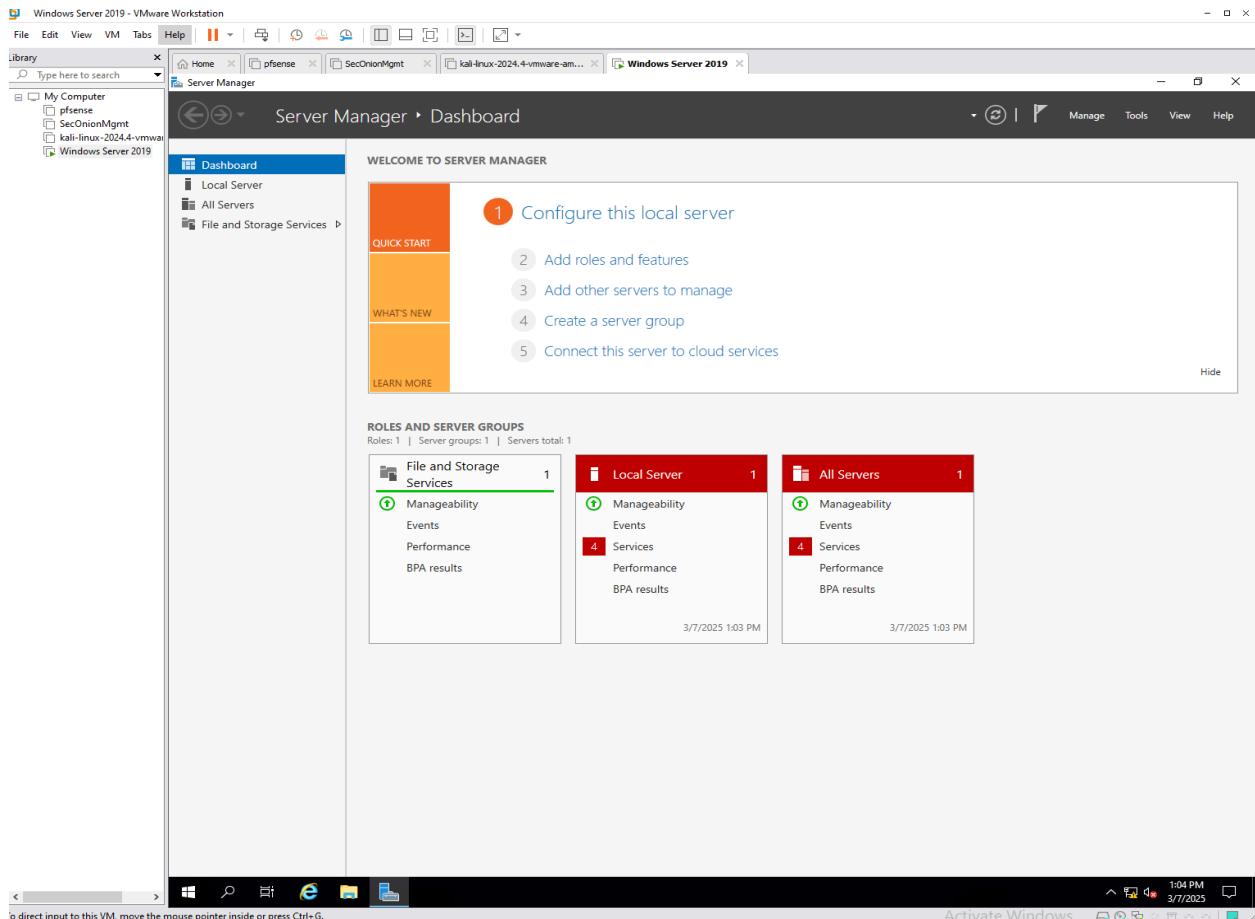
-Waiting for installation of windows



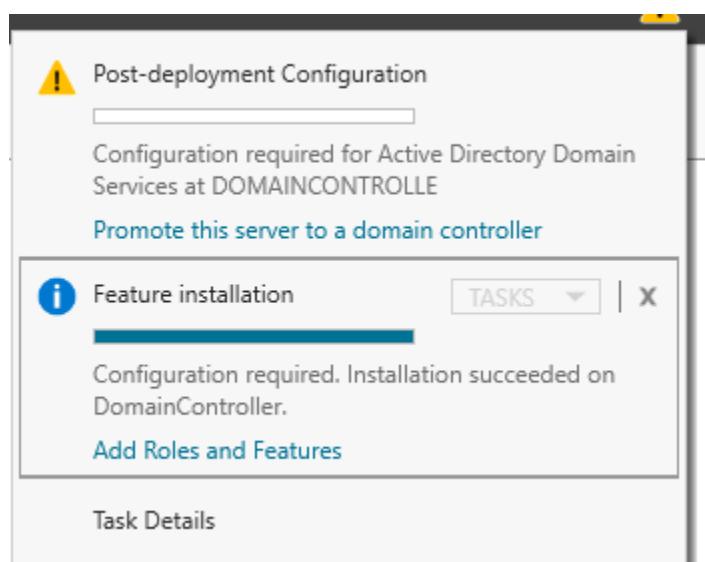
## -Creating a new password



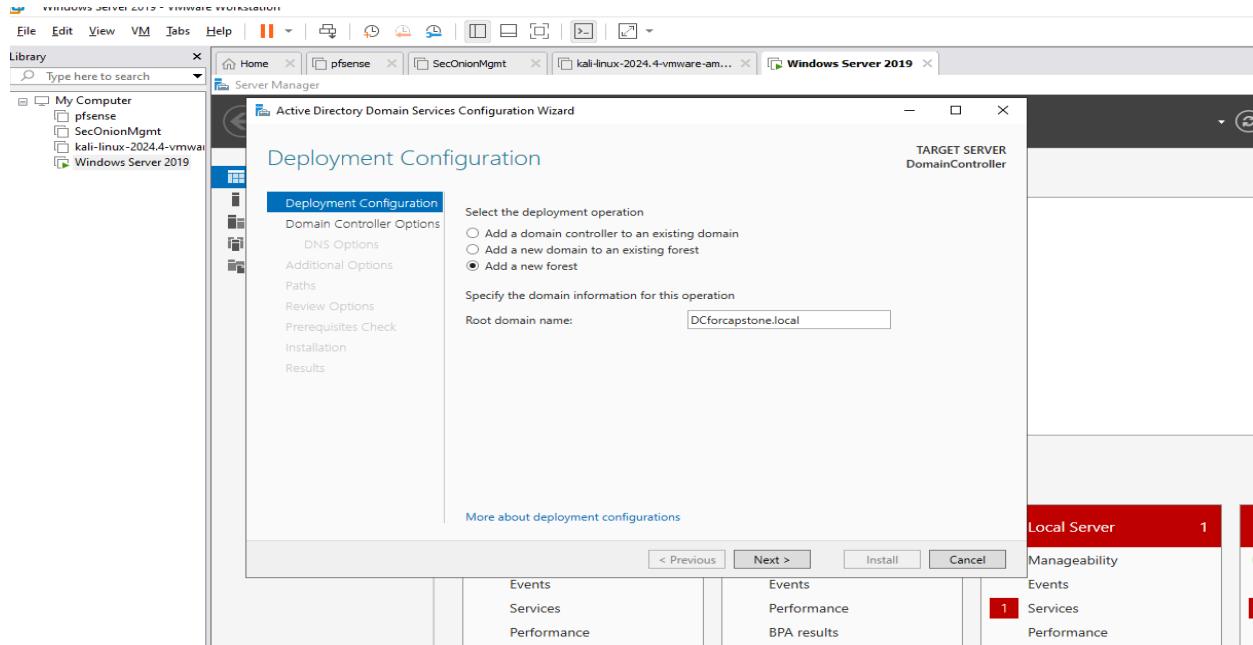
-After entering the password we are sent to the server manager dashboard



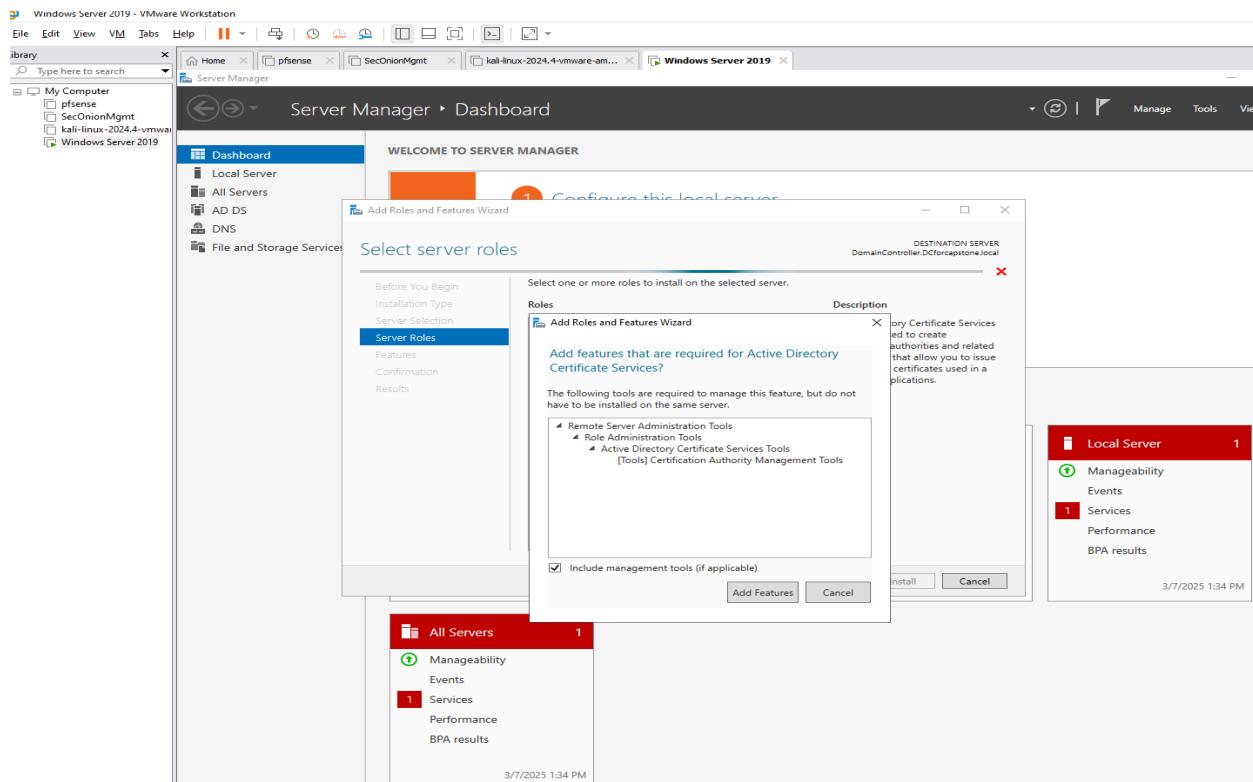
-Going to manage then add roles and features to then add the active directory domain service roles. Then we get a flag to add the server to domain controller



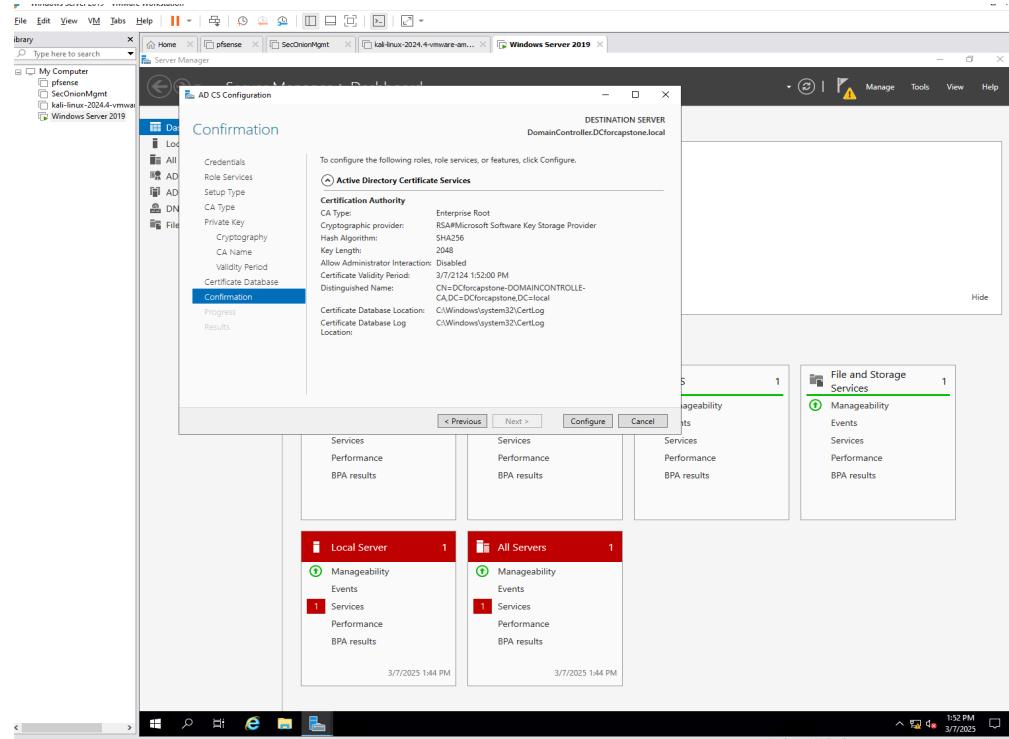
-We can now add the domain controller with a root name and password. We will then install and wait for the reboot



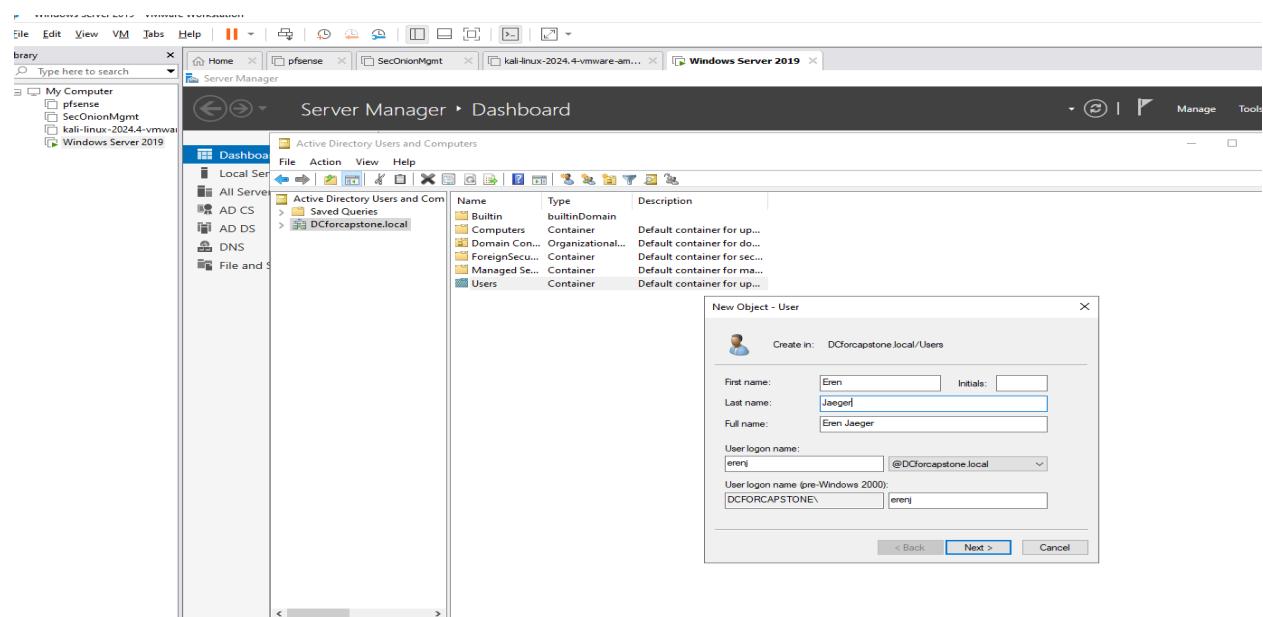
-we will now add the active directory certificate service to the server roles



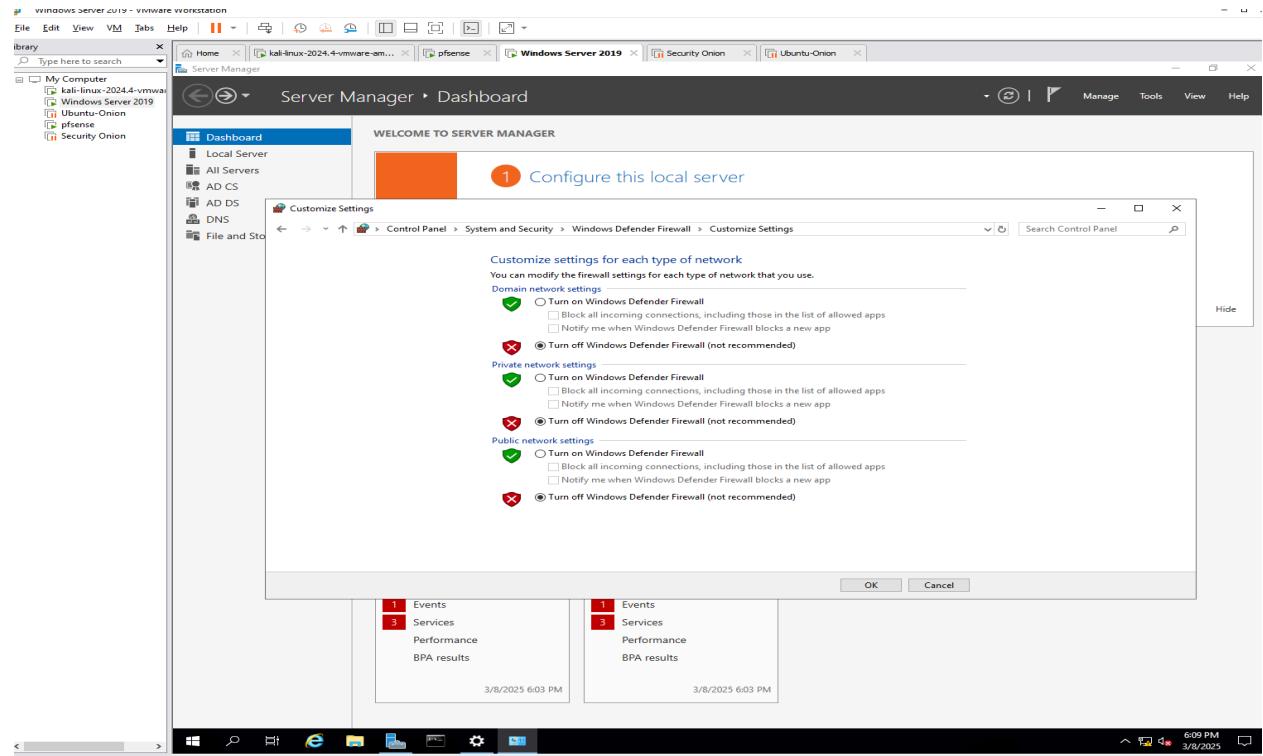
-We then enter the flag for the certificate services and enter credentials to establish the certificate. Then after restarting it to initialize the change.



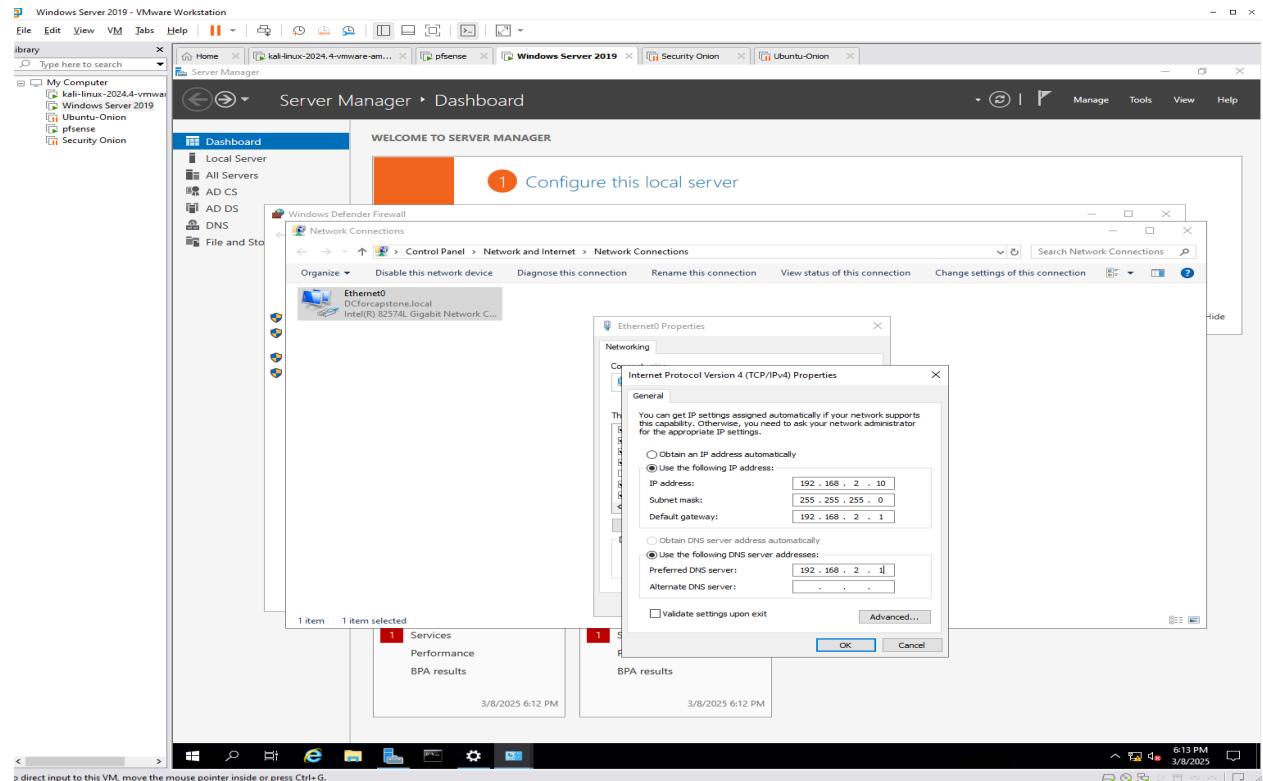
-Entering Tools-DC-Users-to create a new user called Eren Jaeger and creating a password



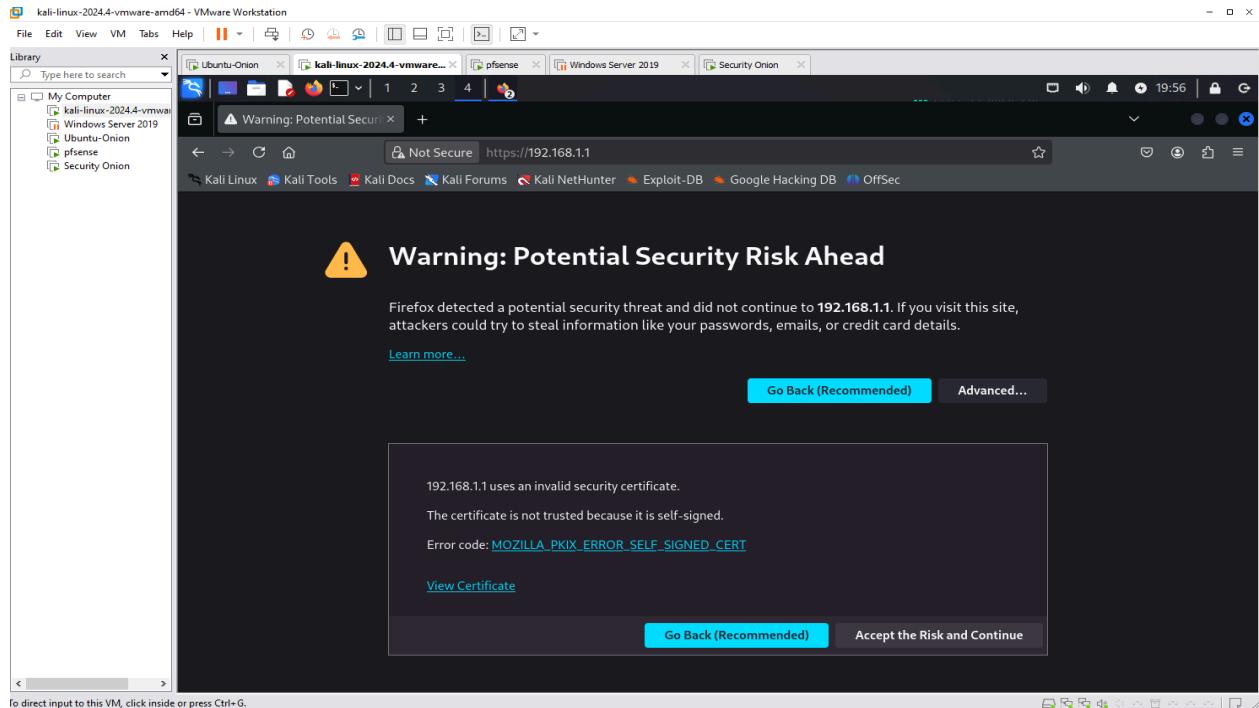
-Since a lab environment we will turn off the windows firewall



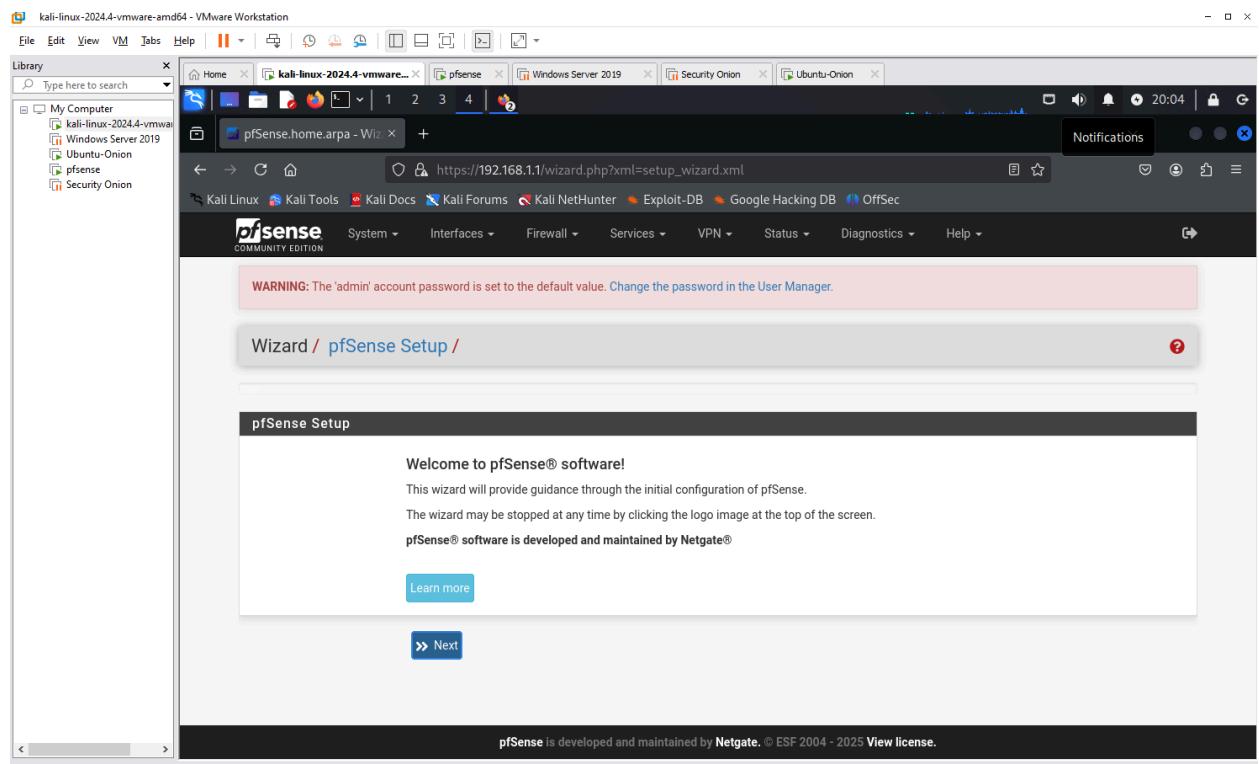
-Entering the control panel to create the TCP/IP properties



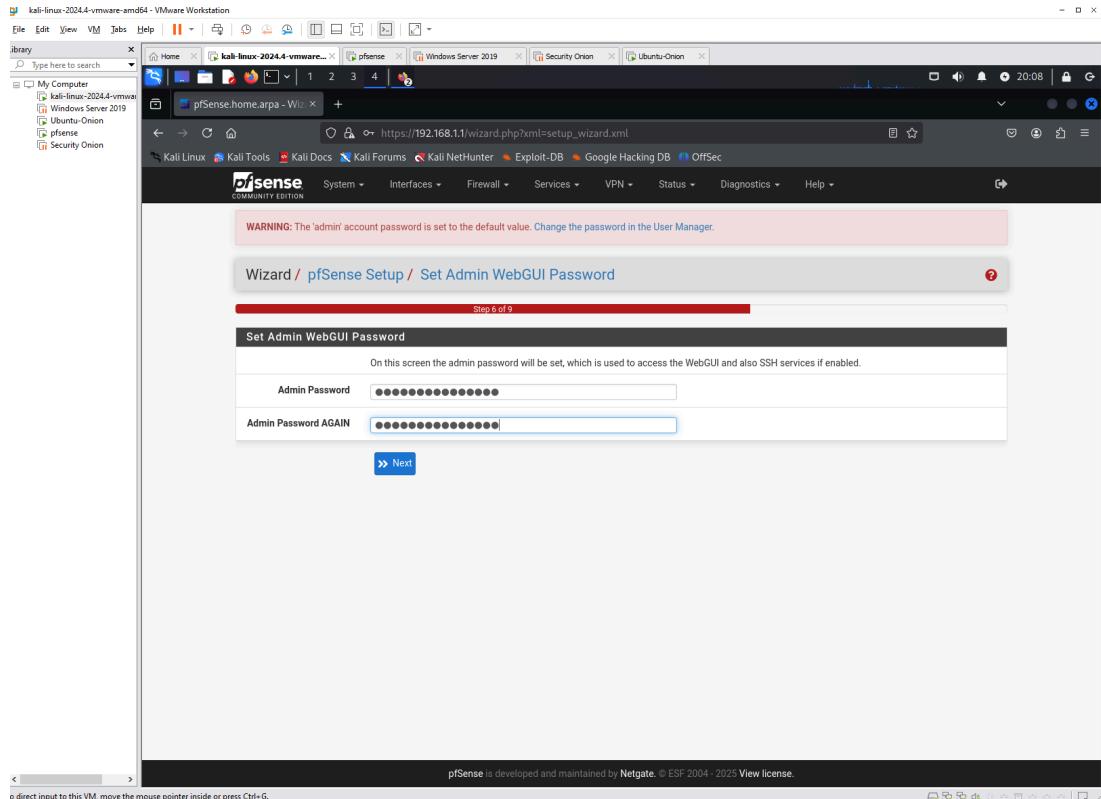
-Now we will move to pfSense settings with Kali by logging in and opening Firefox and entering the IP address: 192.168.1.1 that we configured on our pfSense and accepting the risk and continuing.



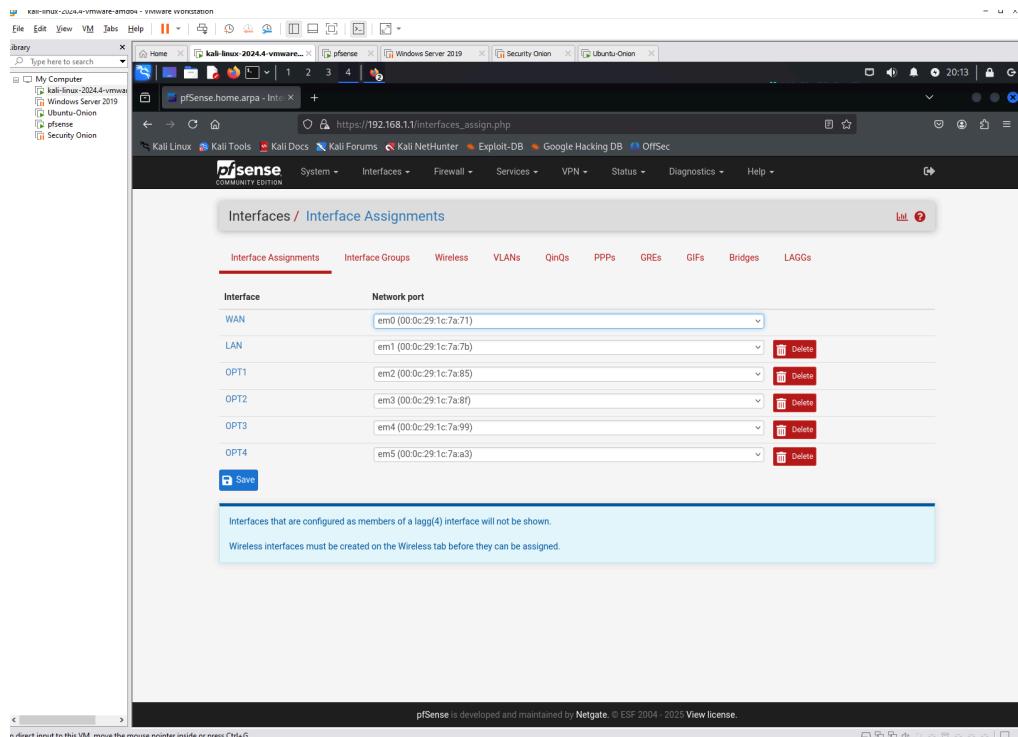
-Entering the username and password to access the setup



-Following the setup with accepting the defaults/only option on clicking next til entering new password and it will reload



-Now we are going to configure the interfaces



-First I changed the LAN to Kali and checked to make sure the ip address was correct

The changes have been applied successfully.

### General Configuration

Enable

Description: Kali

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: XXXX-XXXX-XXXX

MTU: (Blank)

MSS: (Blank)

Speed and Duplex: Default (no preference, typically autoselect)

### Static IPv4 Configuration

IPv4 Address: 192.168.1.1

IPv4 Upstream gateway: None

+ Add a new gateway

-Changed opt1 interface to Victim network again checking the ip was correct

The changes have been applied successfully.

### General Configuration

Enable

Description: VictimNetwork

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: DHCP6

MAC Address: XXXX-XXXX-XXXX

MTU: (Blank)

MSS: (Blank)

Speed and Duplex: Default (no preference, typically autoselect)

### Static IPv4 Configuration

IPv4 Address: 192.168.2.1

IPv4 Upstream gateway: None

+ Add a new gateway

-Setting the opt2 interface to SecOnion again checking the ip was correct

The screenshot shows the pfSense web interface with the URL <https://192.168.1.1/interfaces.php?if=opt2>. The interface is named 'SecOnion' with a static IPv4 address of 192.168.3.1. The configuration includes an MTU of 1500 and an MSS of 60. The 'Speed and Duplex' dropdown is set to 'Default (no preference, typically autoselect)'. A note at the bottom states: 'If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.' A green message bar at the top says 'The changes have been applied successfully.'

-Since we didn't set ip for opt3 we have to enable the interface after naming it SpanPort

The screenshot shows the pfSense web interface with the URL <https://192.168.1.1/interfaces.php?if=opt3>. The interface is named 'SpanPort' with no IPv4 configuration. The configuration includes an MTU of 1500 and an MSS of 60. The 'Speed and Duplex' dropdown is set to 'Default (no preference, typically autoselect)'. A note at the bottom states: 'If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.' A green message bar at the top says 'The changes have been applied successfully.'

-Now opt4 will be named Splunk and checking the ip address

The changes have been applied successfully.

**General Configuration**

- Enable:  Enable interface
- Description: Splunk
- IPv4 Configuration Type: Static IPv4
- IPv6 Configuration Type: DHCP6
- MAC Address: XXXXXX-XXXXXX
- MTU: (If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.)
- MSS: (If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IP6 header size) will be in effect.)
- Speed and Duplex: Default (no preference, typically autoselect)

**Static IPv4 Configuration**

- IPv4 Address: 192.168.4.1
- IPv4 Upstream gateway: None
- + Add a new gateway

-Finalized assignments

Interface	Network port
WAN	em0 (00:0c:29:1c:7a:71)
Kali	em1 (00:0c:29:1c:7a:7b)
VictimNetwork	em2 (00:0c:29:1c:7a:85)
SecOnion	em3 (00:0c:29:1c:7a:8f)
SpanPort	em4 (00:0c:29:1c:7a:99)
Splunk	em5 (00:0c:29:1c:7a:a3)

**Interface Assignments**

Interfaces that are configured as members of a lagg(4) interface will not be shown.  
Wireless interfaces must be created on the Wireless tab before they can be assigned.

**pfSense** is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

-Now we are going to create the Bridge from the VictimNetwork and the SpanPort

The screenshot shows the pfSense web interface under the 'Interfaces / Bridges / Edit' section. The 'Member Interfaces' section contains 'WAN', 'KALI', 'VICTIMNETWORK', and 'SECIONON'. The 'Span Port' section contains 'VICTIMNETWORK', 'SECIONON', 'SPANPORT', and 'SPLIT'. The 'Edge Ports' section contains 'WAN', 'KALI', 'VICTIMNETWORK', and 'SECIONON'. The 'Auto Edge Ports' section contains 'WAN' and 'KALI'.

-Adding one rule to the WAN so we can get all alerts and logs from security onion

The screenshot shows the pfSense web interface under the 'Firewall / Rules / Edit' section. The 'Edit Firewall Rule' section has 'Action' set to 'Pass'. The 'Source' section has 'Source' set to 'Any'. The 'Destination' section has 'Destination' set to 'Any'. The 'Extra Options' section has 'Log' checked.

## Resources

Damon, Joseph. "Virtual Home Lab for Blue Team Security – Network Topology – Section 2." *Joseph Damon* |, 28 Aug. 2023,  
[josephhmdamon.com/virtual-home-lab-network-topology/](http://josephhmdamon.com/virtual-home-lab-network-topology/)

Day, Day. "Building a Cybersecurity Homelab for Detection & Monitoring." *Cyberwox Academy*, 8 Aug. 2022,  
[cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/](http://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/)

O'Brien, Gerard. "Gerard O'Brien." *YouTube*, YouTube, 15 Feb. 2023,  
[www.youtube.com/@gerardobrien](http://www.youtube.com/@gerardobrien)