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.

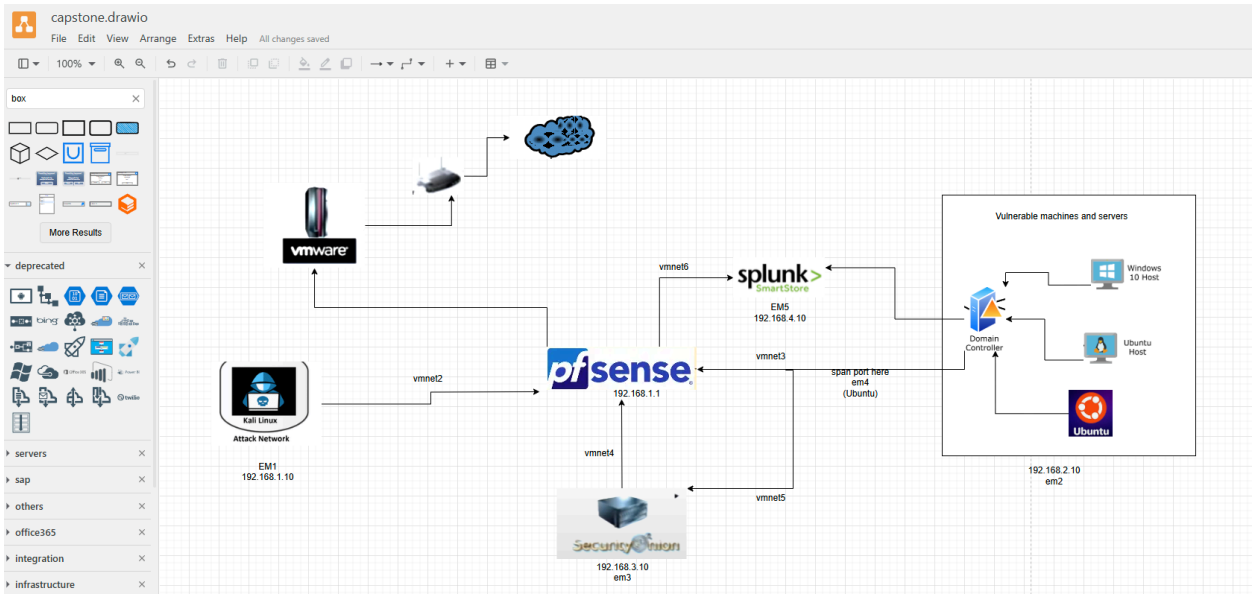
To continue, setting up Windows and Ubuntu to function with the network infrastructure was an intriguing and fun part of the project. These helped with connectivity, segmentation, and showed me how a virtual machine can interact within the network I built. It was at times tricky and hard to configure 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 fute use of the pfsense and anticipate the next steps.

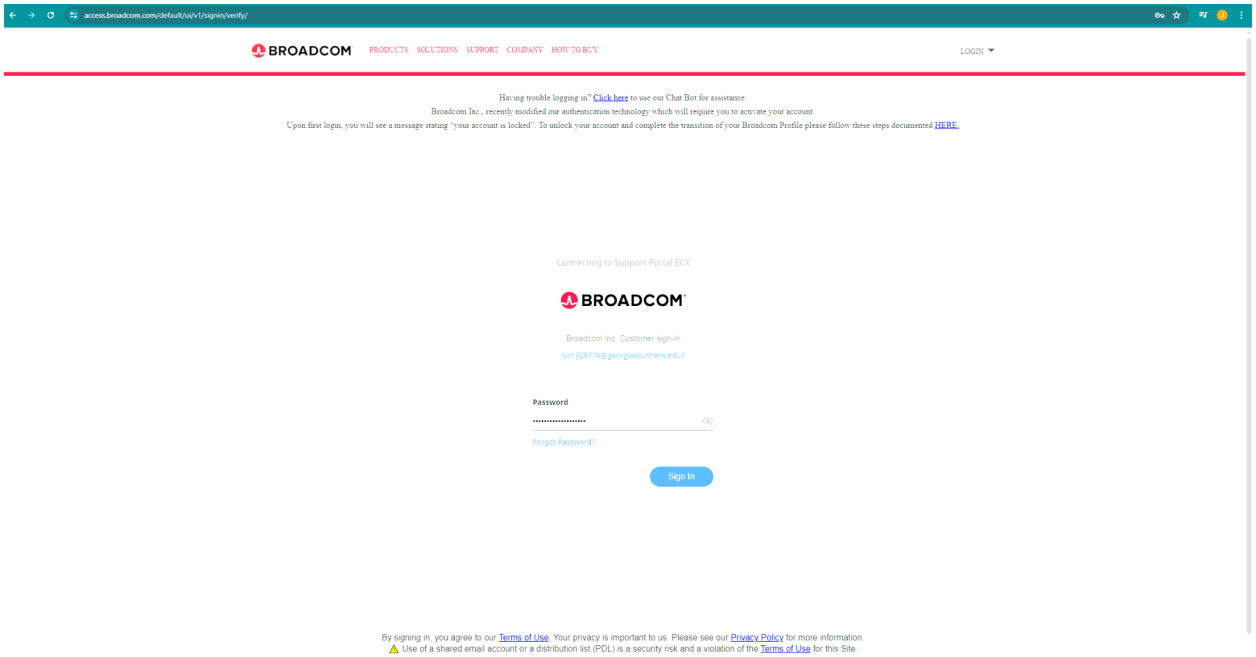
The images below serve as my evidence of work completed. I tried to make as many screenshots and tried to be thorough as possible without being too long. There were many times where I had to delete images to add a newer and better image. Hopefully my screenshots are clear and coincide to show you my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

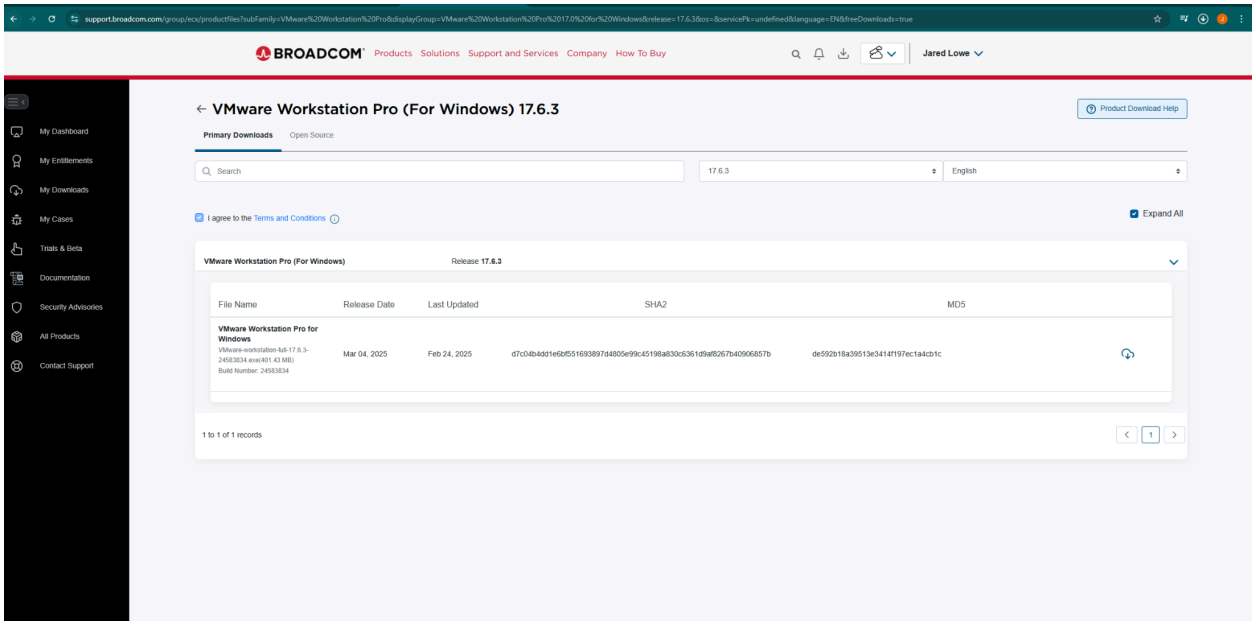
TOC


capstone.drawio
File Edit View Arrange Extras Help All changes saved
vmware
vmnet6
splunk>
SmartStore
EM5
192.168.4.10
Vulnerable machines and servers
Windows 10 Host
Domain Controller
Ubuntu Host
Ubuntu
pfsense
192.168.1.1
vmnet3
span port here
em4
(Ubuntu)
vmnet2
Kali Linux
Attack Network
EM1
192.168.1.10
vmnet4
vmnet5
Security Onion
192.168.3.10
em3
192.168.2.10
em2

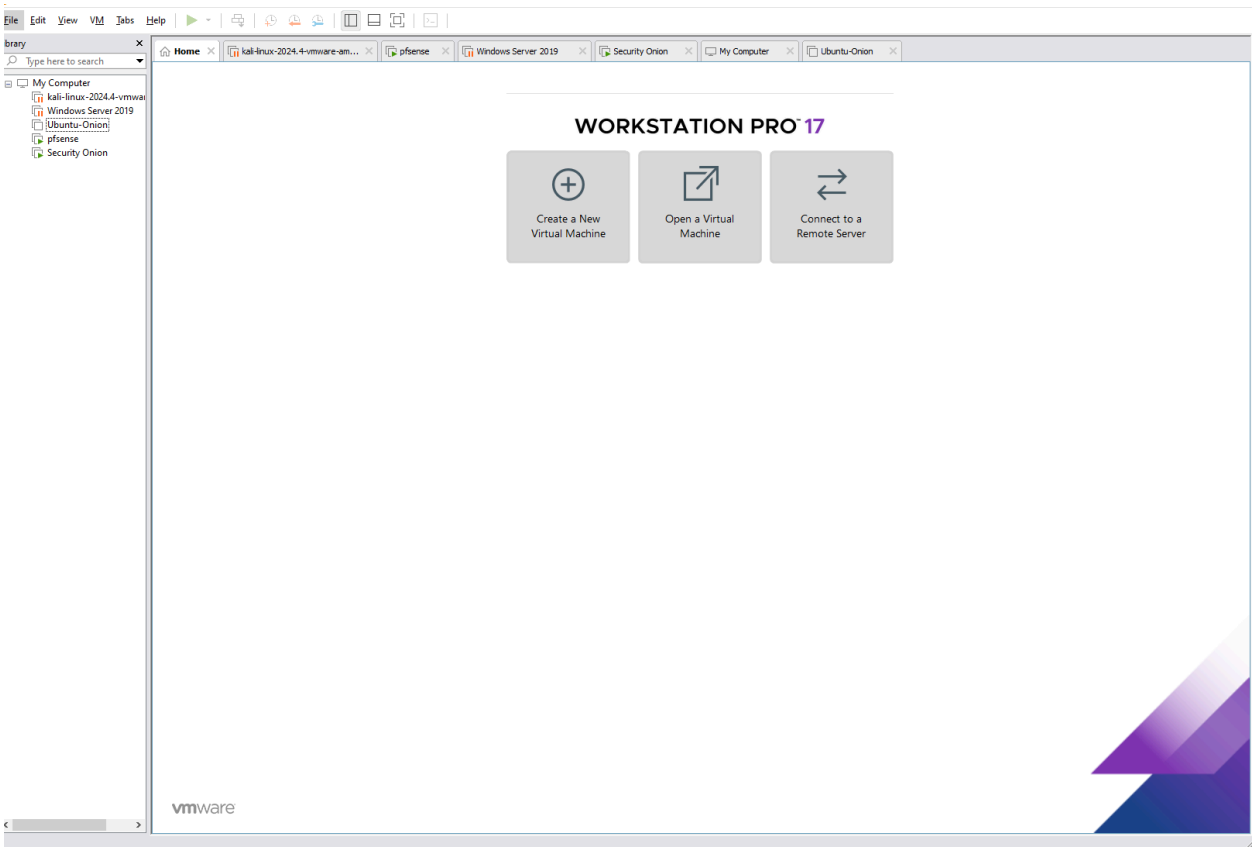
-Logging into Broadcom to acquire VMware Workstation Pro



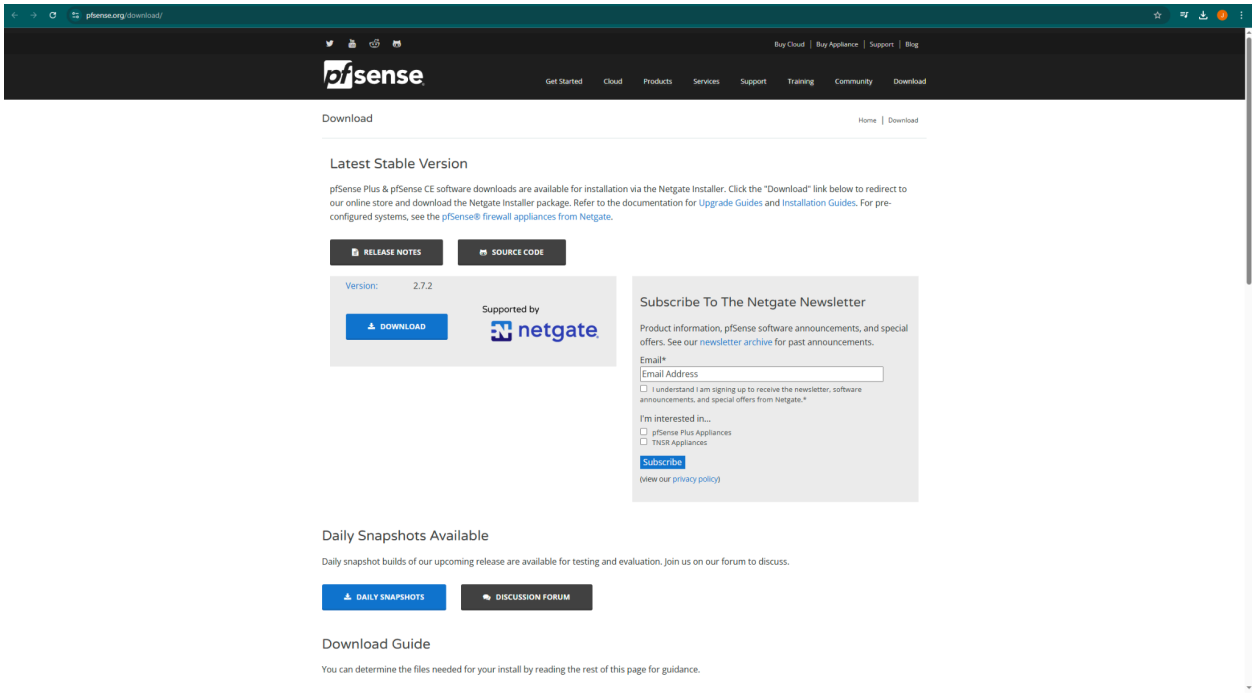
-VMware download



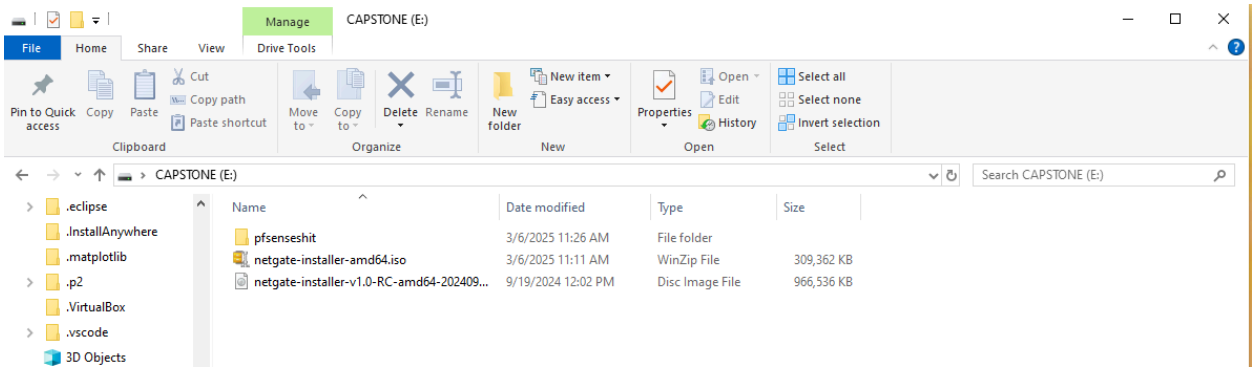
-The Workstation program



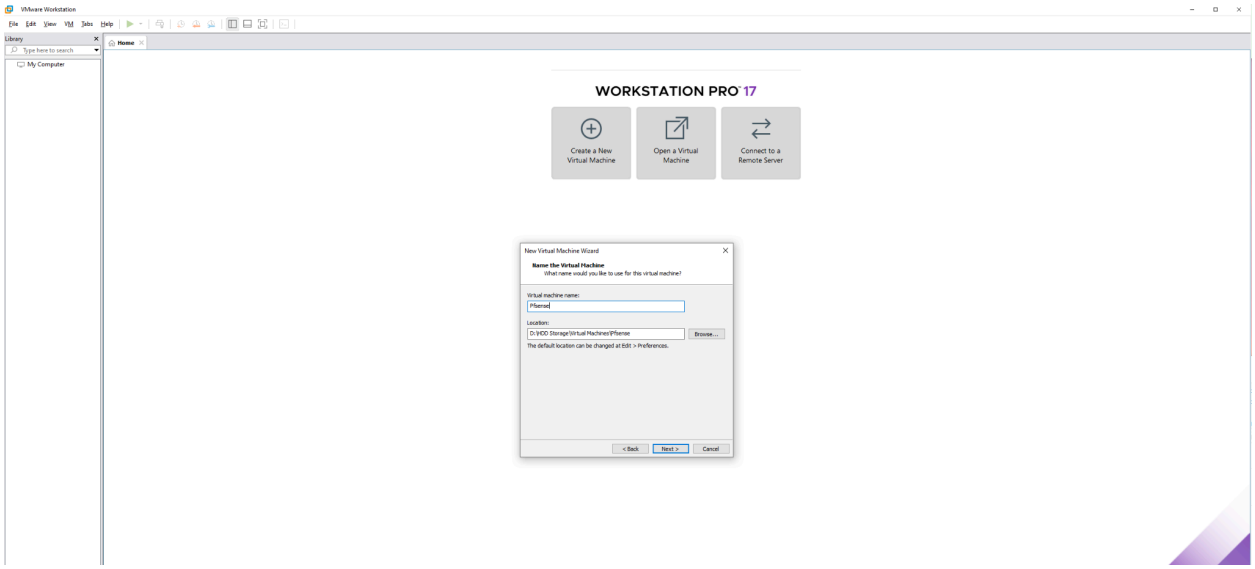
-Downloading pfsense



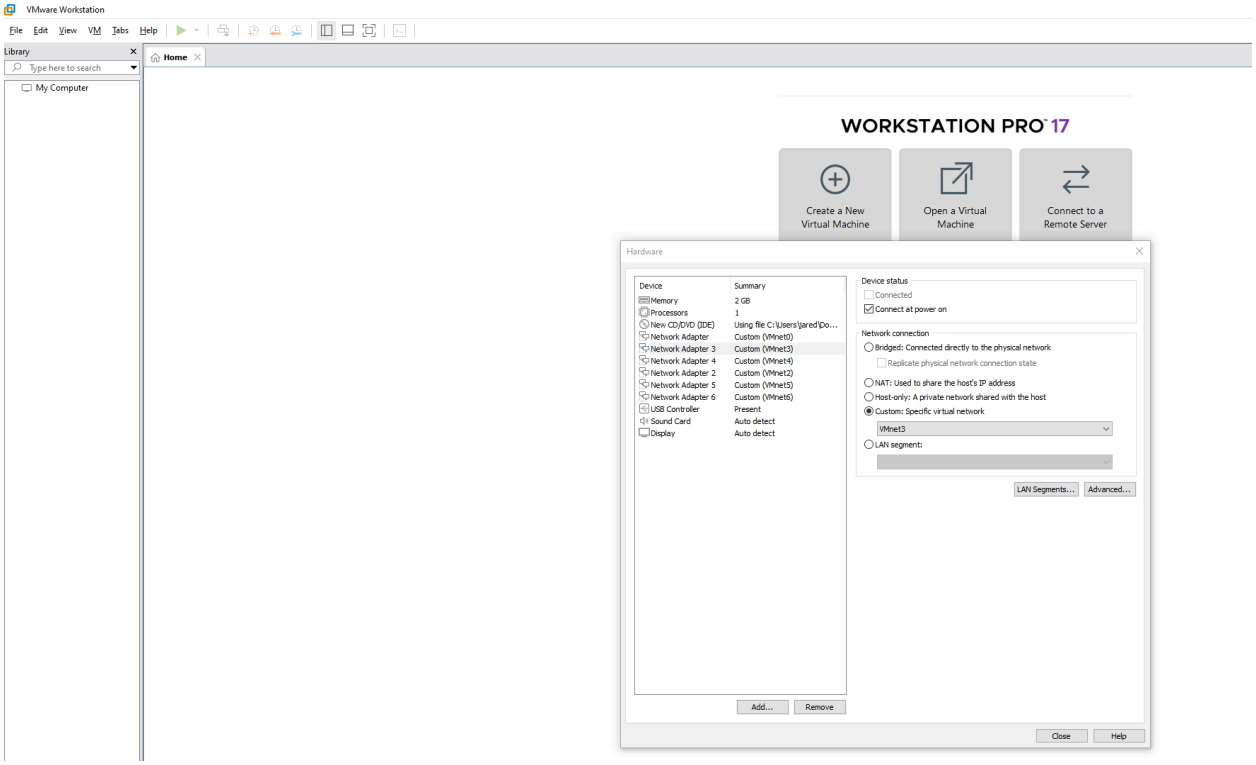
-Unzipping the pfsense file with 7-zip to extract the iso file



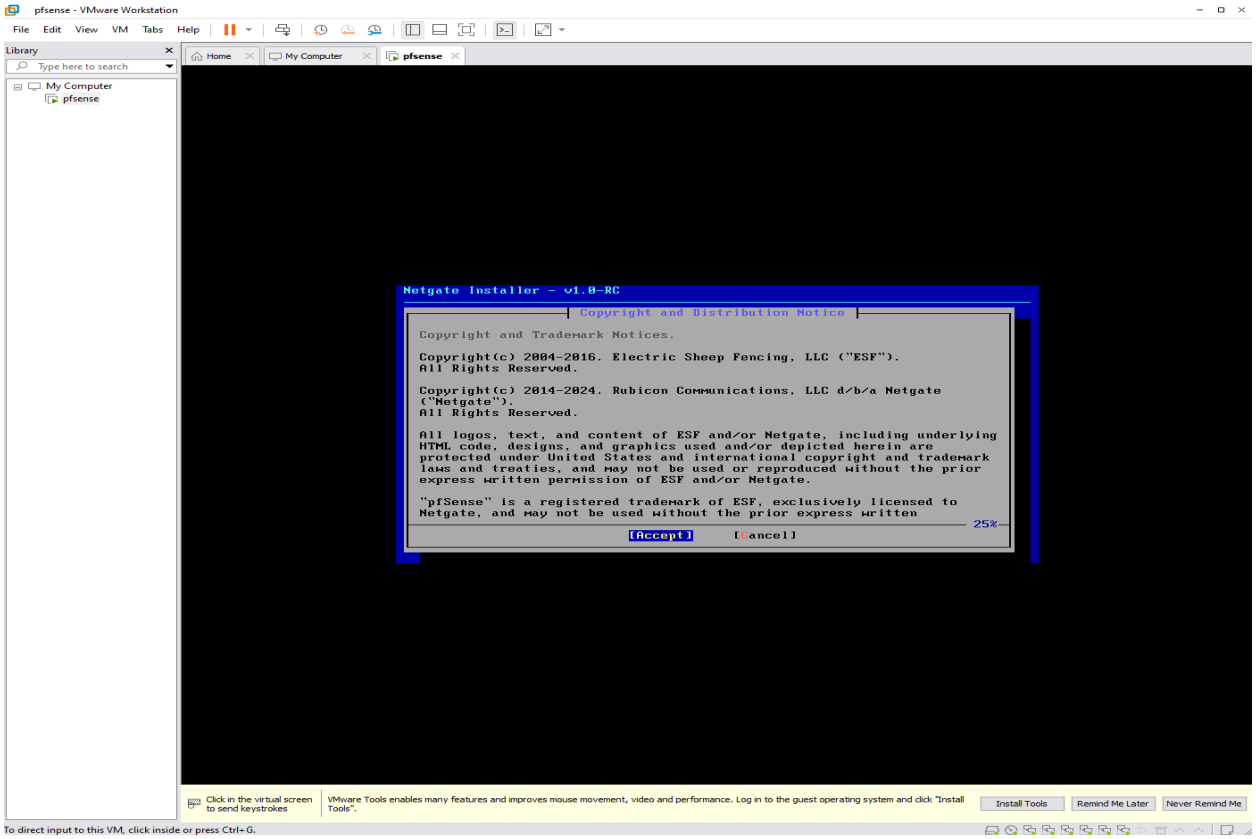
-Adding pfsense as a virtual machine

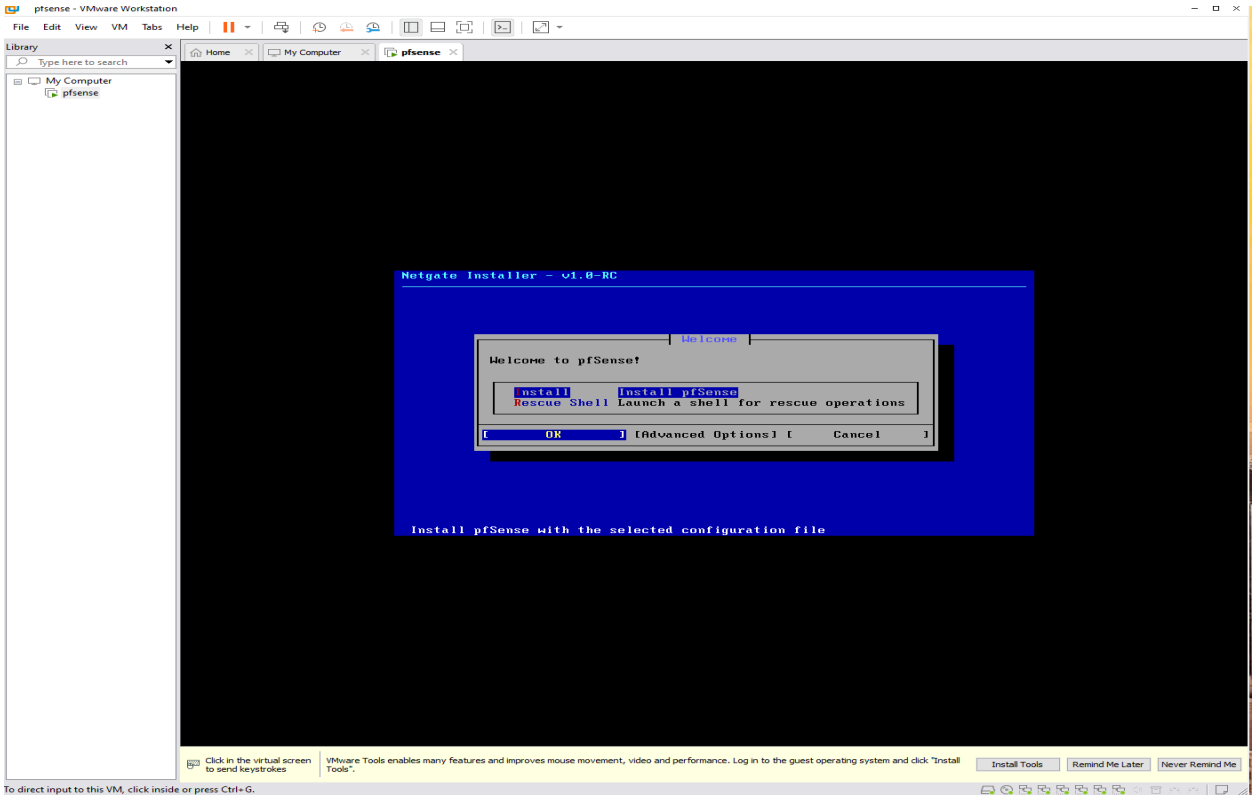


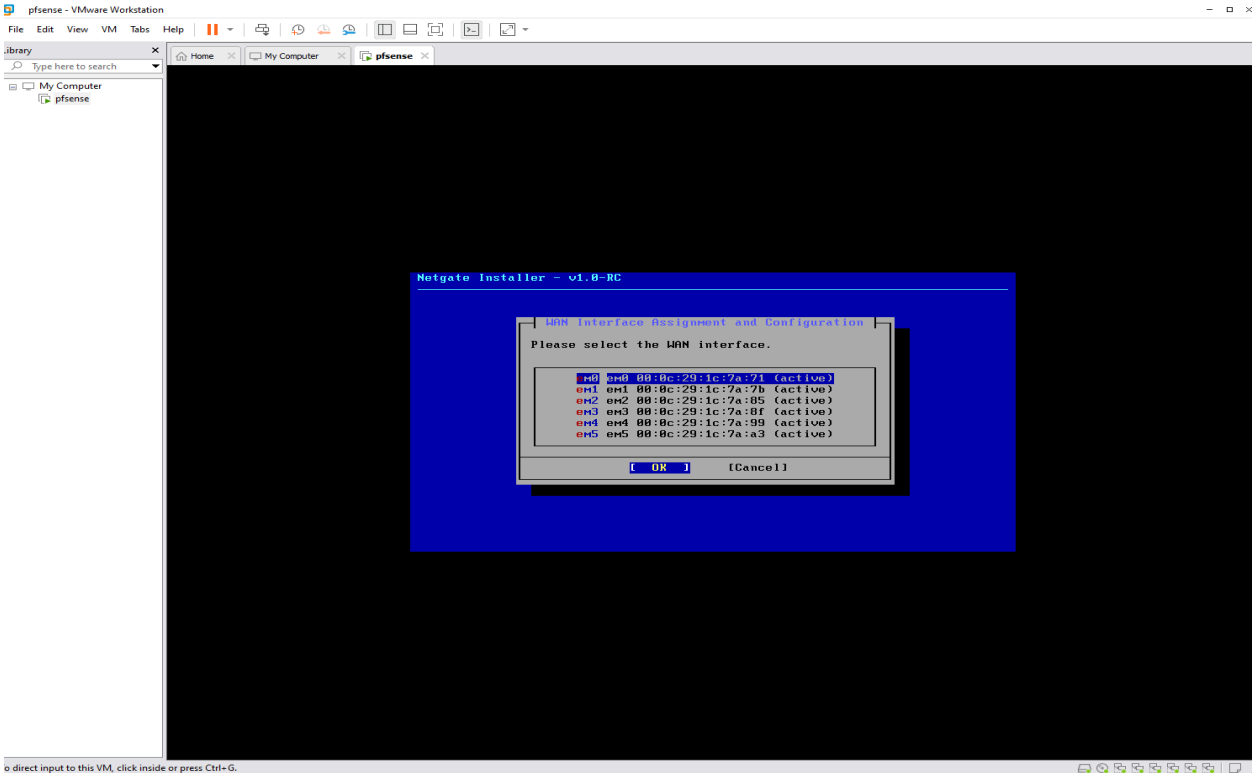
-configuring pfsense and adding 5 new network adapter with own specific virtual network

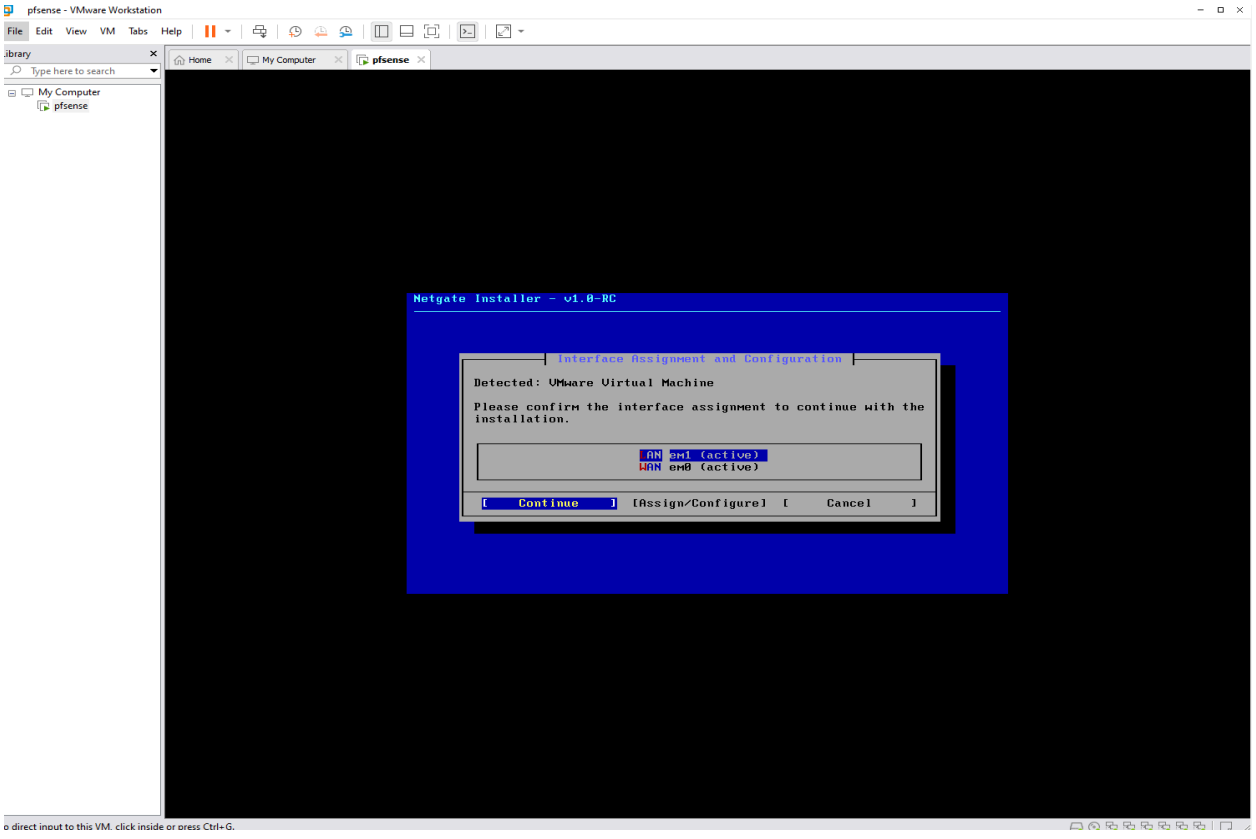


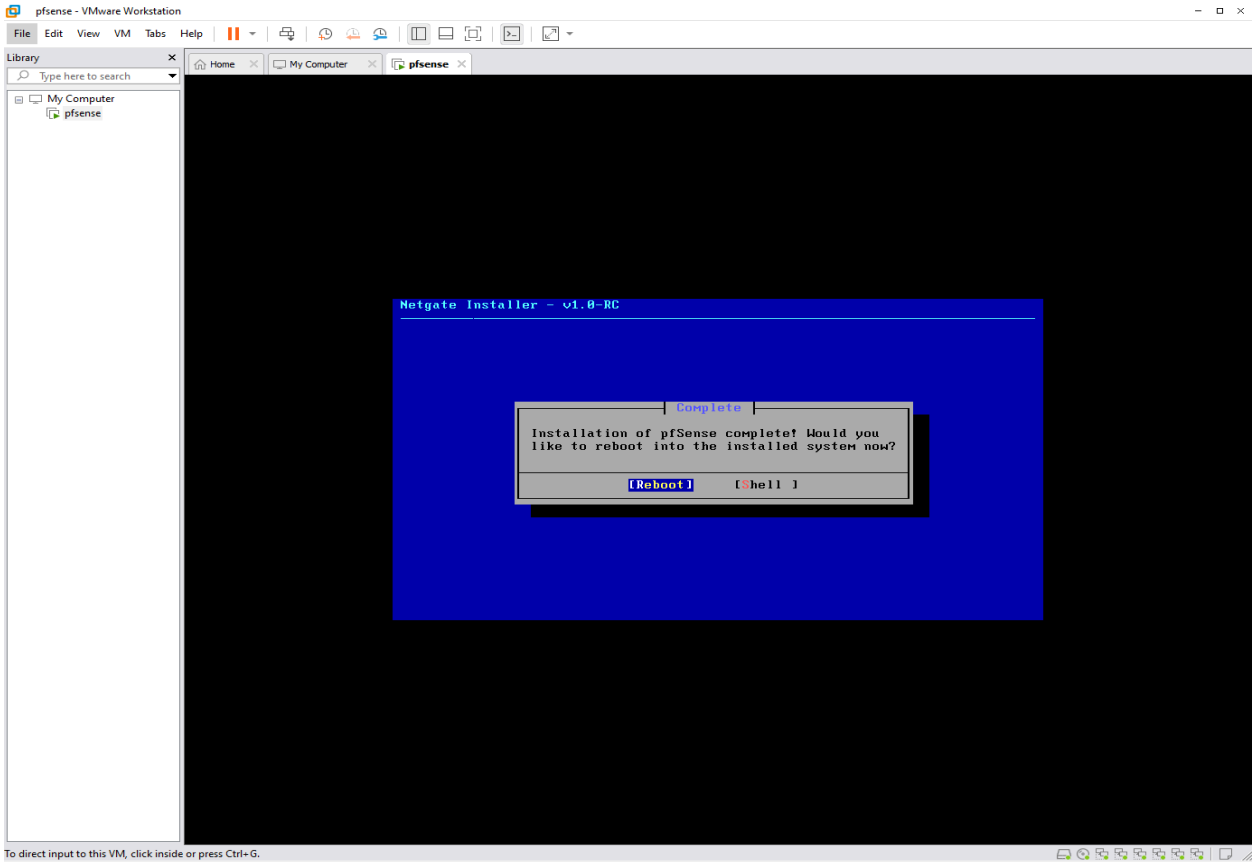
-The following images show entering the pfsense and enabling it inside the VM(5 images)



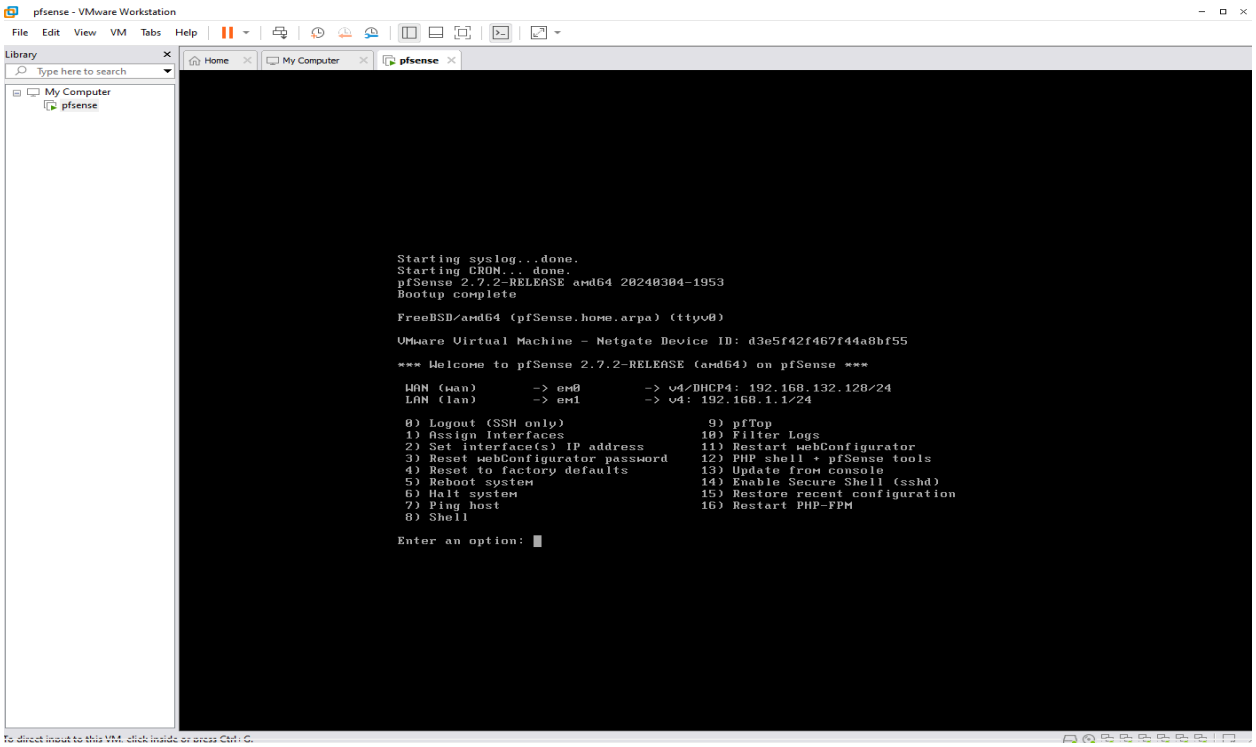



pfsense - VMware Workstation
File Edit View VM Tabs Help
Home
My Computer
pfsense
Netgate Installer - v1.0-RC
WAN Interface Assignment and Configuration
Please select the WAN interface.
em0 em0 00:0c:29:1c:7a:71 (active)
em1 em1 00:0c:29:1c:7a:7b (active)
em2 em2 00:0c:29:1c:7a:85 (active)
em3 em3 00:0c:29:1c:7a:8f (active)
em4 em4 00:0c:29:1c:7a:99 (active)
em5 em5 00:0c:29:1c:7a:a3 (active)
[OK] [Cancel]

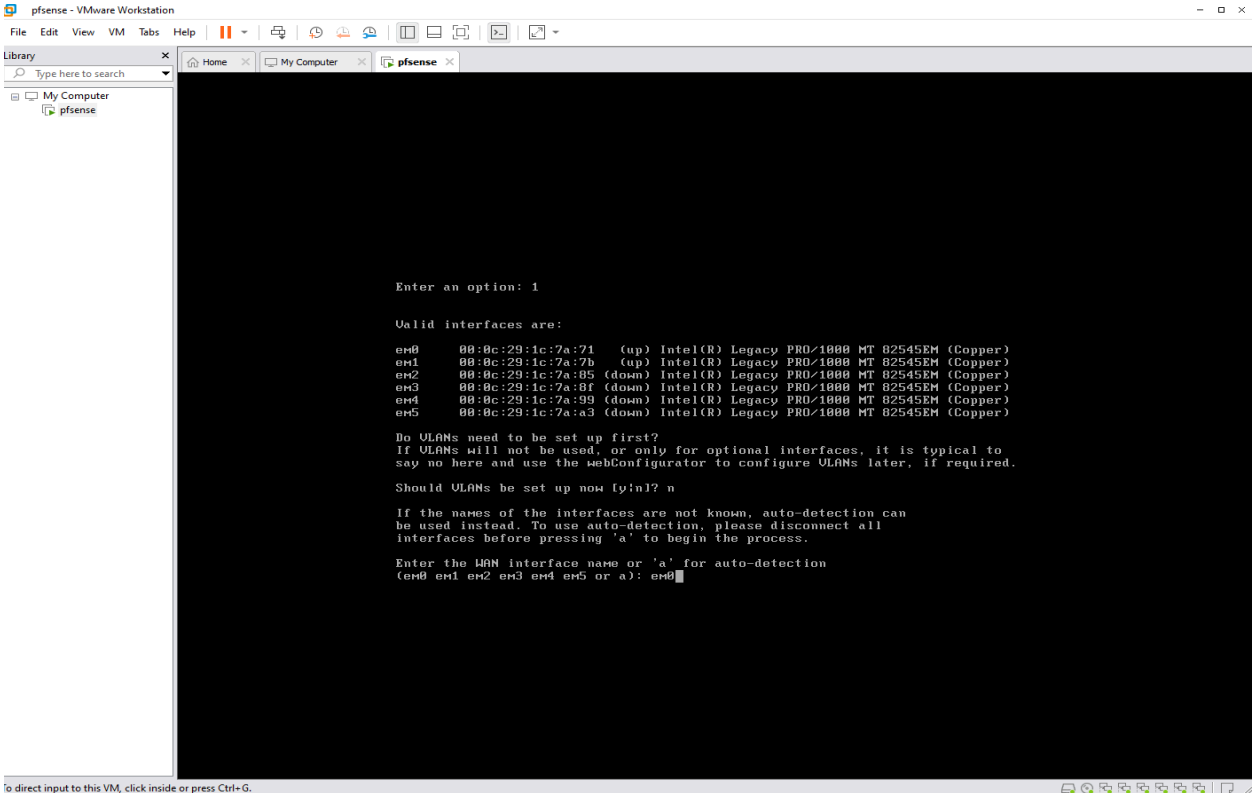

pfsense - VMware Workstation
File Edit View VM Tabs Help
Home
My Computer
pfsense
Netgate Installer - v1.0-RC
Interface Assignment and Configuration
Detected: VMware Virtual Machine
Please confirm the interface assignment to continue with the installation.
LAN em1 (active)
WAN em0 (active)
[Continue] [Assign/Configure] [Cancel]

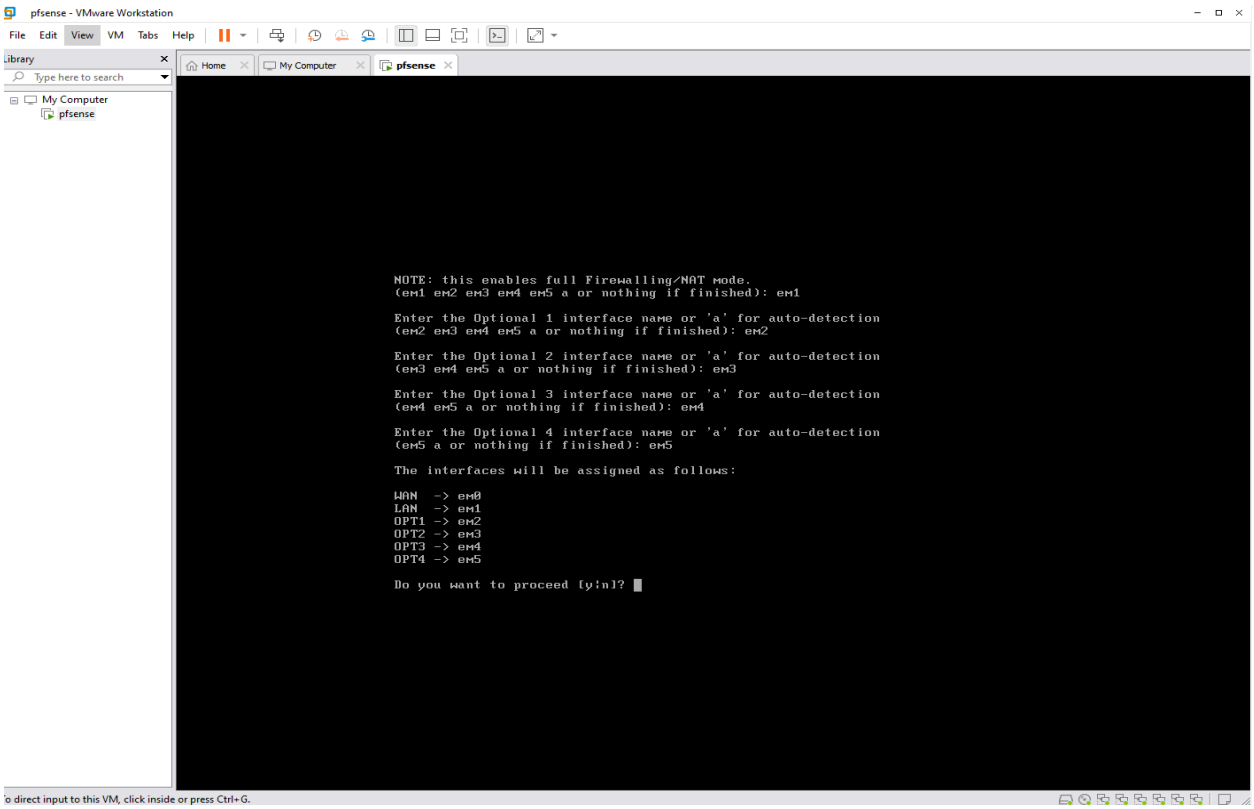


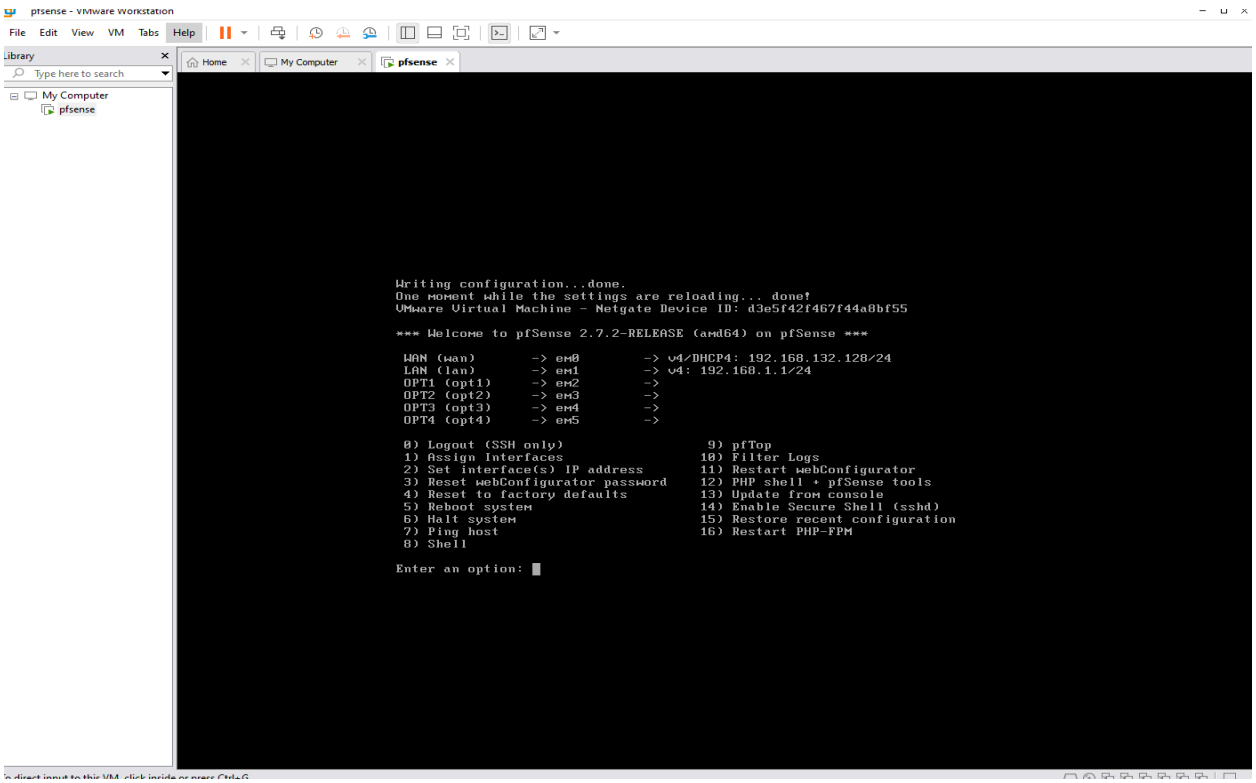
-after rebooting now we can set up the connections



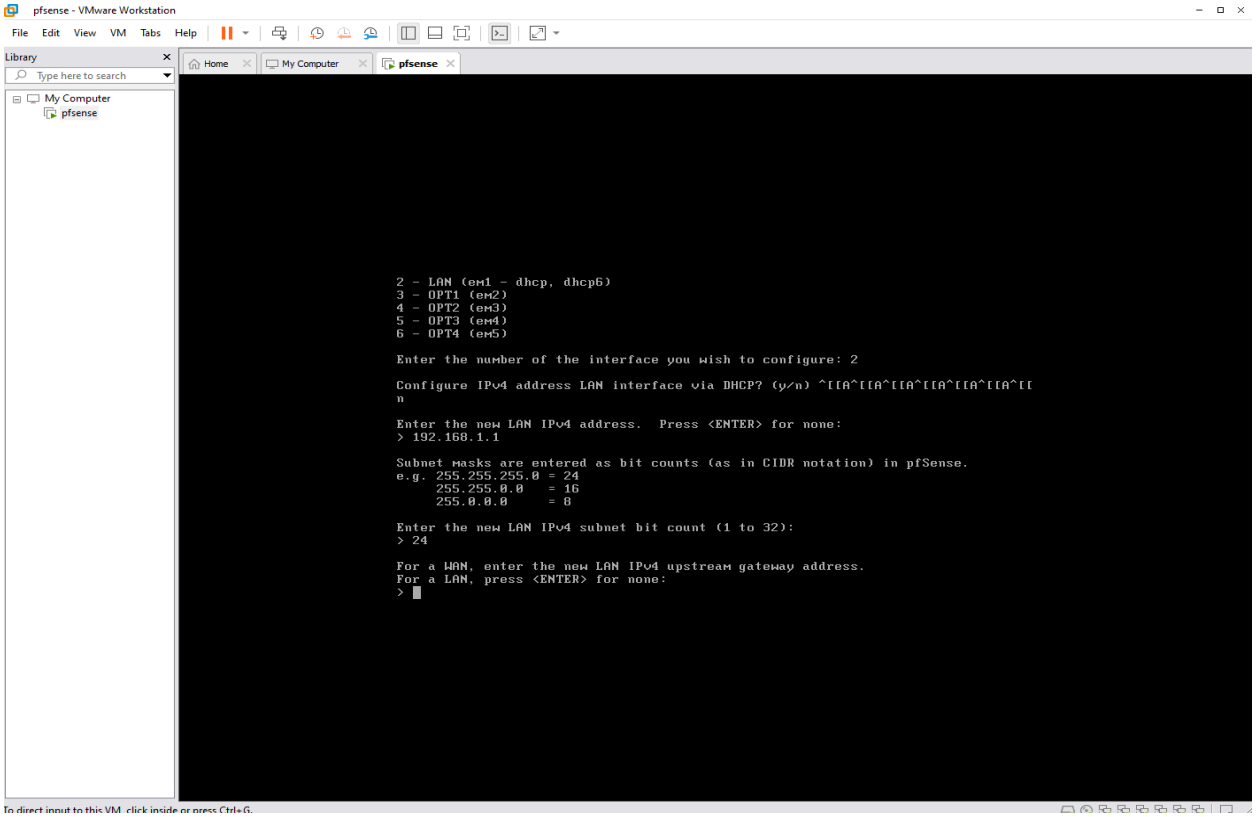
-the following images will show the connections into the interfaces(3 images)

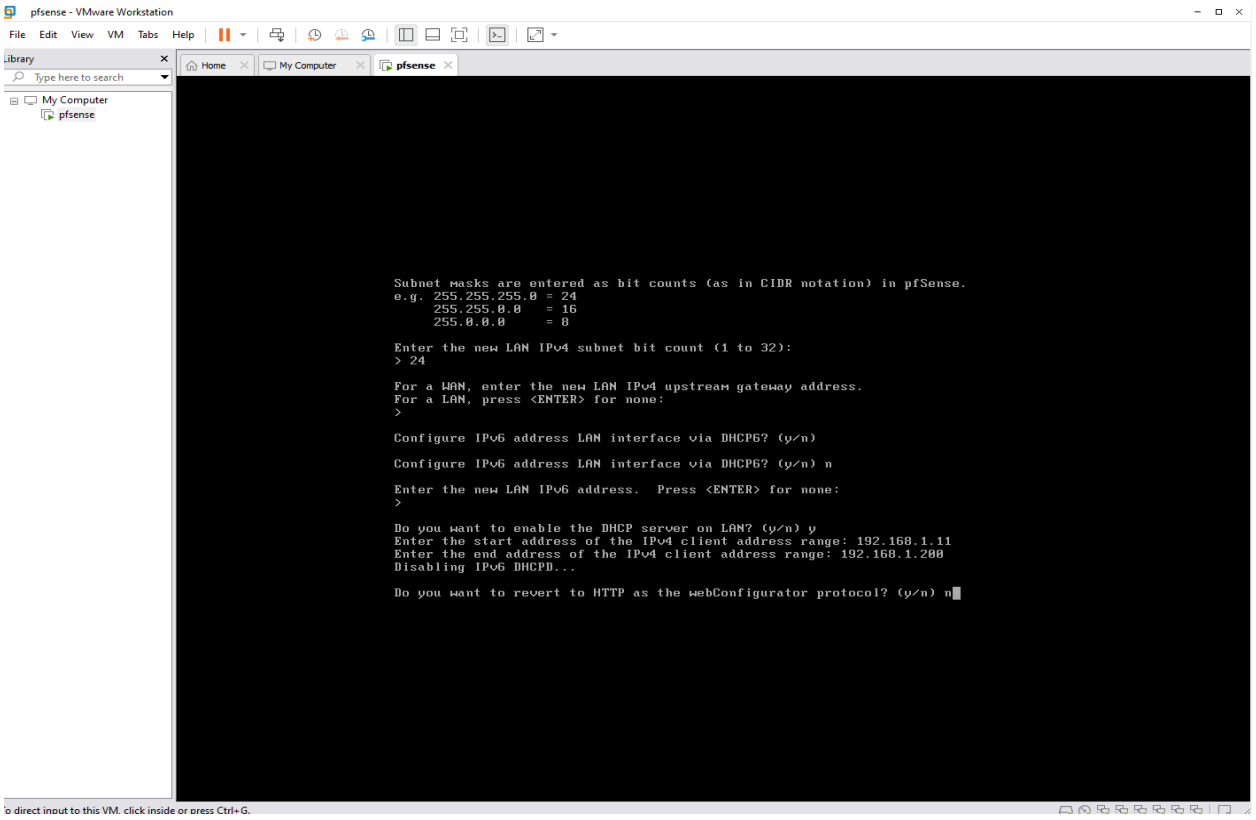




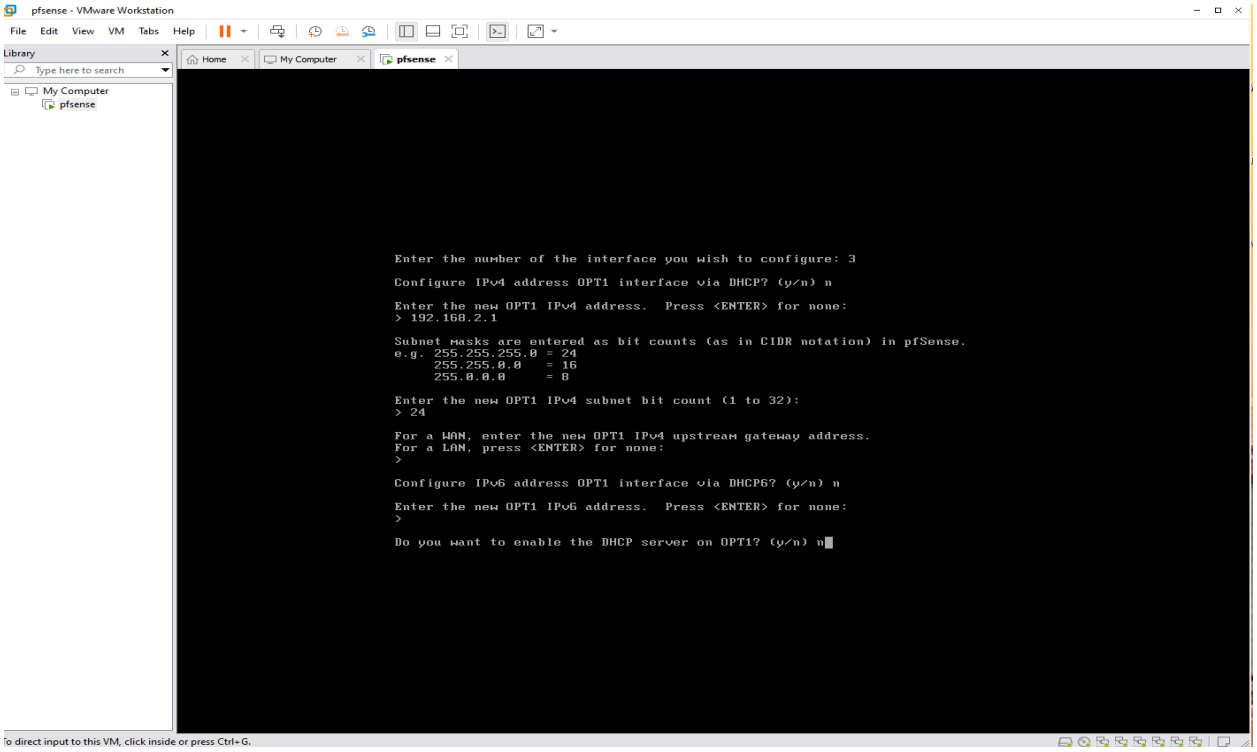

pfsense - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pfsense
Home
My Computer
pfsense
Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: d3e5f42f467f44a8bf55
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.132.128/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
OPT1 (opt1) -> em2 ->
OPT2 (opt2) -> em3 ->
OPT3 (opt3) -> em4 ->
OPT4 (opt4) -> em5 ->
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

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

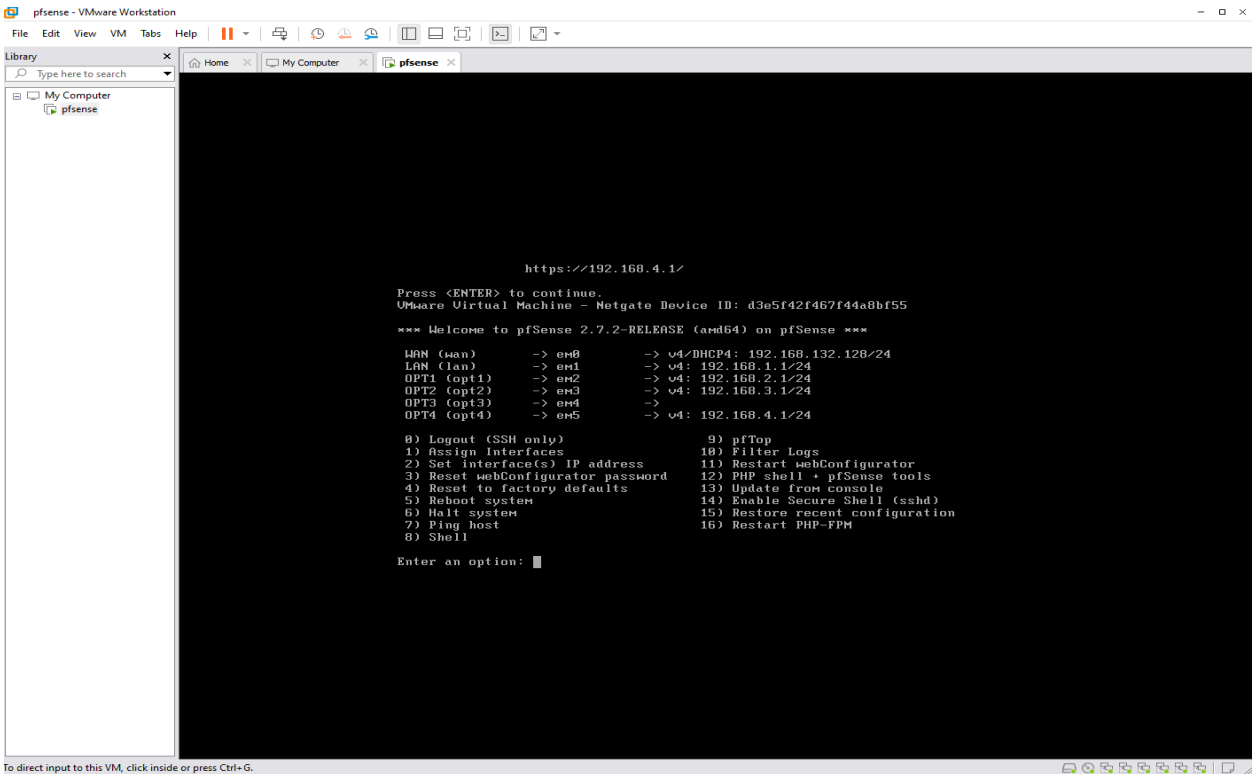




-To minimize the amount of images I set op1, opt2, and opt4 to these settings and leaving opt3 blank so it can have pinpoint traffic that security onion can monitor

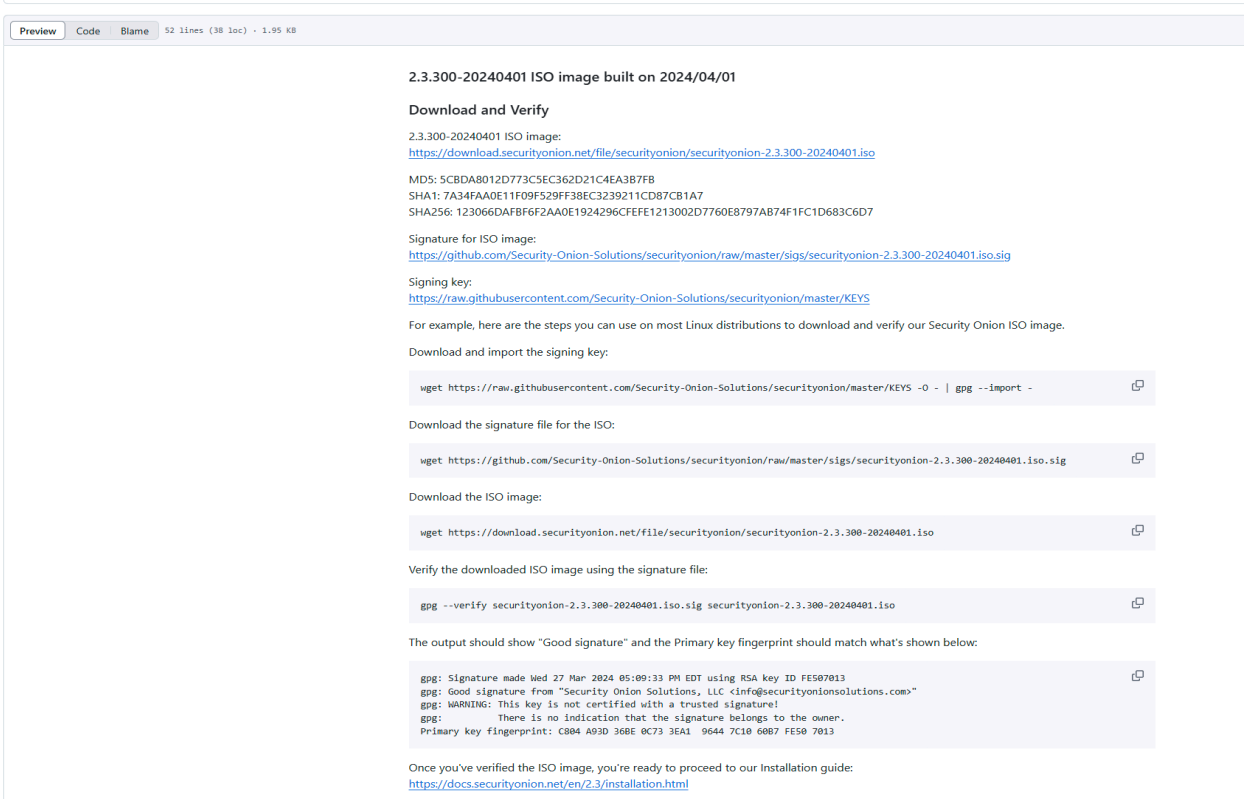


-This is the finished interface setup



-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 (38 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

MD5: 5CBDA8012D773C5EC362D21C4EA3B7FB
SHA1: 7A34FAA0E11F09F529FF38EC3239211CD87CB1A7
SHA256: 123066DAFBF6F2AA0E1924296CFEFE1213002D7760E8797AB74F1FC1D683C6D7

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:

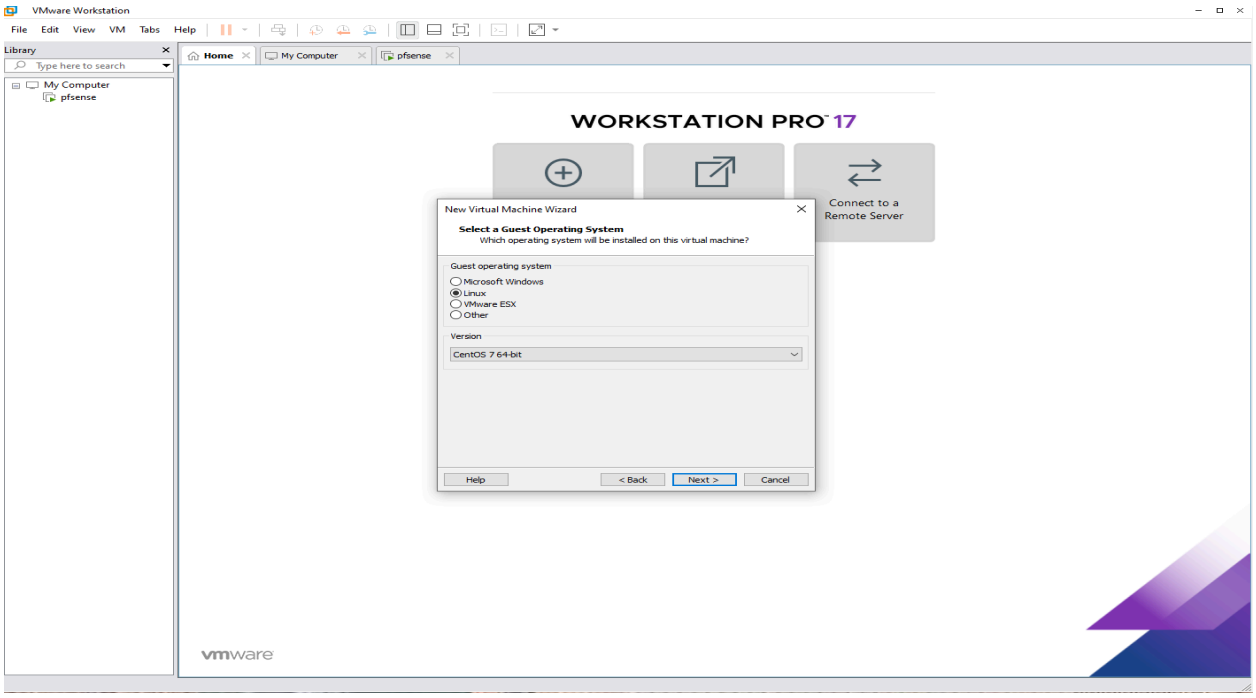
```
gpg --verify securityonion-2.3.300-20240401.iso.sig securityonion-2.3.300-20240401.iso
```

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

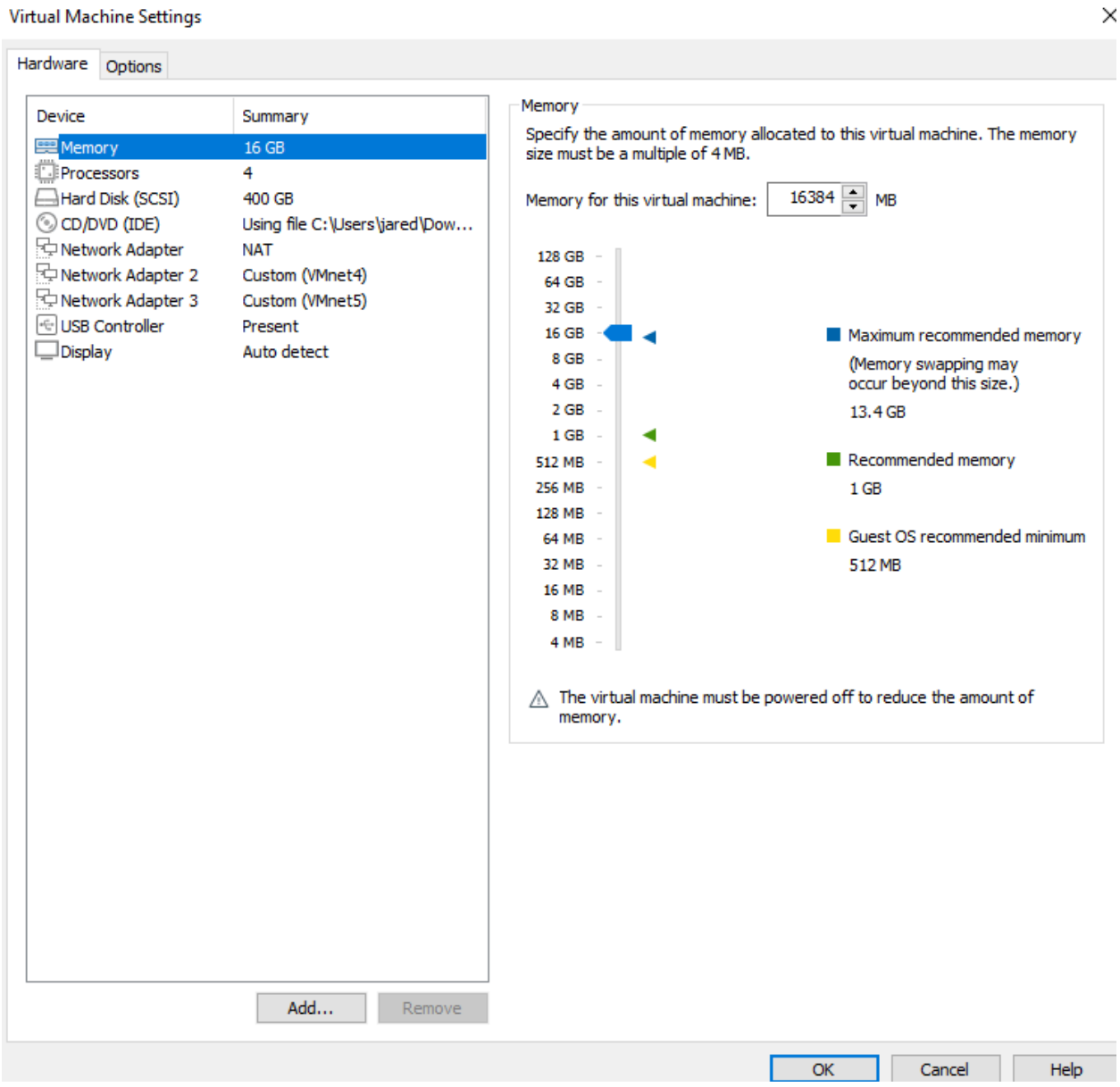
```
gpg: Signature made Wed 27 Mar 2024 05:09:33 PM EDT using RSA key ID FE507013
gpg: Good signature from "Security Onion Solutions, LLC <info@securityonionsolutions.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C804 A93D 36BE 0C73 3EA1  9644 7C10 60B7 FE50 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

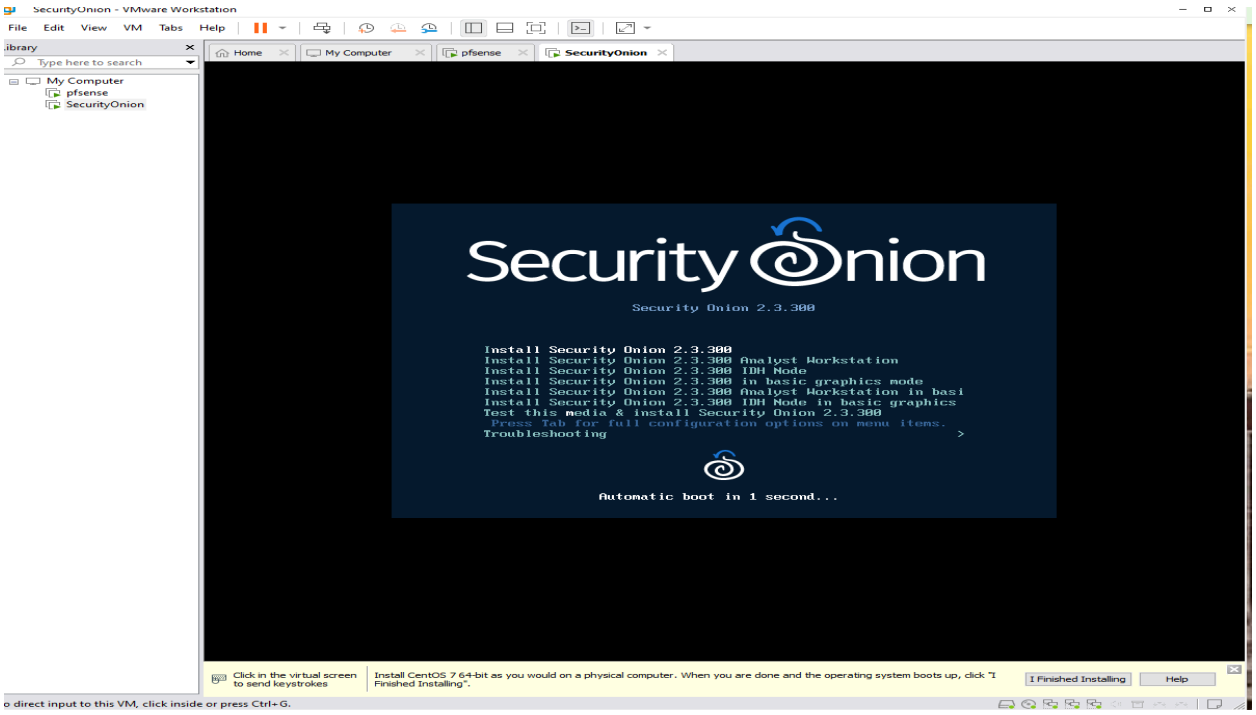
-Setting the OS and version for security Onion



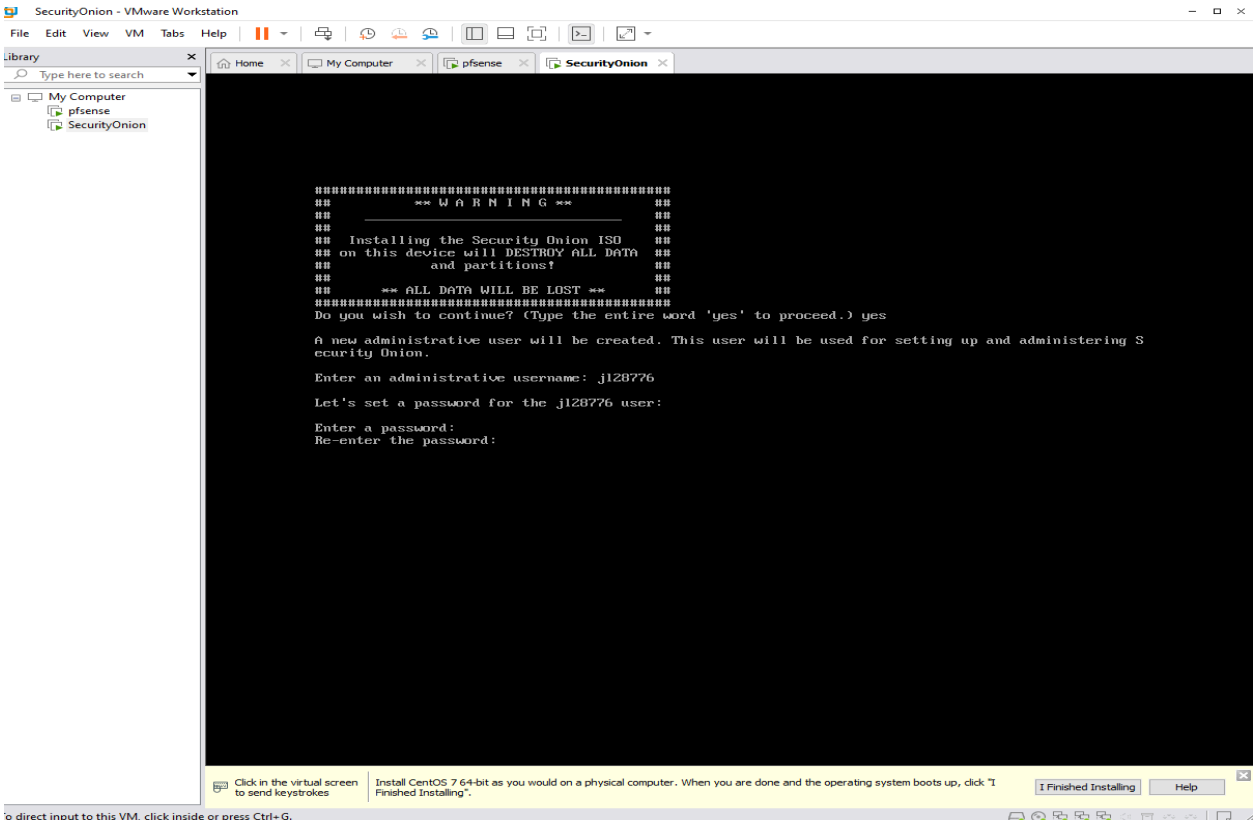
-setting up the hardware. Setting the memory and processors to the minimum it recommends for security Onion. Adding 2 network adapters where we match one to vmnet4 tp pair with pfsense and vmnet5 to port.



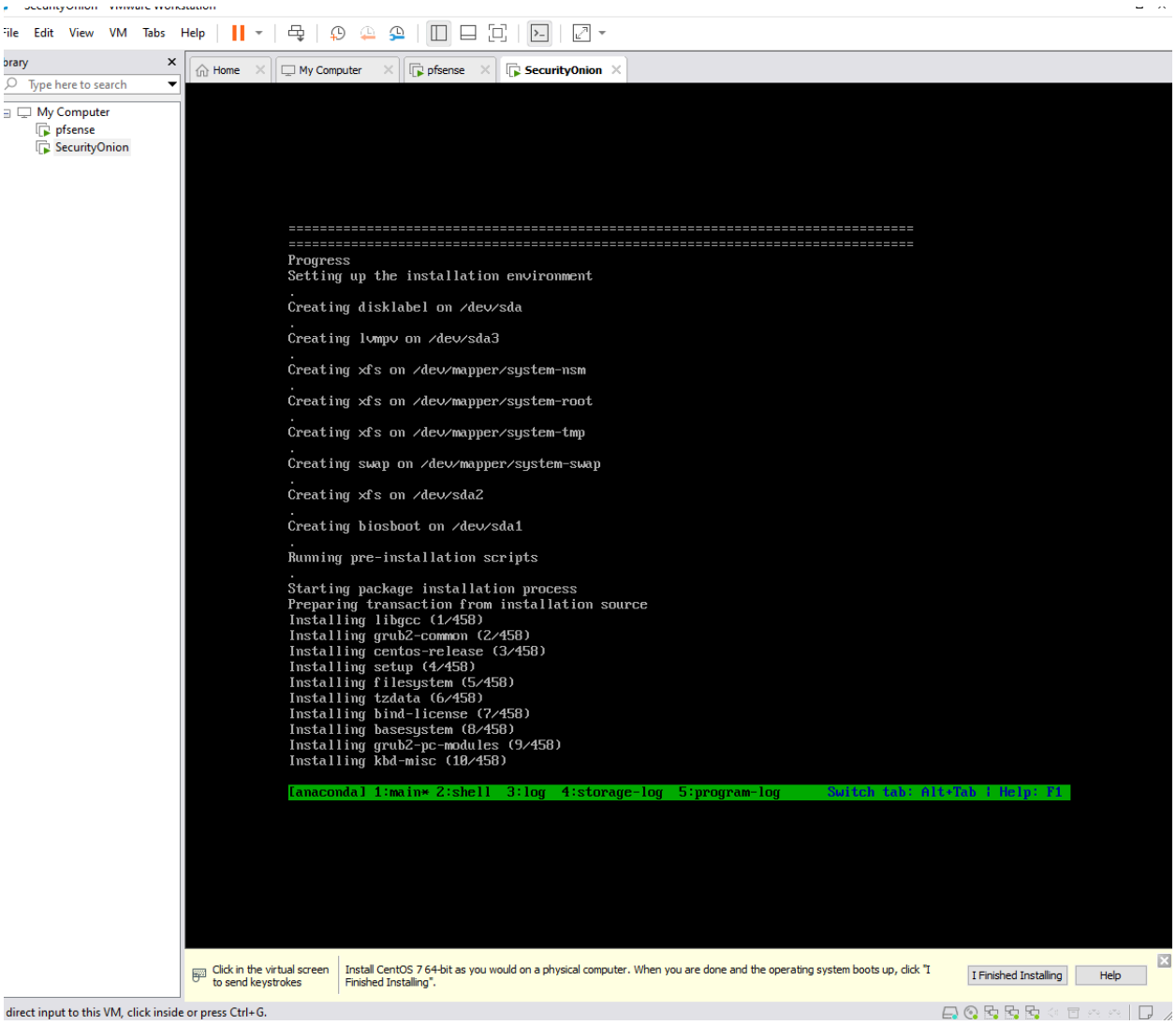
-now we can enter the security onion



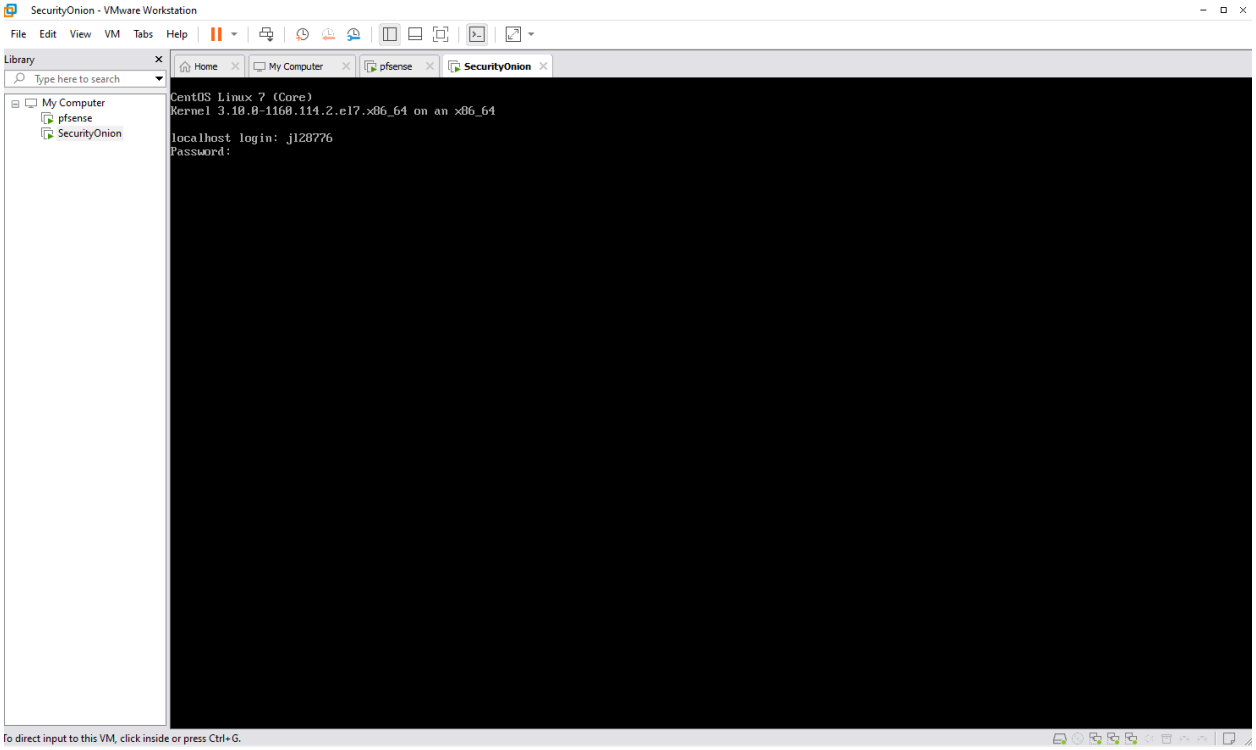
-now we can create a username and password for security onion where i used my GSU username for this username and just onion as the password



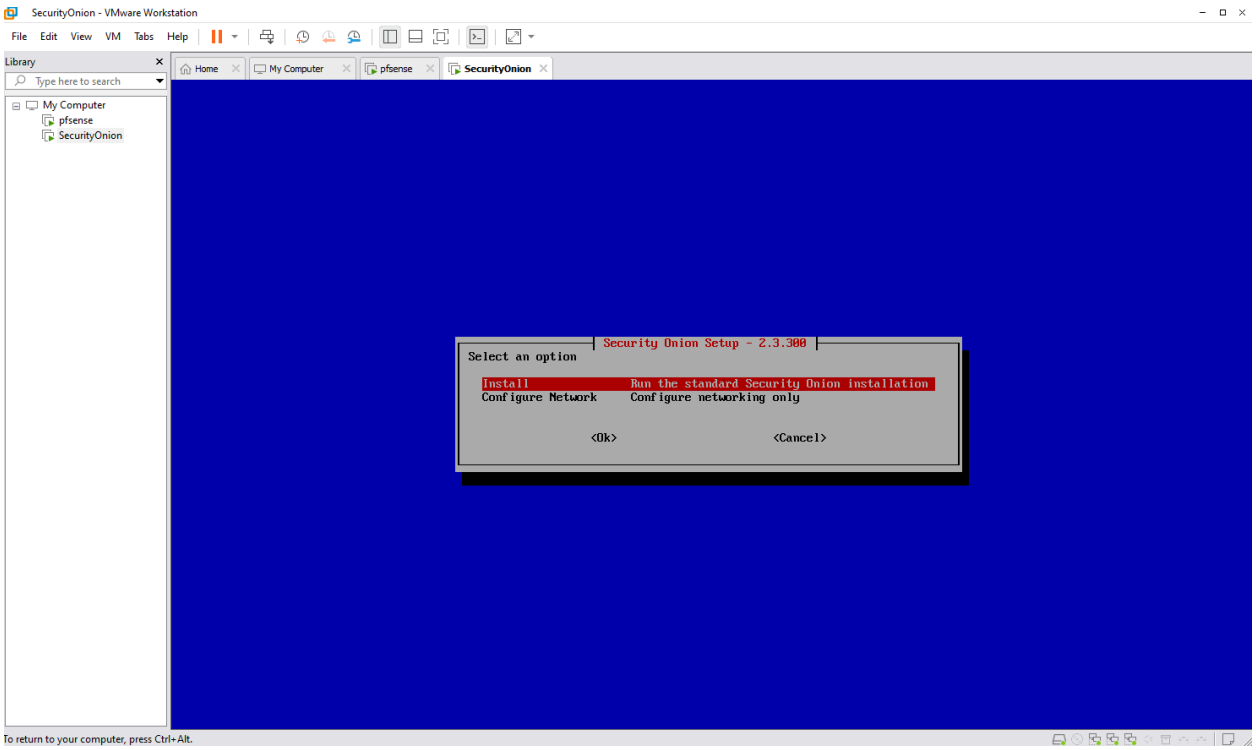
-Long installation process(30 min)

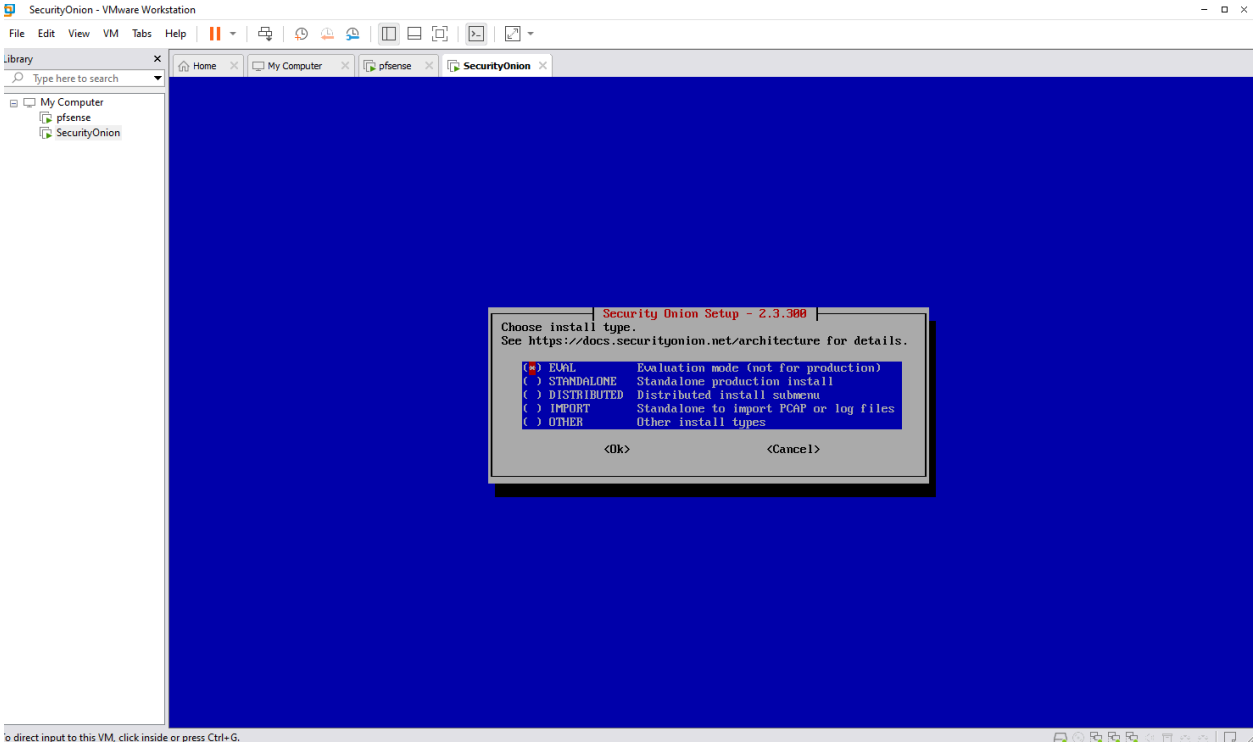


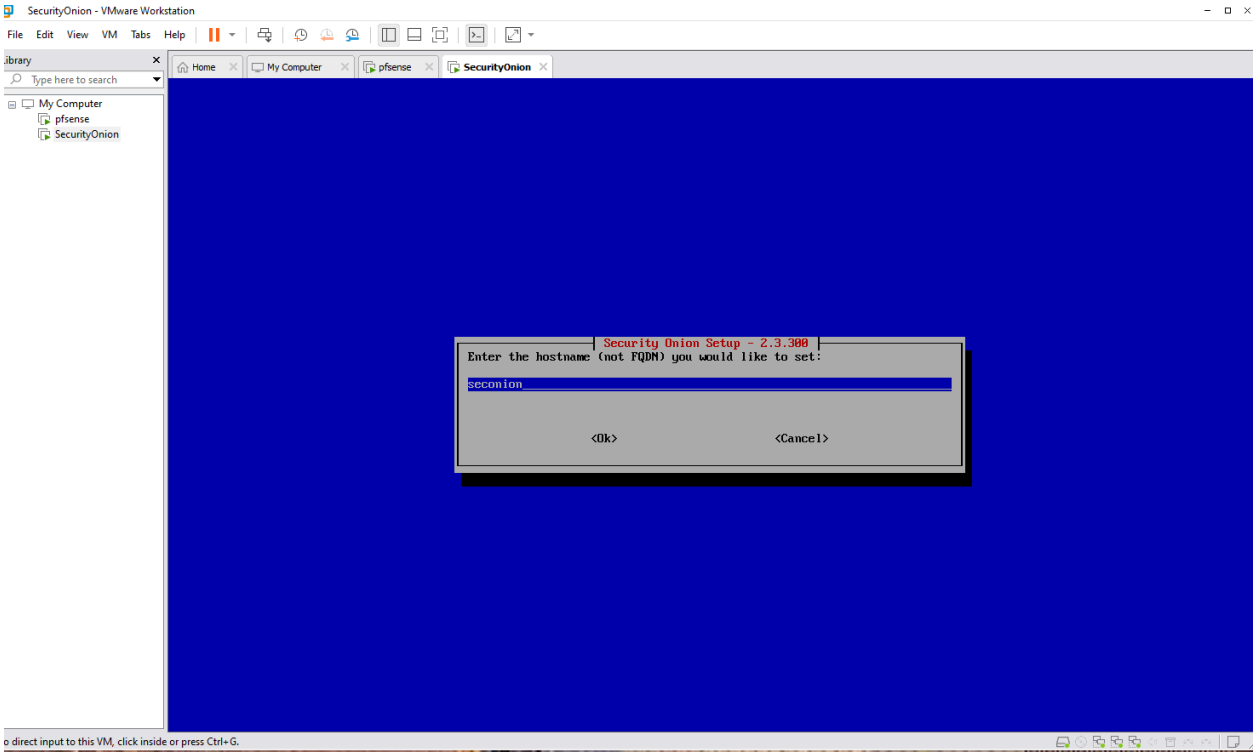
-After installation and reboot we sign into the onion

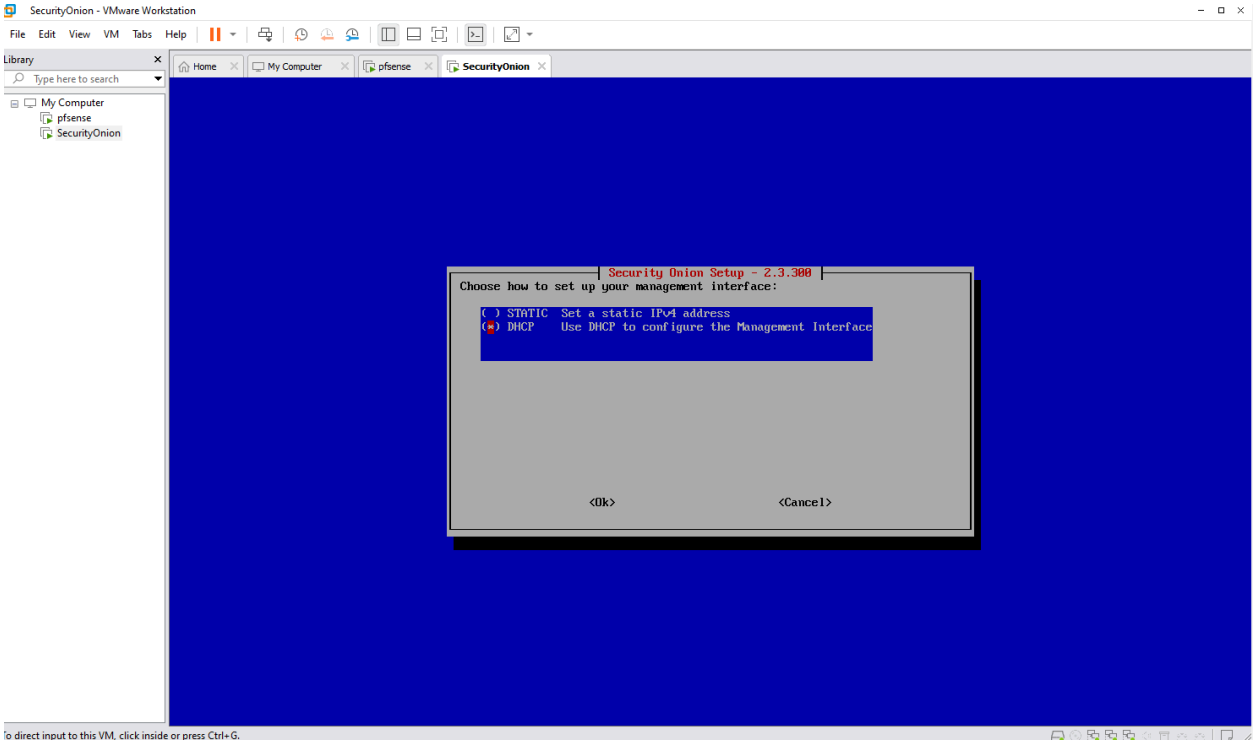


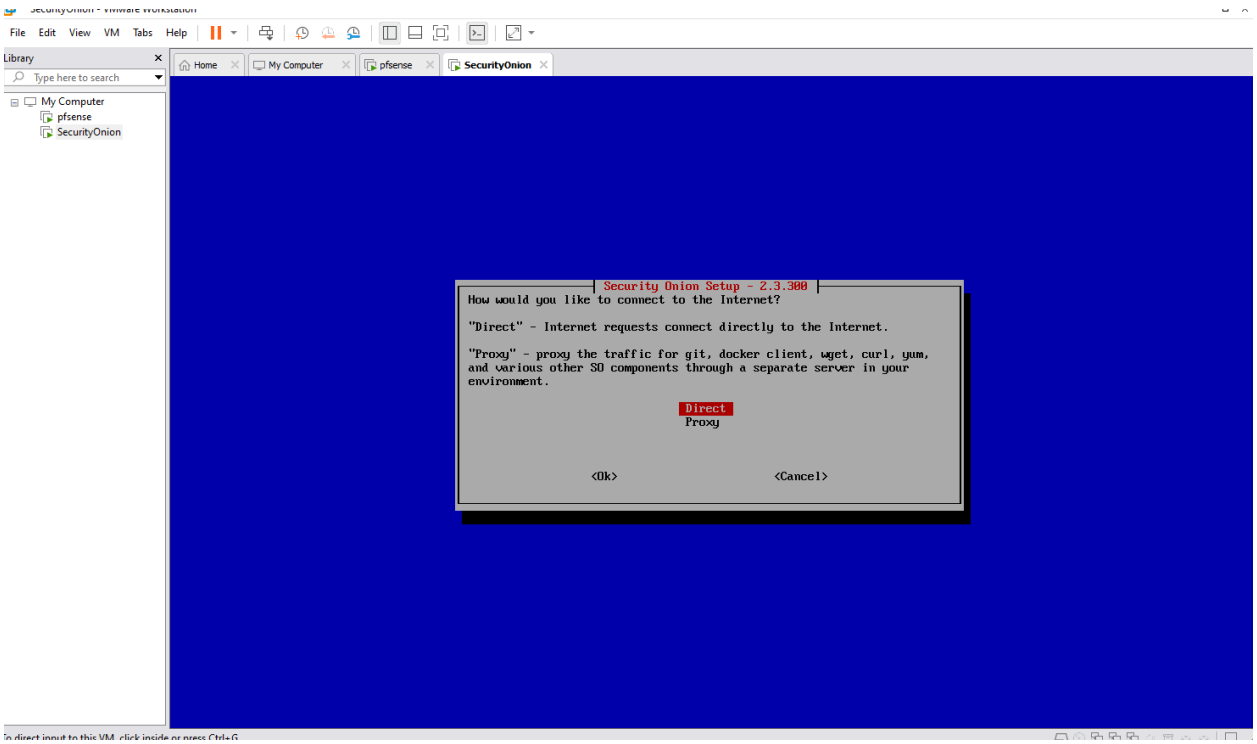
-The following is the installation progress(9 images)

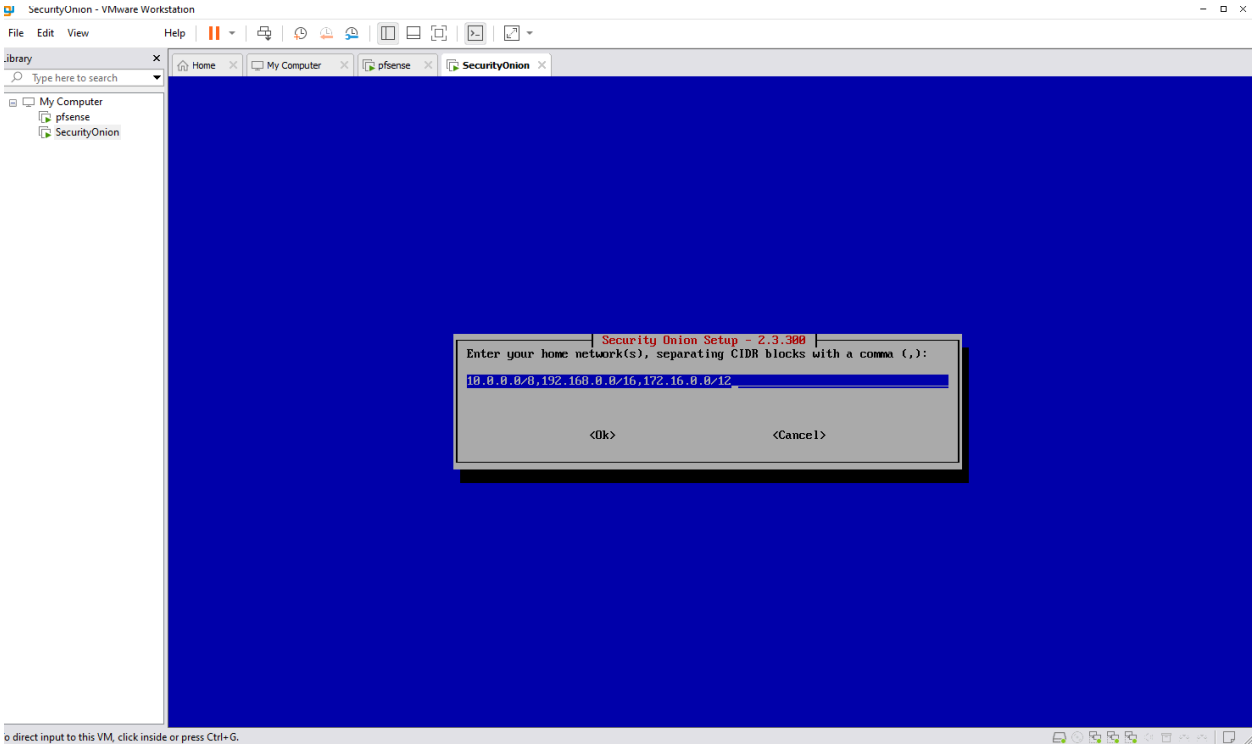


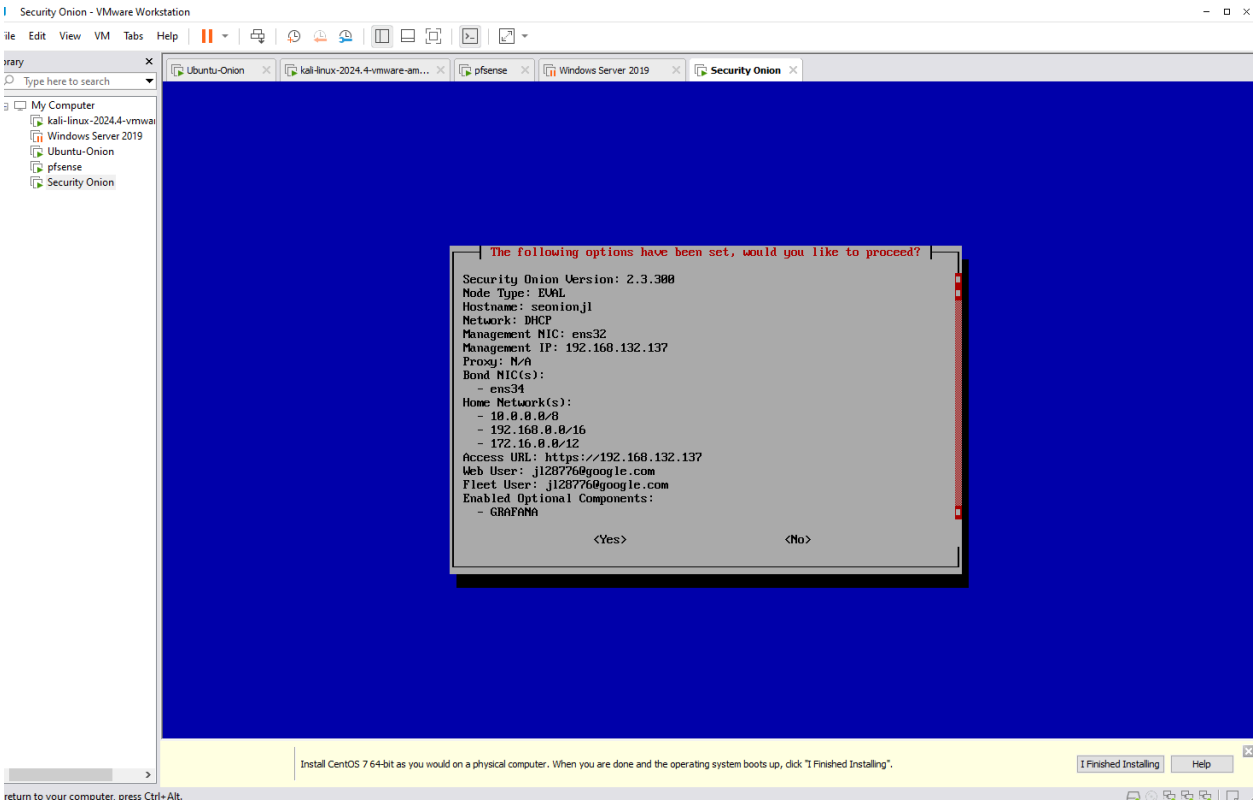

SecurityOnion - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pfsense
SecurityOnion
Home
My Computer
pfsense
SecurityOnion
Security Onion Setup - 2.3.300
Choose install type.
See https://docs.securityonion.net/architecture for details.
(*) EVAL Evaluation mode (not for production)
( ) STANDALONE Standalone production install
( ) DISTRIBUTED Distributed install submenu
( ) IMPORT Standalone to import PCAP or log files
( ) OTHER Other install types
<Ok>
<Cancel>
o direct input to this VM, click inside or press Ctrl+G.

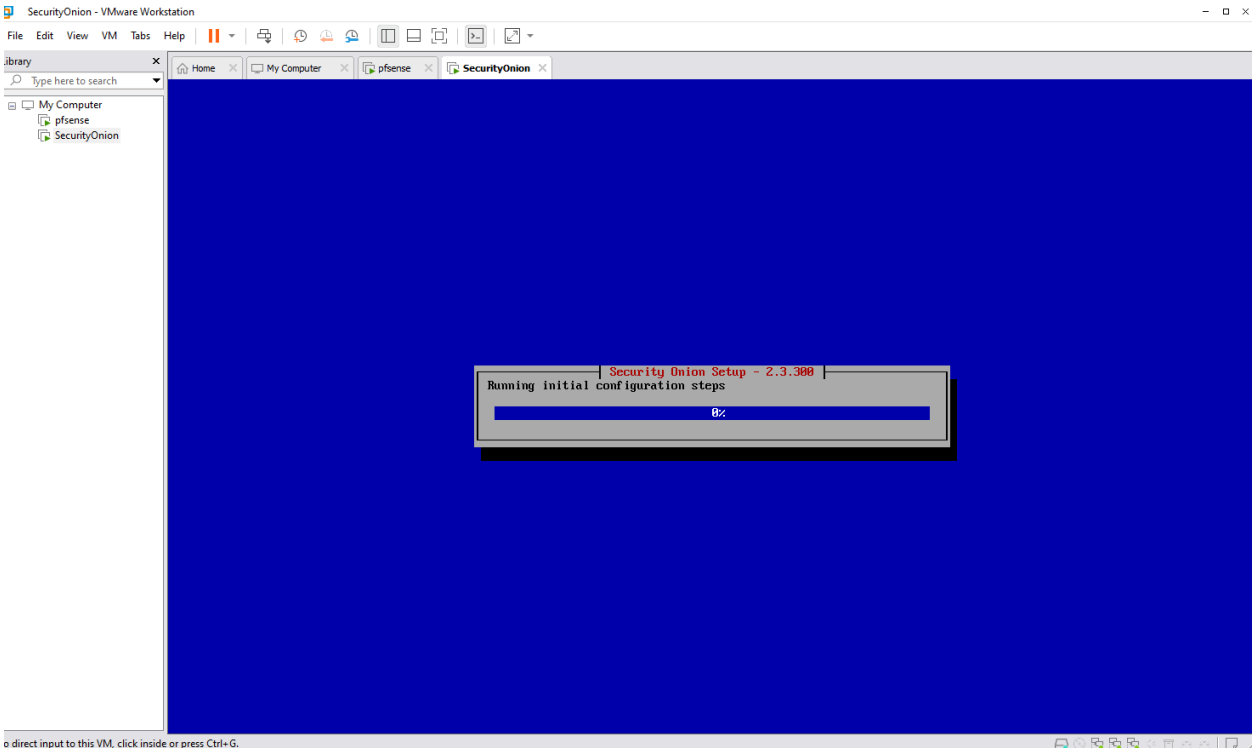

SecurityOnion - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pfsense
SecurityOnion
Home
My Computer
pfsense
SecurityOnion
Security Onion Setup - 2.3.300
Enter the hostname (not FQDN) you would like to set:
seconion
<Ok>
<Cancel>
o direct input to this VM, click inside or press Ctrl+G.


SecurityOnion - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pfsense
SecurityOnion
Home
My Computer
pfsense
SecurityOnion
Security Onion Setup - 2.3.300
Choose how to set up your management interface:
( ) STATIC Set a static IPv4 address
(*) DHCP Use DHCP to configure the Management Interface
<Ok>
<Cancel>
To direct input to this VM, click inside or press Ctrl+G.

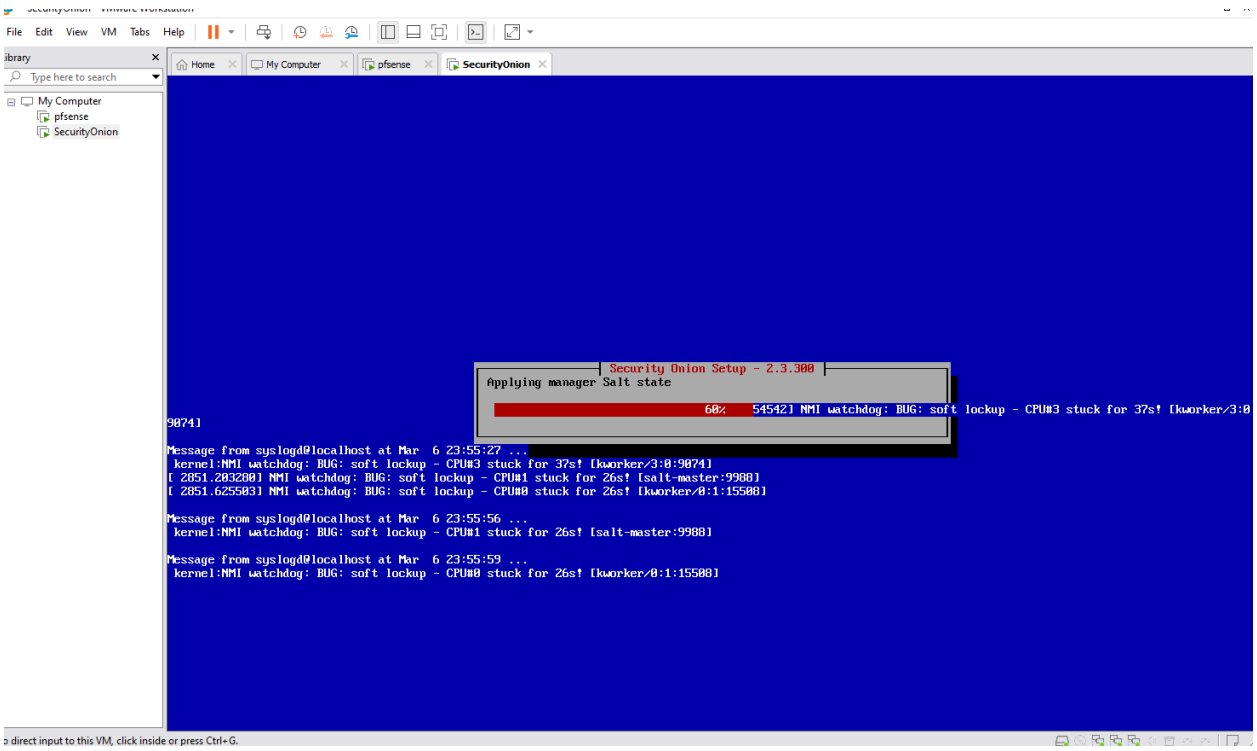

File Edit View VM Tabs Help
Library
Type here to search
My Computer
pfsense
SecurityOnion
Home
My Computer
pfsense
SecurityOnion
Security Onion Setup - 2.3.300
How would you like to connect to the Internet?
"Direct" - Internet requests connect directly to the Internet.
"Proxy" - proxy the traffic for git, docker client, wget, curl, yum, and various other SO components through a separate server in your environment.
Direct
Proxy
<Ok>
<Cancel>


SecurityOnion - VMware Workstation
File Edit View Help
Home
My Computer
pfsense
SecurityOnion
Security Onion Setup - 2.3.300
Enter your home network(s), separating CIDR blocks with a comma (,):
10.0.0.0/8,192.168.0.0/16,172.16.0.0/12
<Ok>
<Cancel>

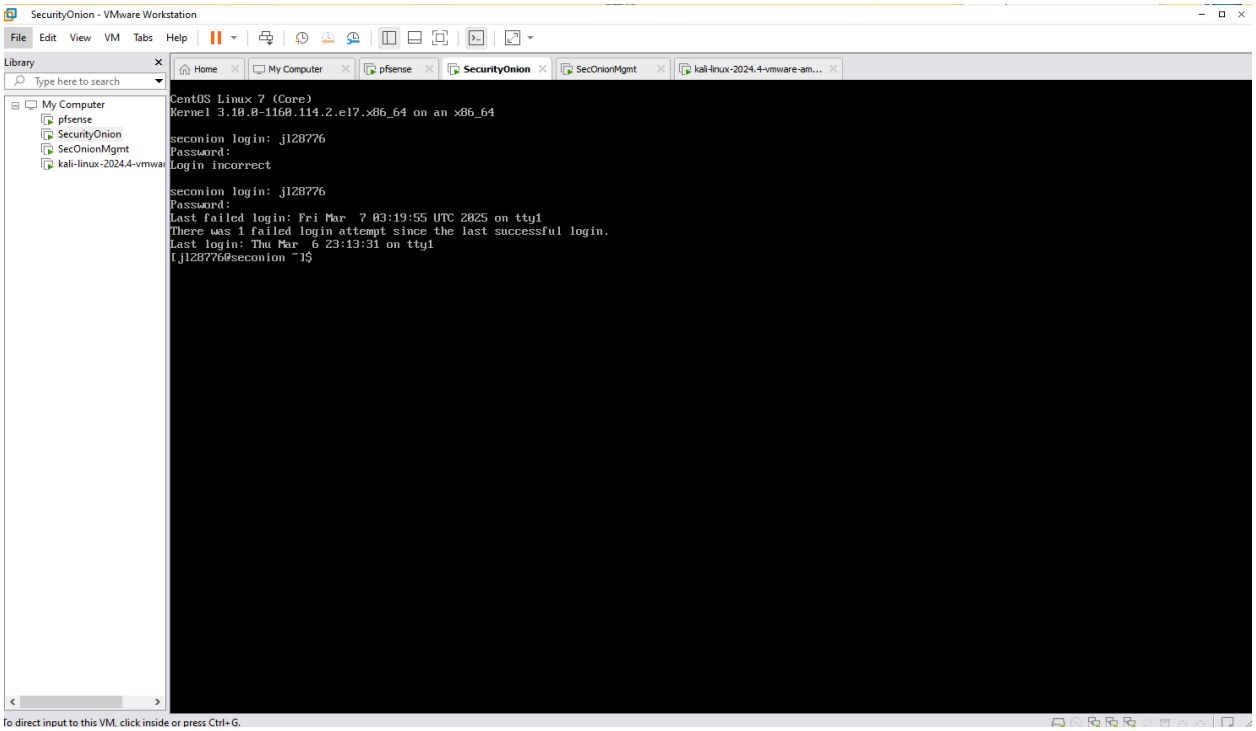

Security Onion - VMware Workstation
File Edit View VM Tabs Help
Ubuntu-Onion
kali-linux-2024.4-vmware-am...
pfsense
Windows Server 2019
Security Onion
The following options have been set, would you like to proceed?
Security Onion Version: 2.3.300
Node Type: EVAL
Hostname: seonionjl
Network: DHCP
Management NIC: ens32
Management IP: 192.168.132.137
Proxy: N/A
Bond NIC(s):
- ens34
Home Network(s):
- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12
Access URL: https://192.168.132.137
Web User: jl287760google.com
Fleet User: jl287760google.com
Enabled Optional Components:
- GRAFANA
<Yes>
<No>
Install CentOS 7 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help



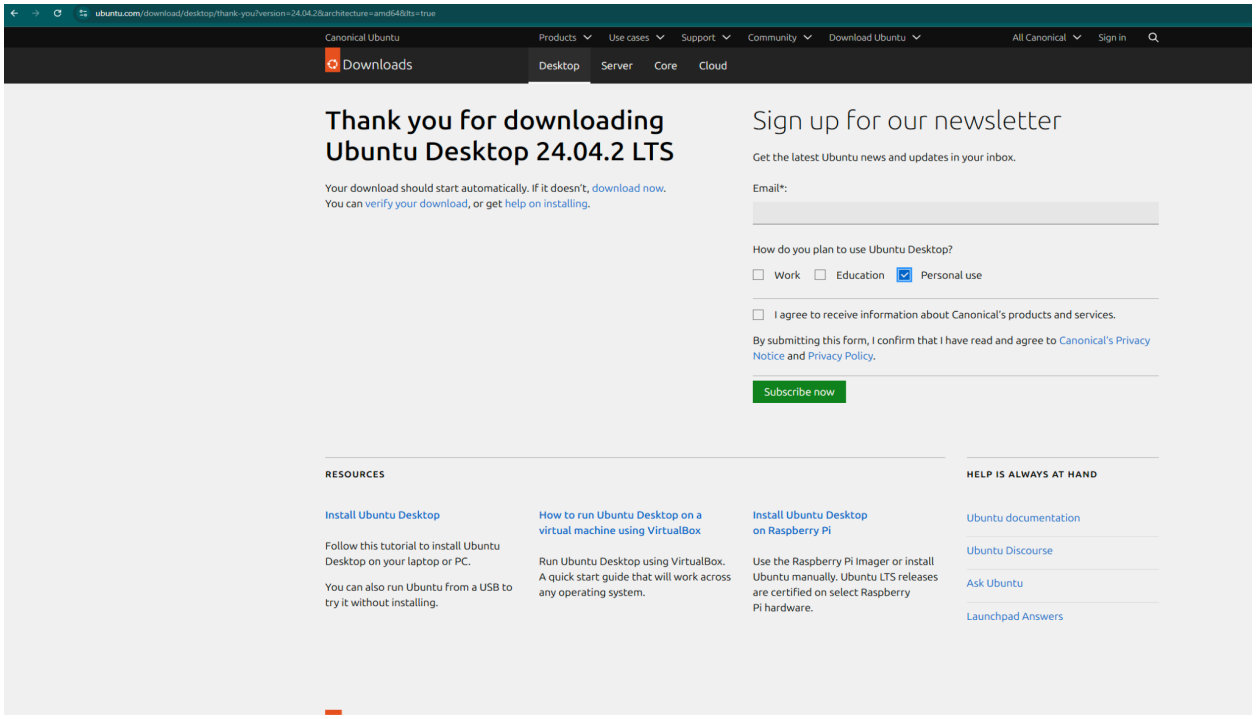
-This took around 1 hour



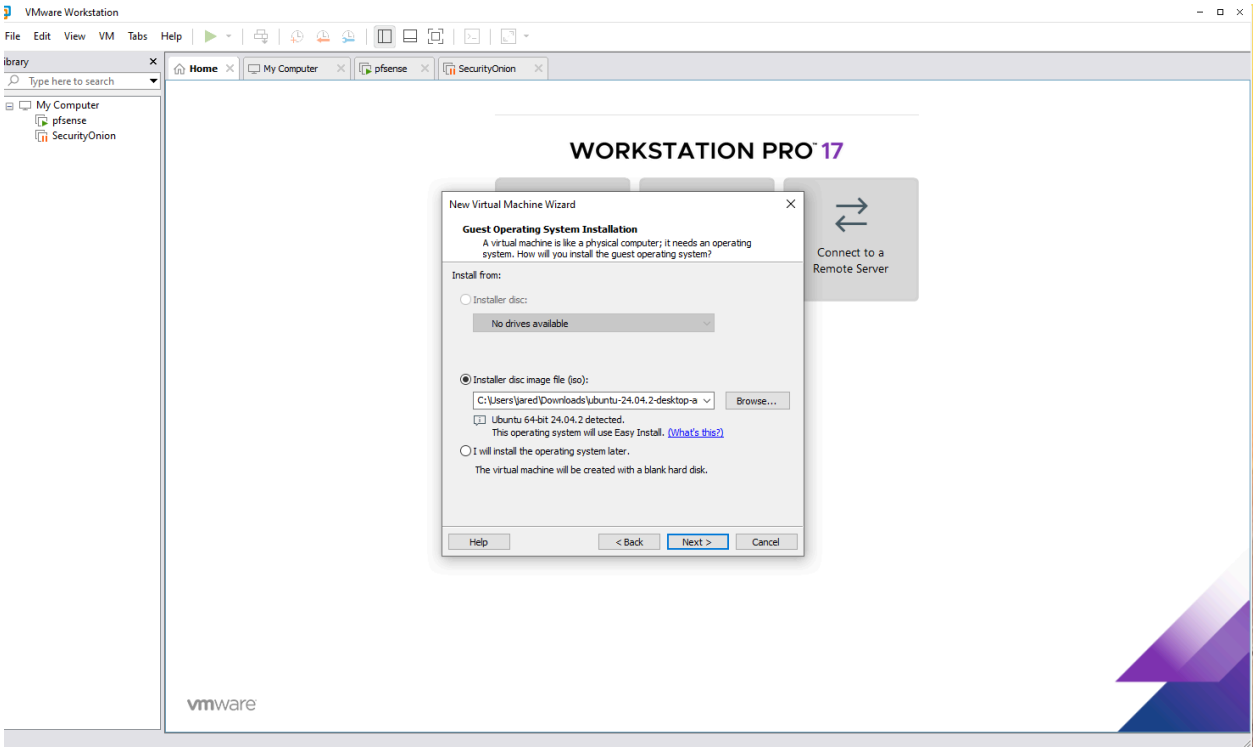
-After installation and rebooting we can login into seconion. Now we will need to configure ubuntu to allow the connection together and grab it’s ip address



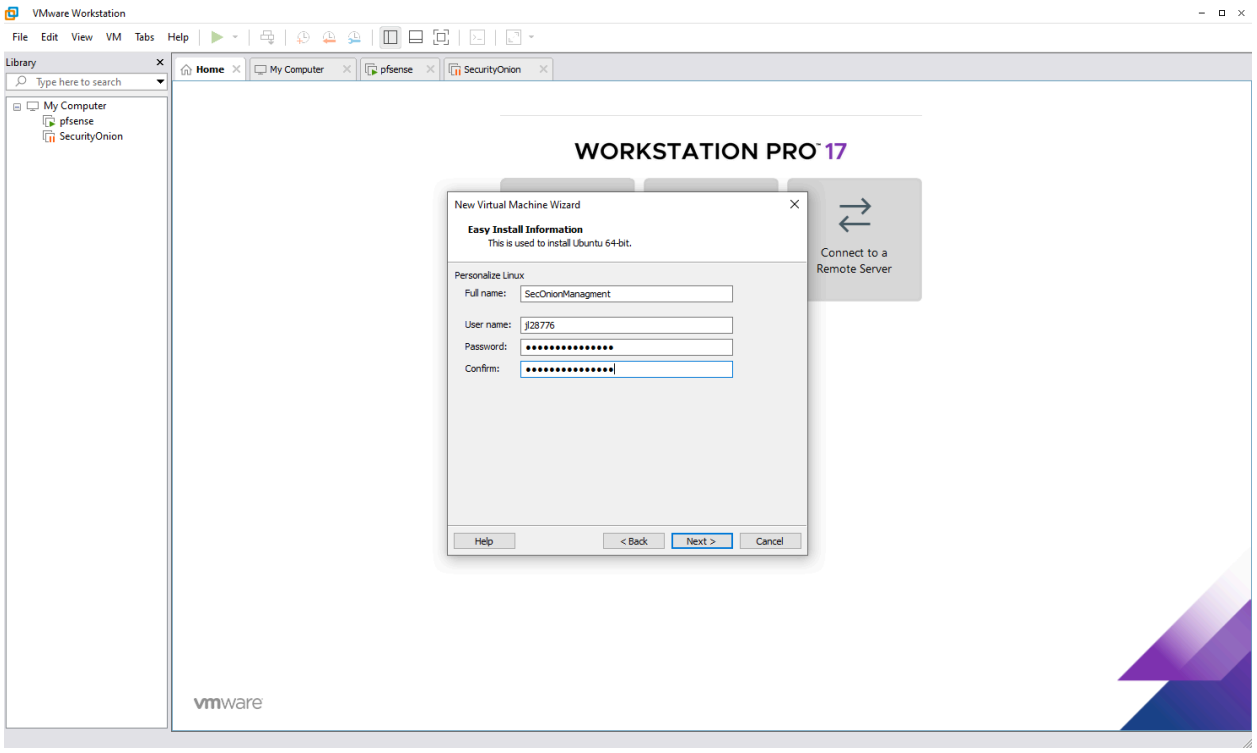
-Now we will add ubuntu as a VM host



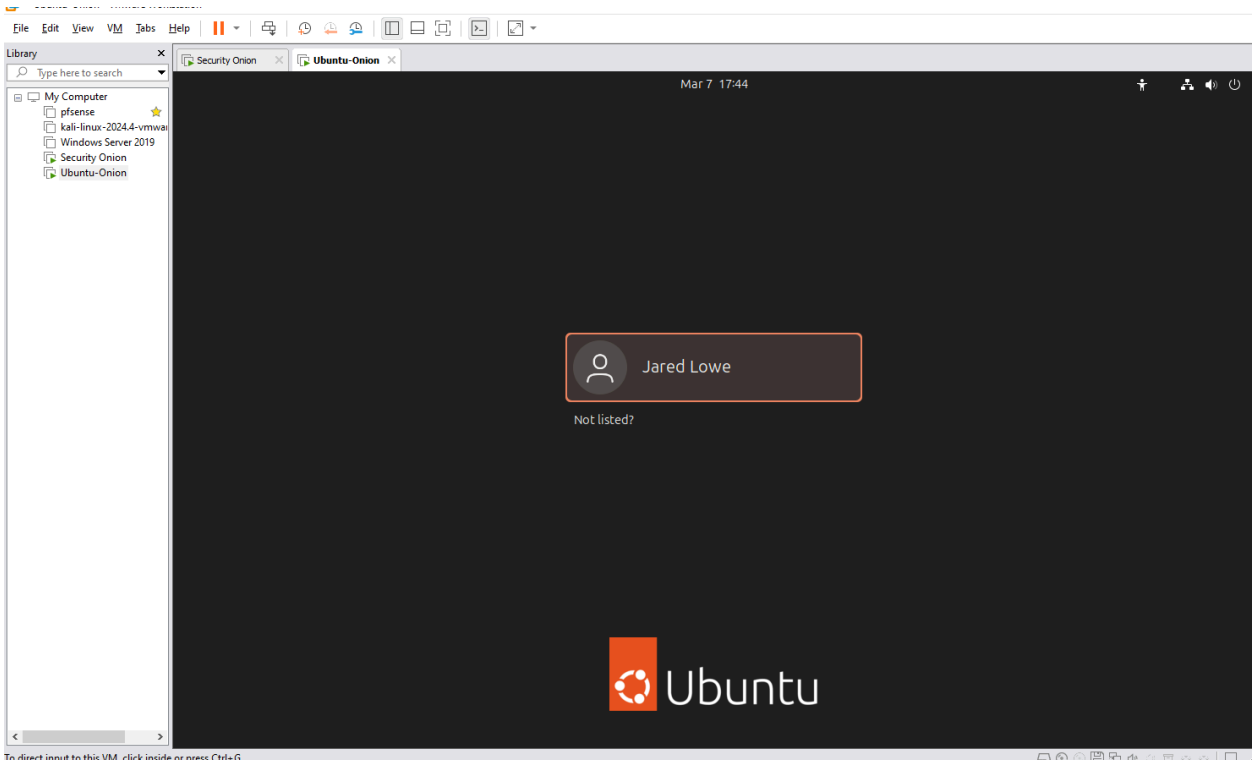
-Installing the disc image file (iso)



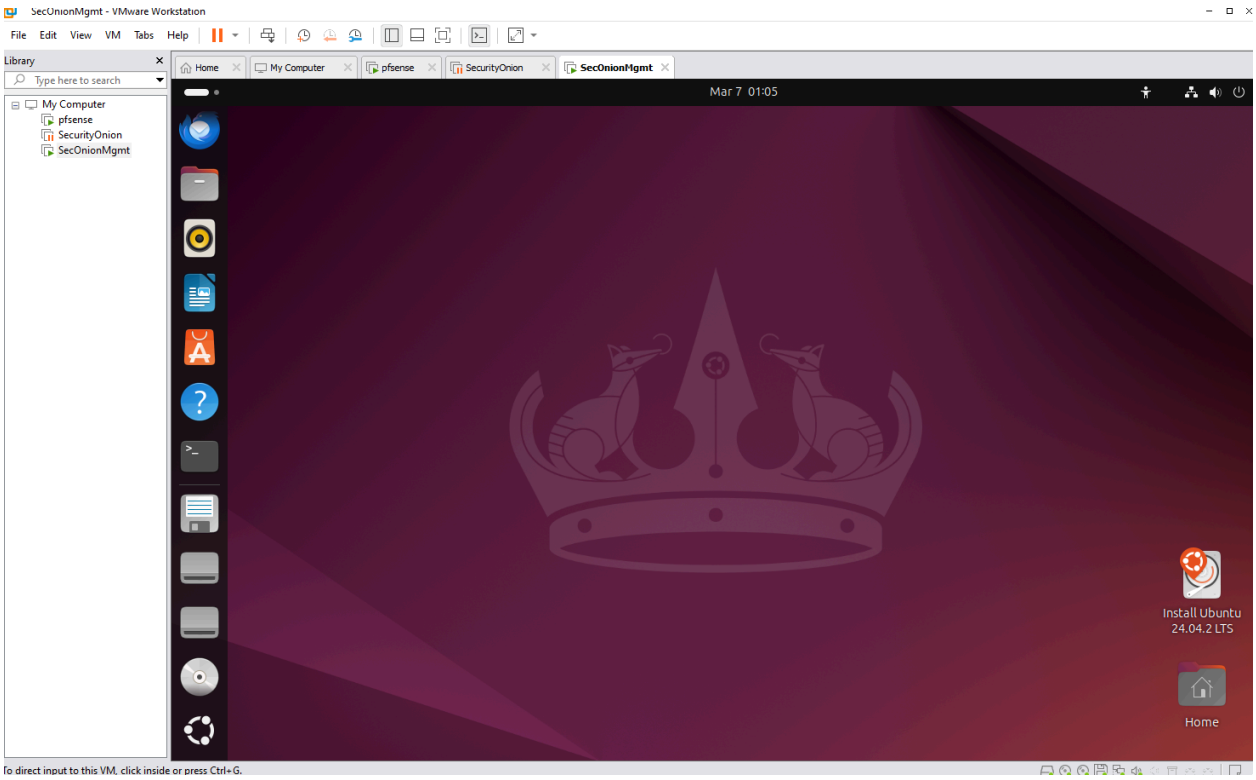
-Going to initialize it with the security onion so I named it SecOnionManagment and gave it a username and password. Also why we do not add any other configurations



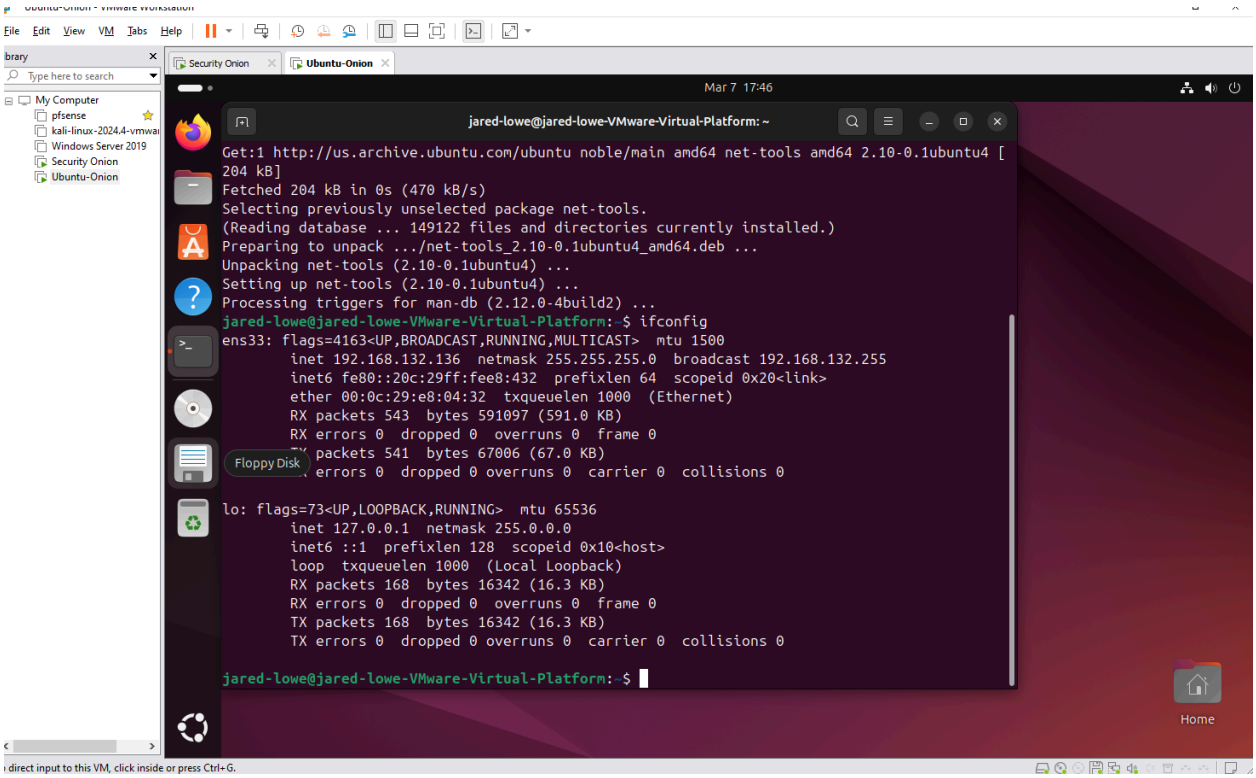
-after default set up we get access to the ubuntu login



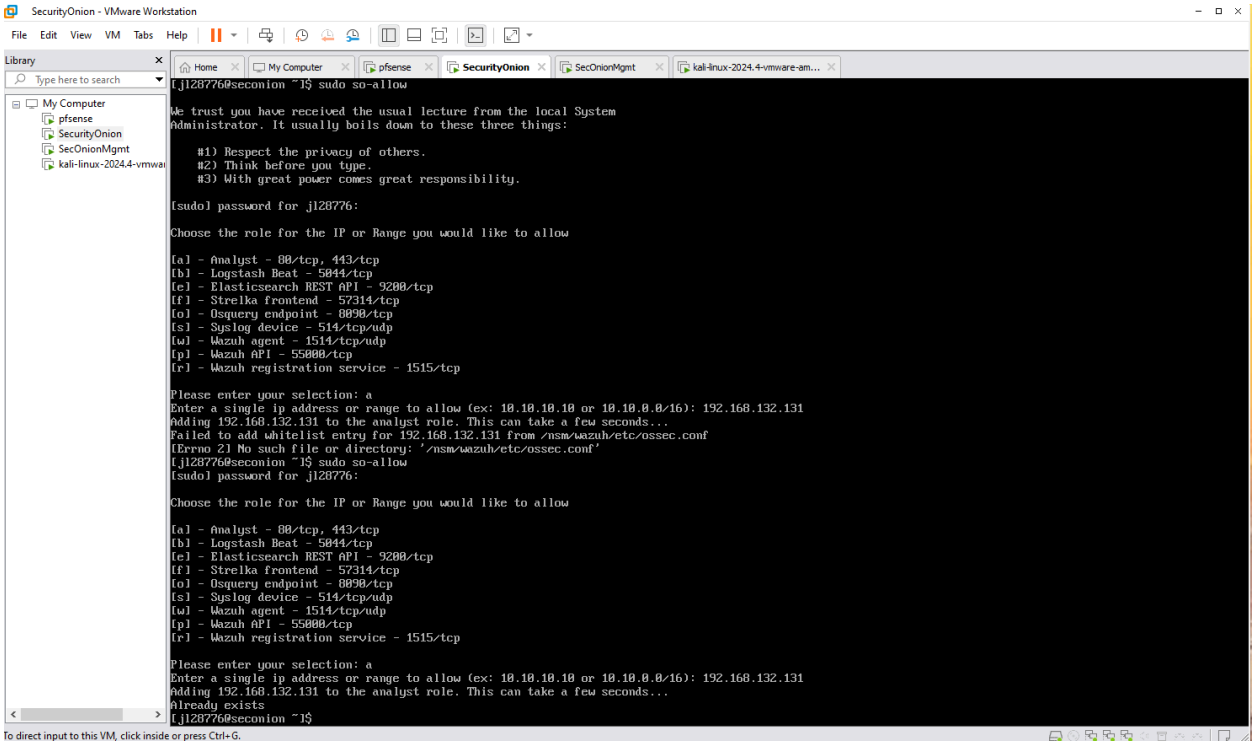
-Now entering the Ubuntu VM

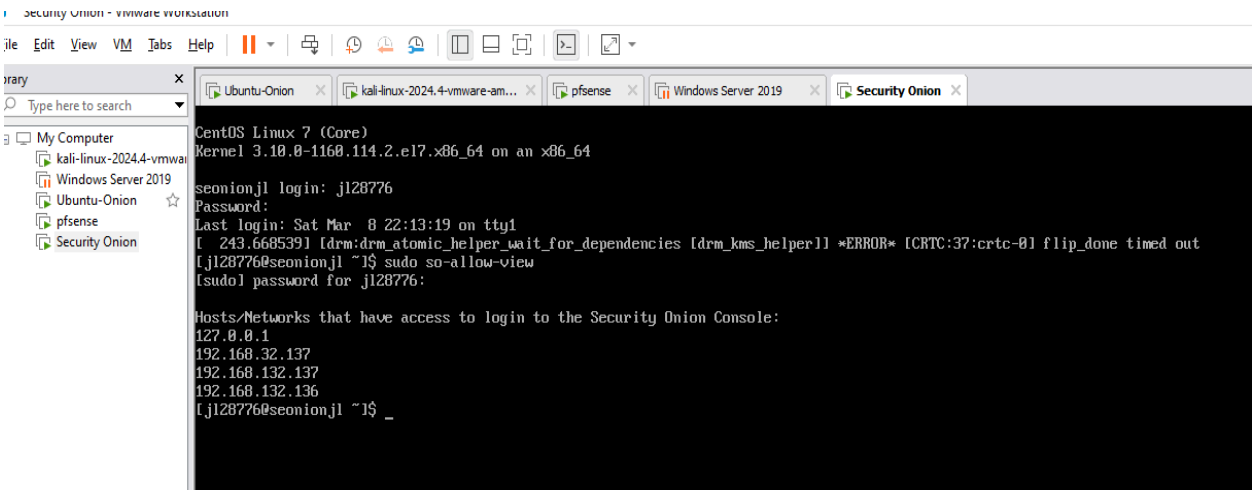


-I used install net tool to be able to use ifconfig and get the ip address for future use

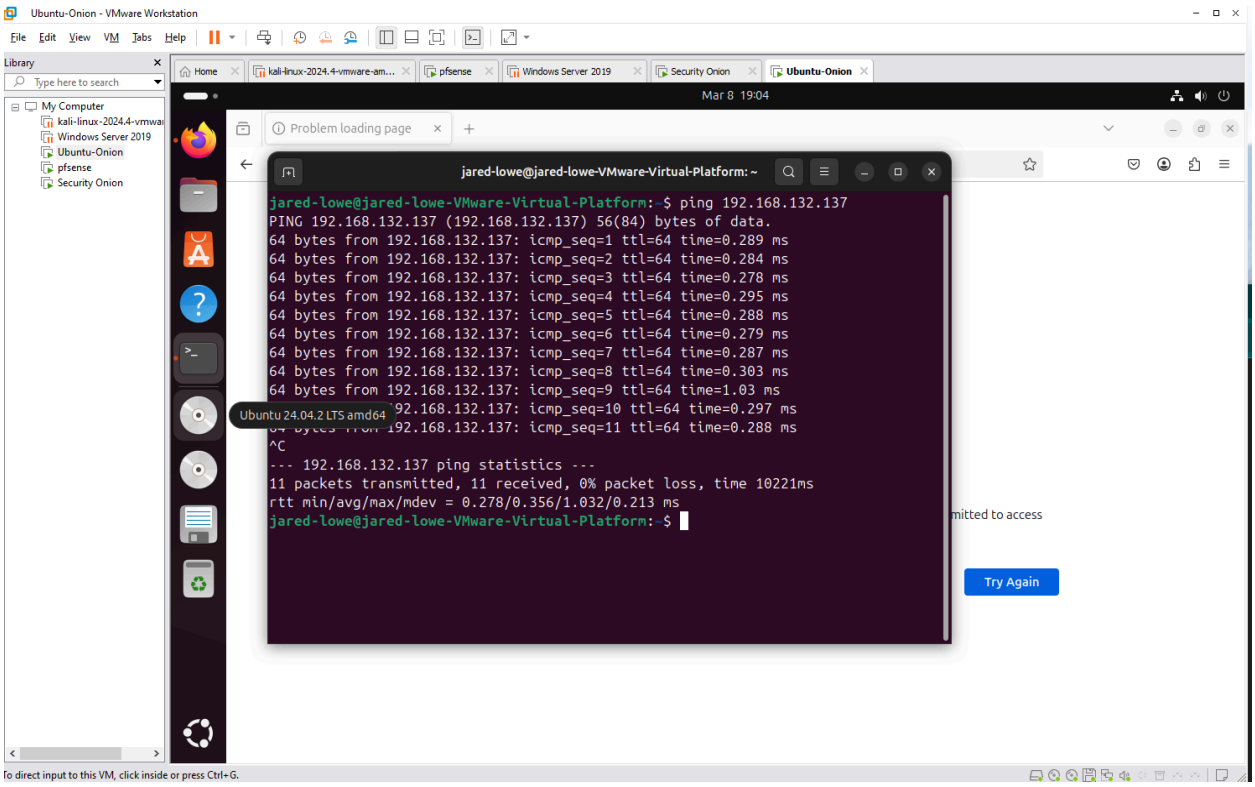


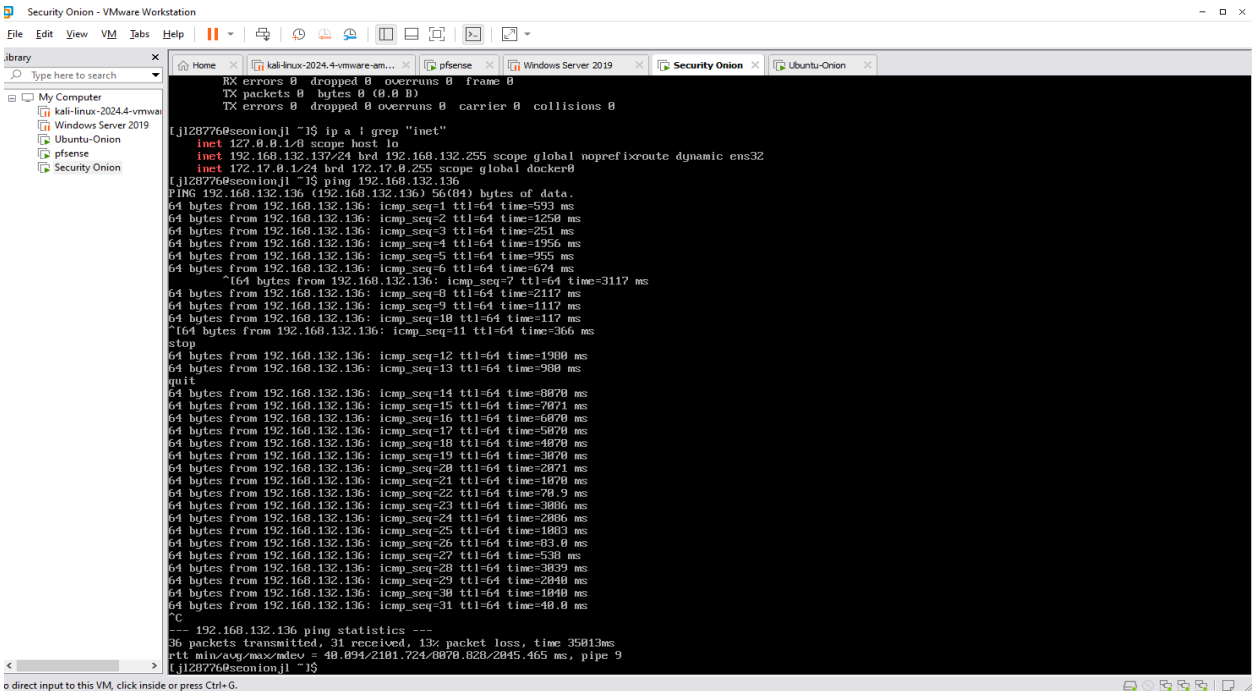
-After 2nd attempt we added the ubuntu vm to the analyst role



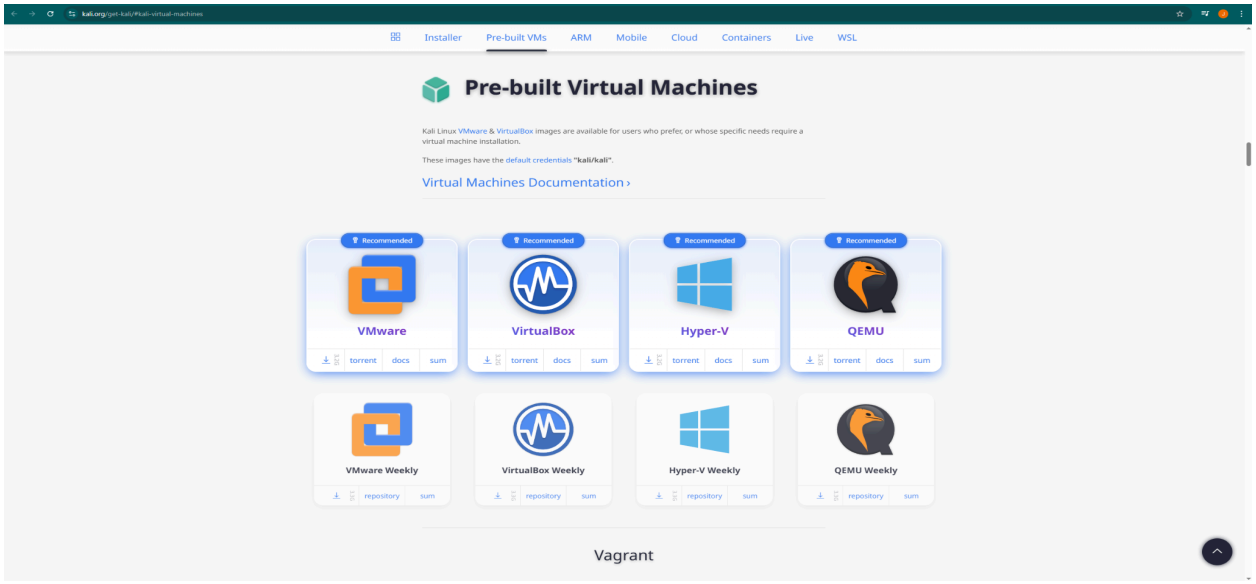


NOTE:I WAS UNABLE TO ACCESS THE UBUNTU THROUGH http://192.168.132.137 ON UBUNTU BUT SET PINGS FROM BOTH THE ONION AND UBUNTU SO IT CAN BE REACHED BUT AFTER A WEEK TRYING TO FIGURE IT OUT I GOT THIS AND THEN I WILL EVENTUALLY FIX IT(2 IMAGES SHOWING PING)

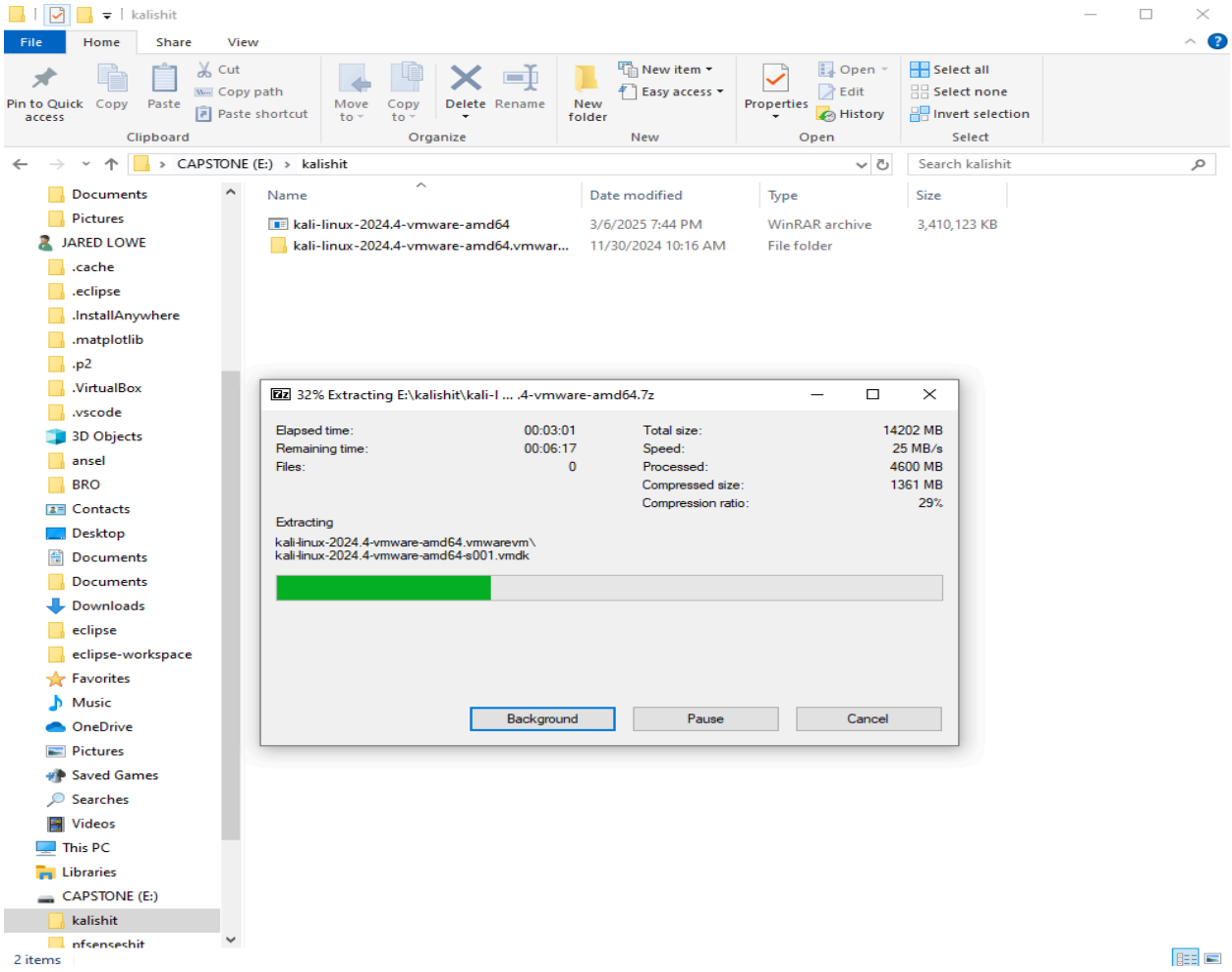




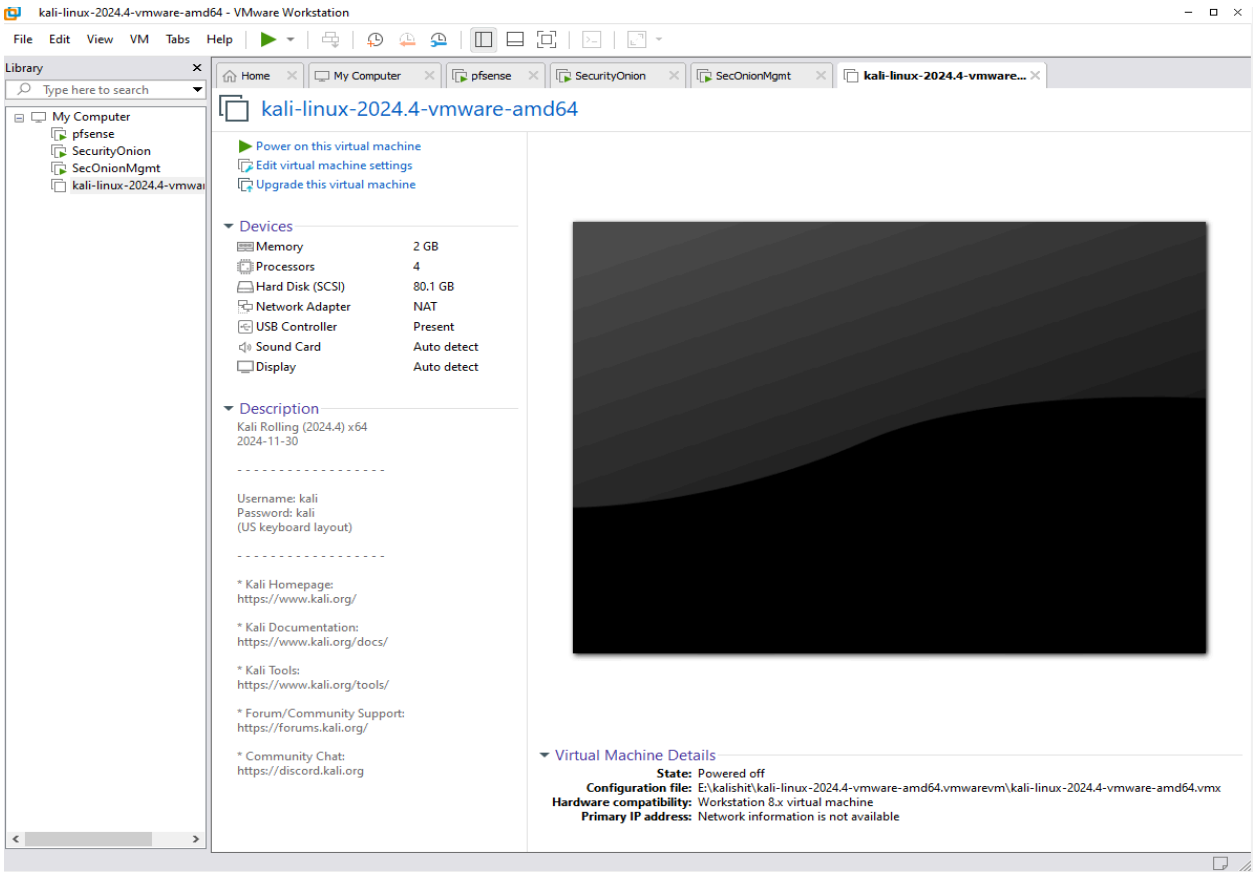
-Now we are going to add the attack machine which is Linux



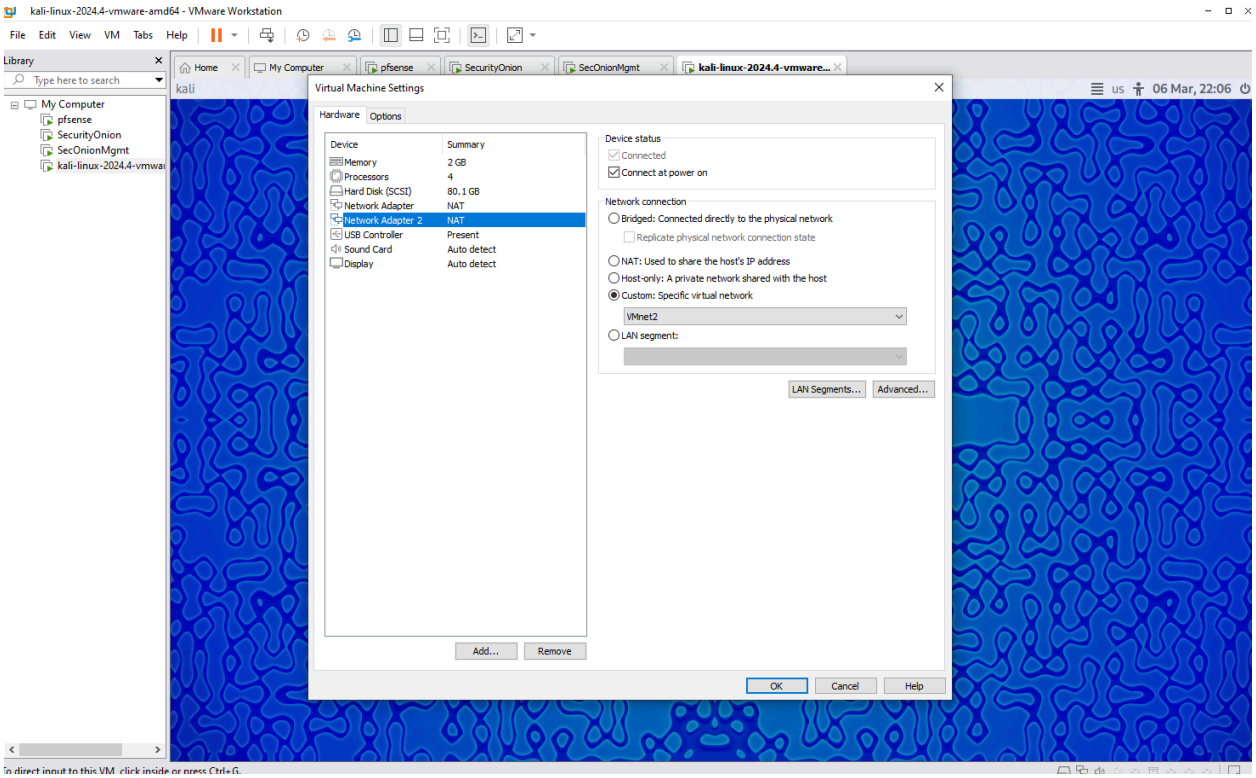
-Unzipping the file



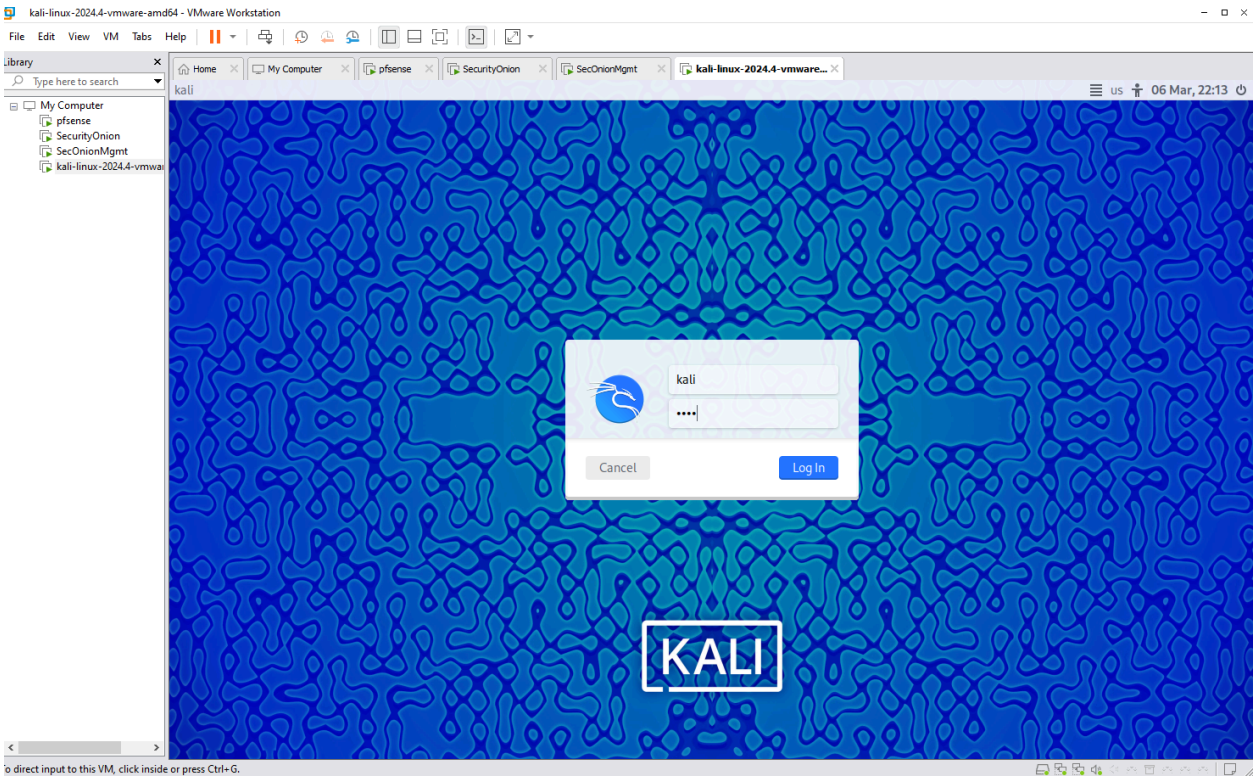
-Instead I used open a virtual machine and find the Kali-Linux disc file and open to immediately get the VM



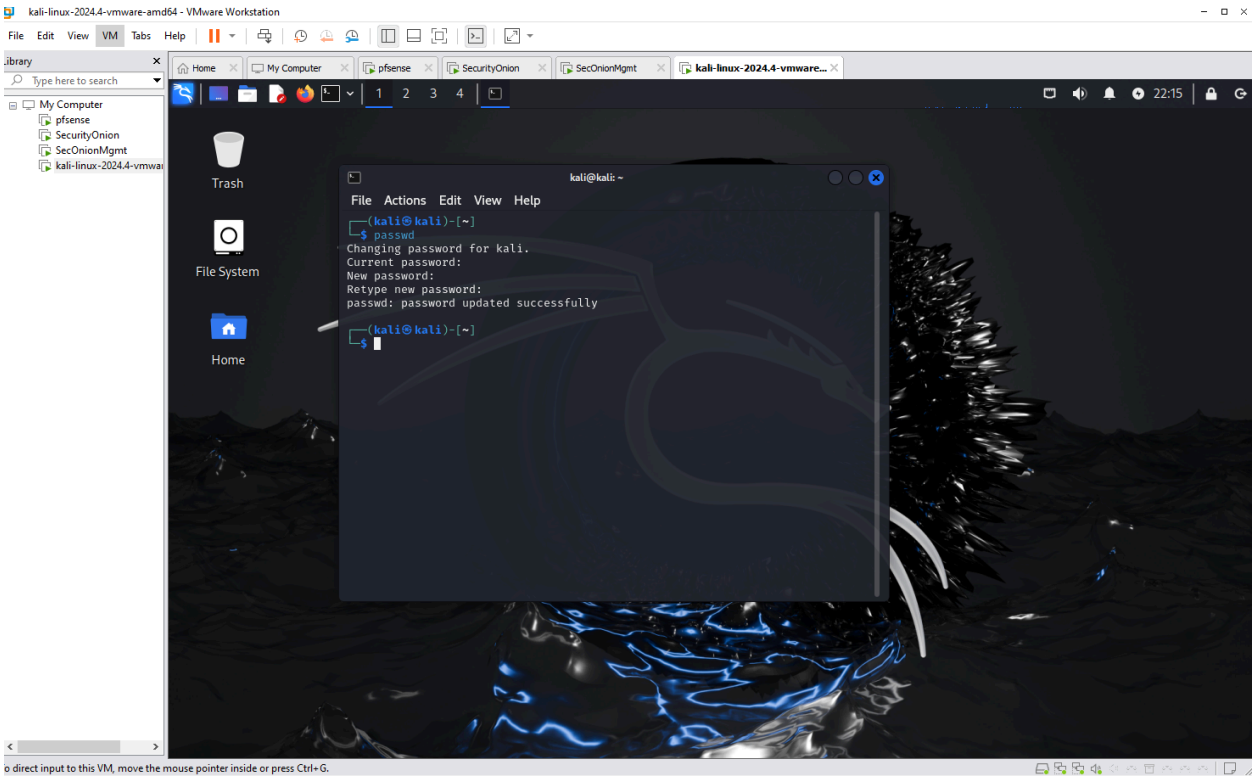
-Adding a new network adapter that has vmnet2 network



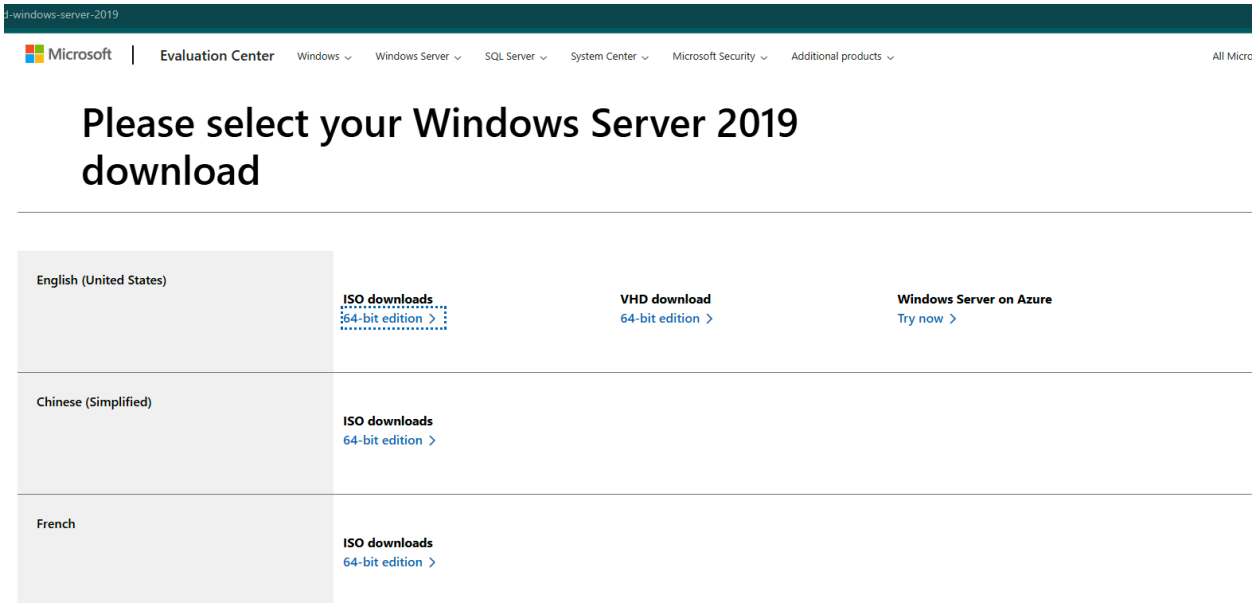
-Now can access it



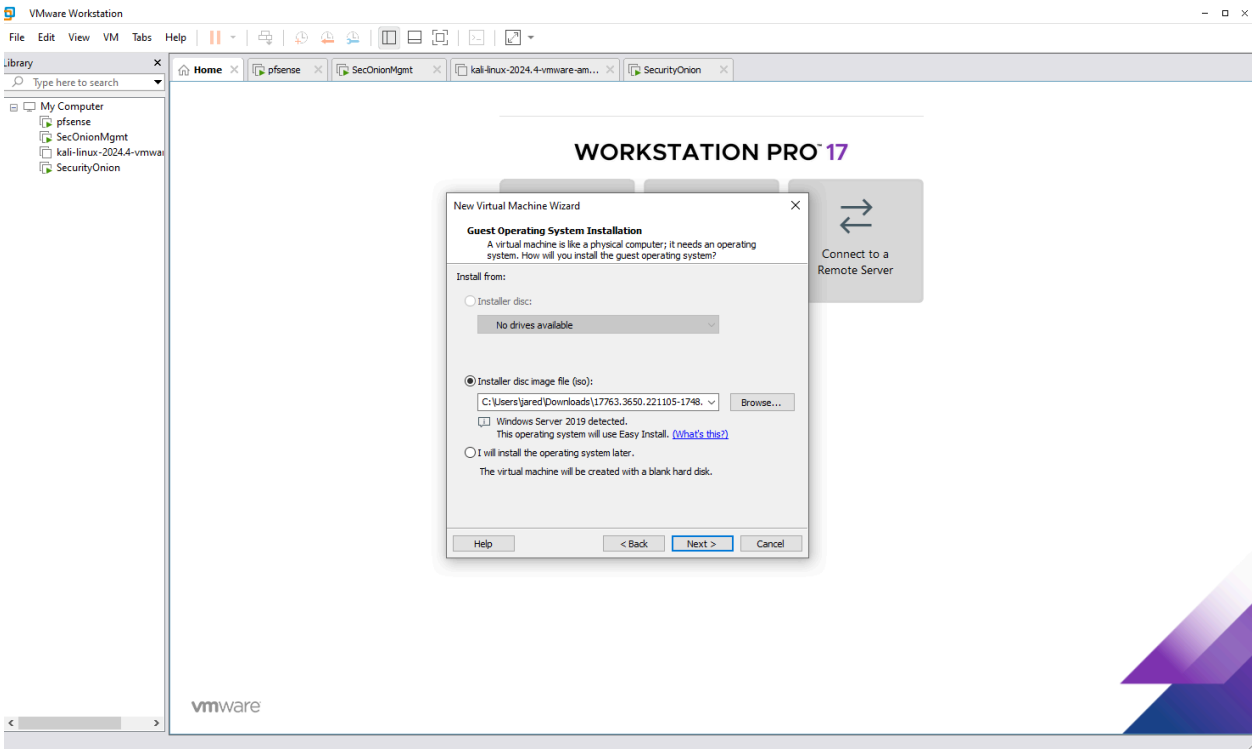
-Now creating a unique password. This is all for this installation because we will soon use this to attack systems and also change pfsense settings.



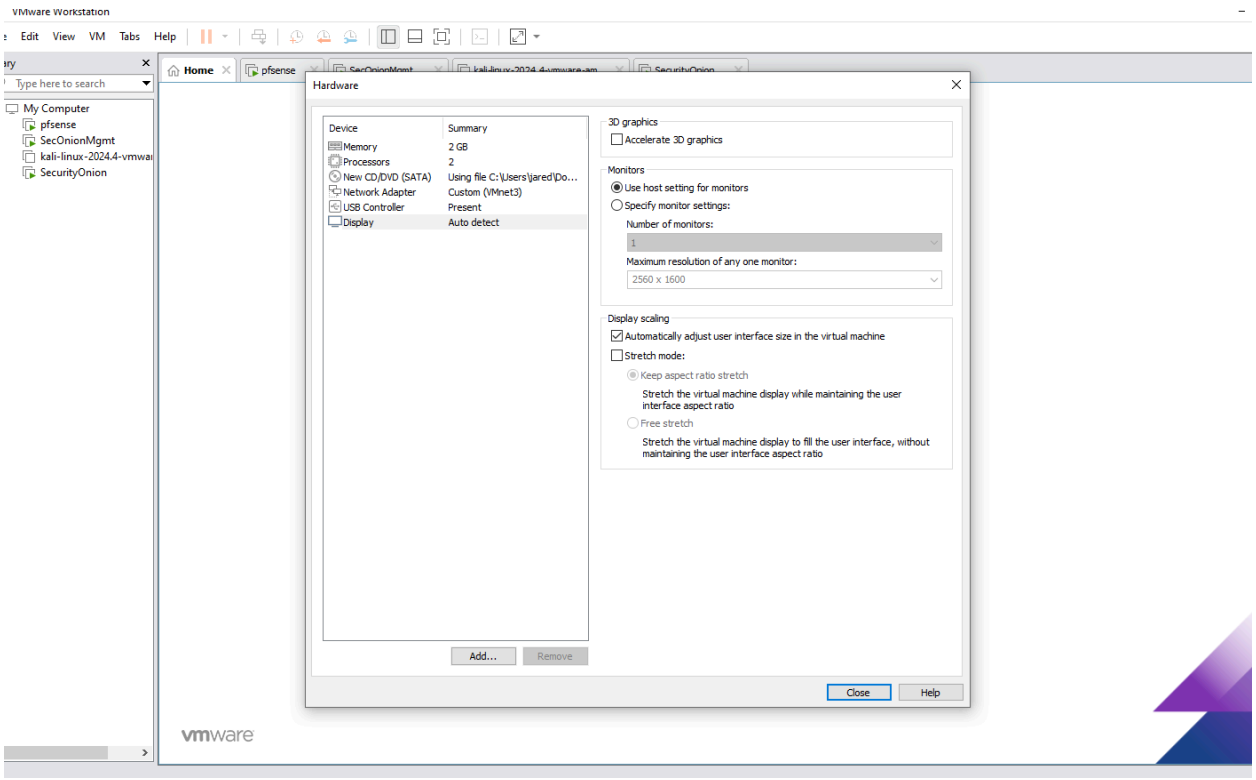
-Now we are going to add a windows VM



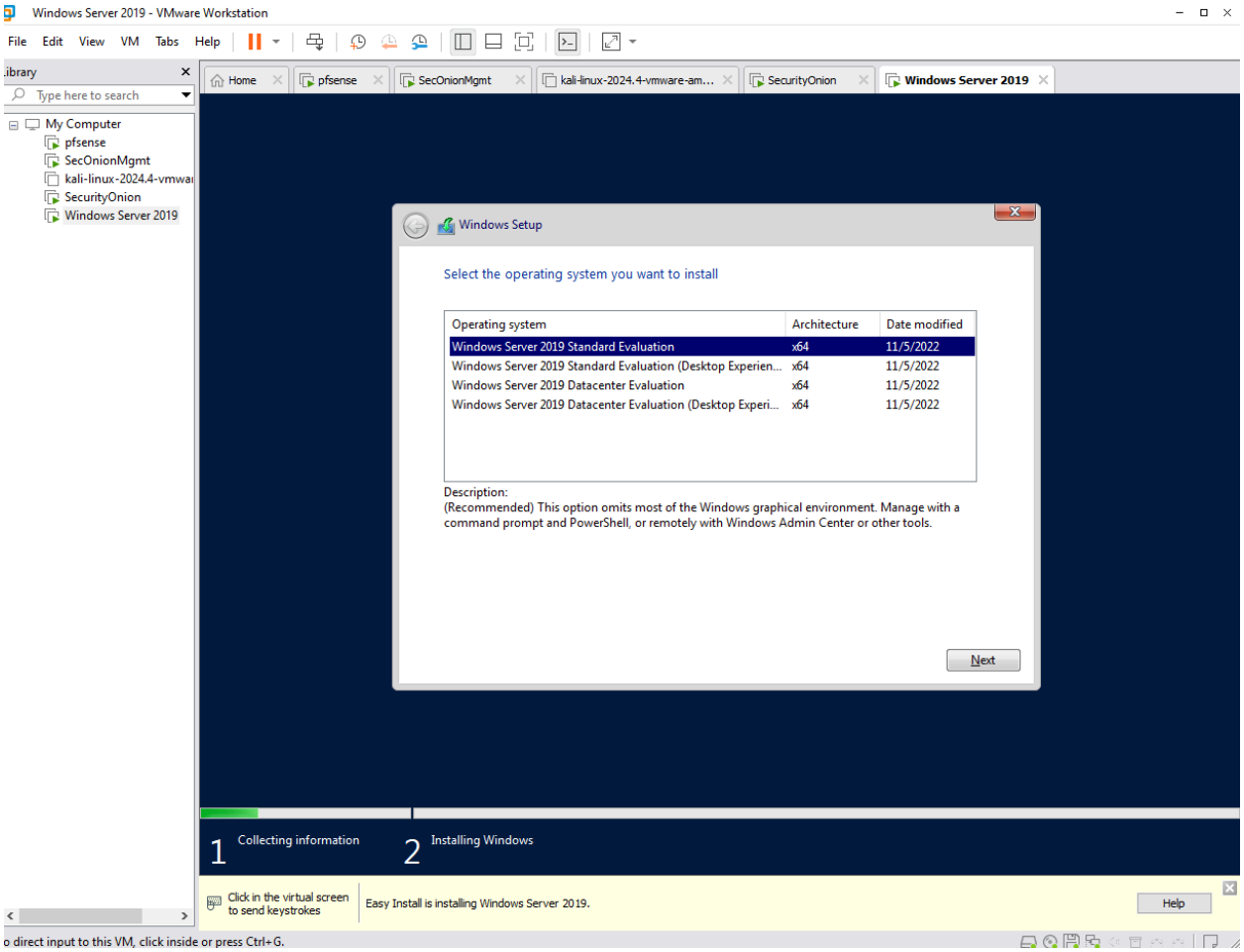
-Adding the windows server as a VM



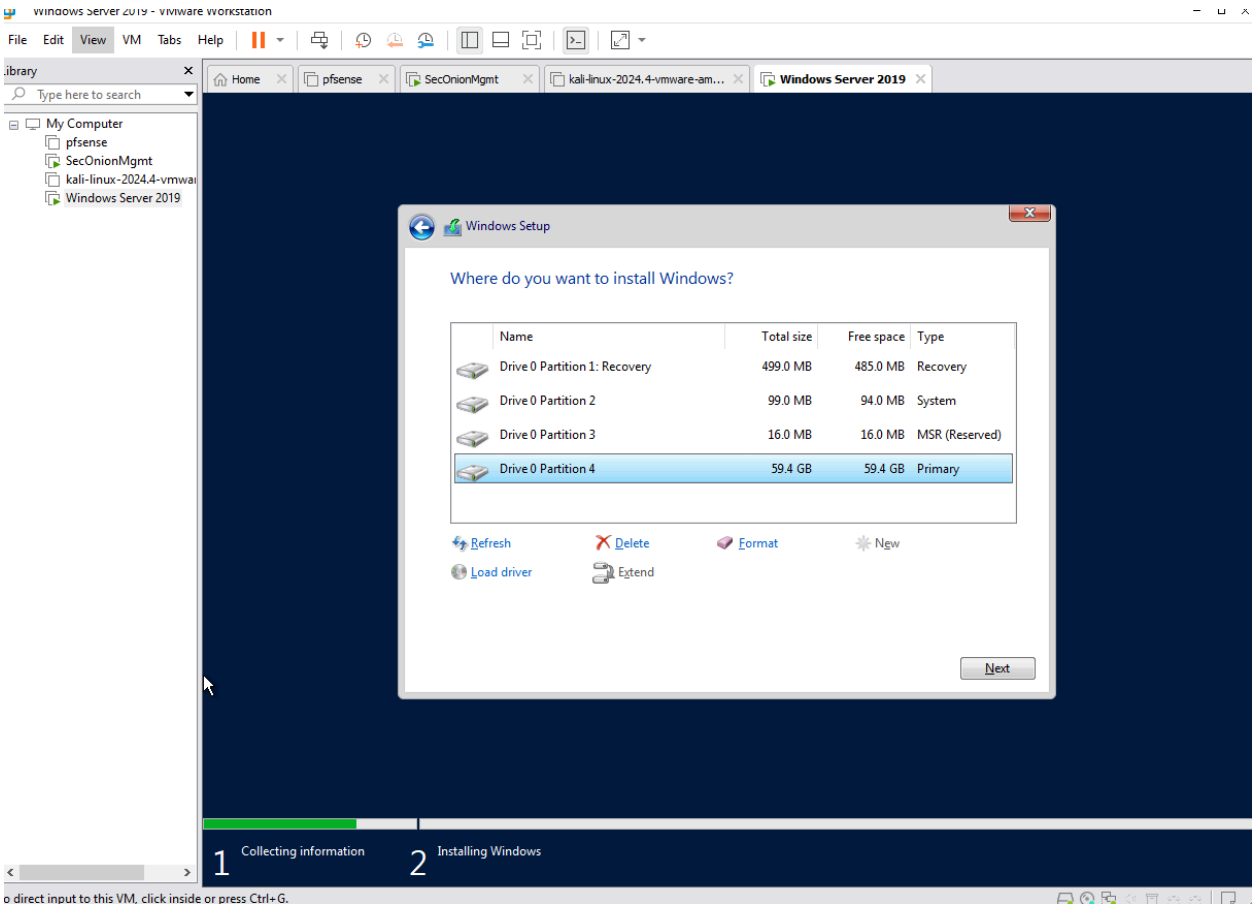
-Keeping default expect changing the network adapter to our vmnet3



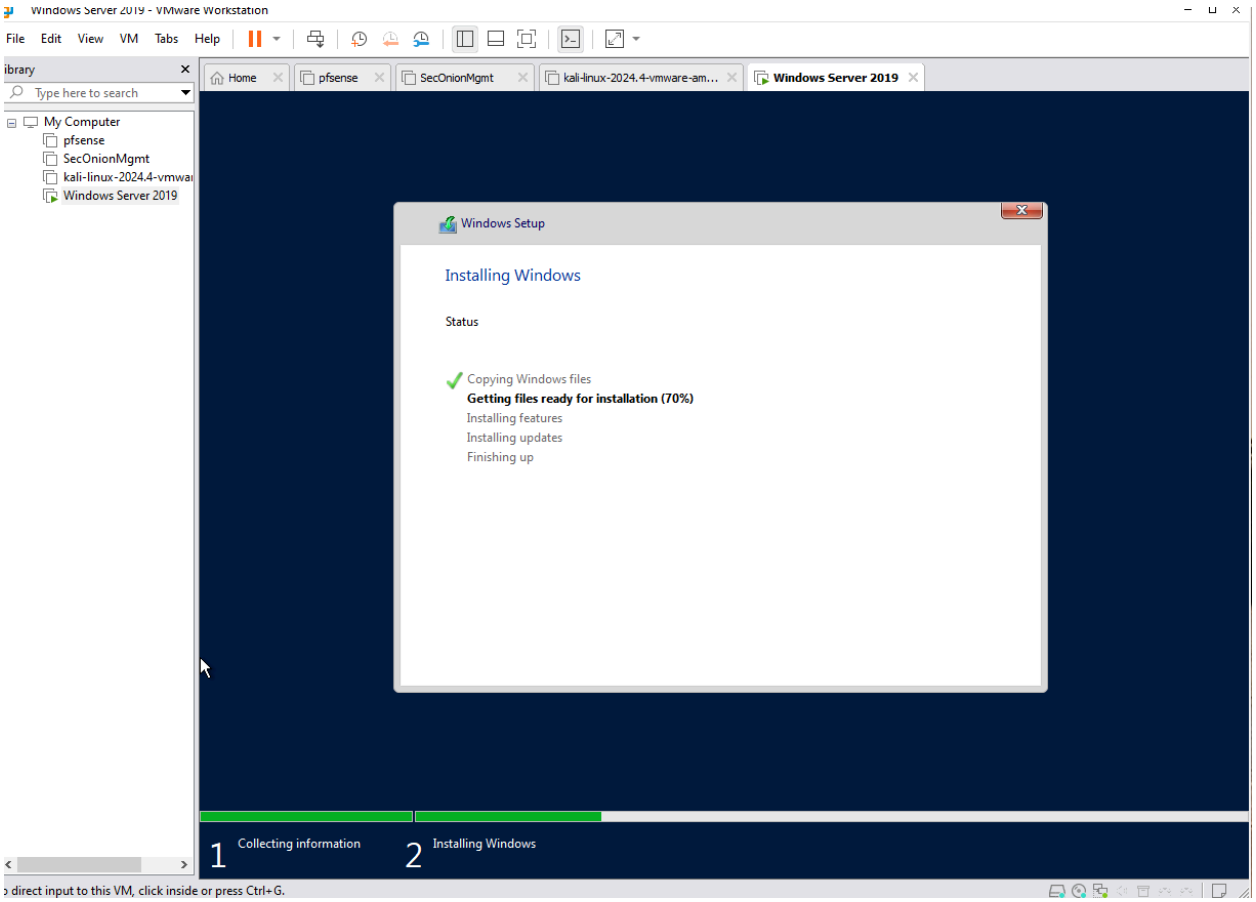
-Entering the windows server selecting the second option



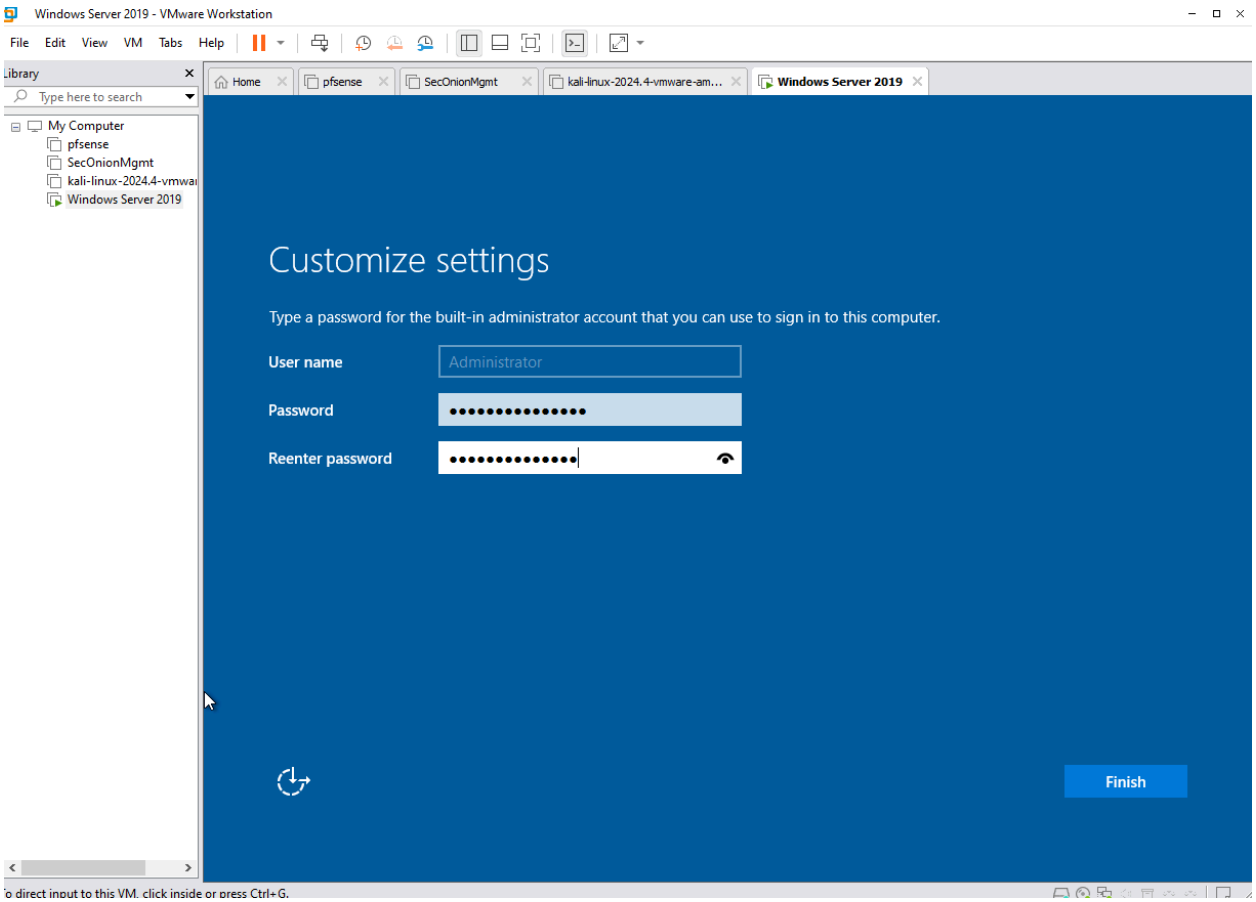
-Now we have created a new custom installation



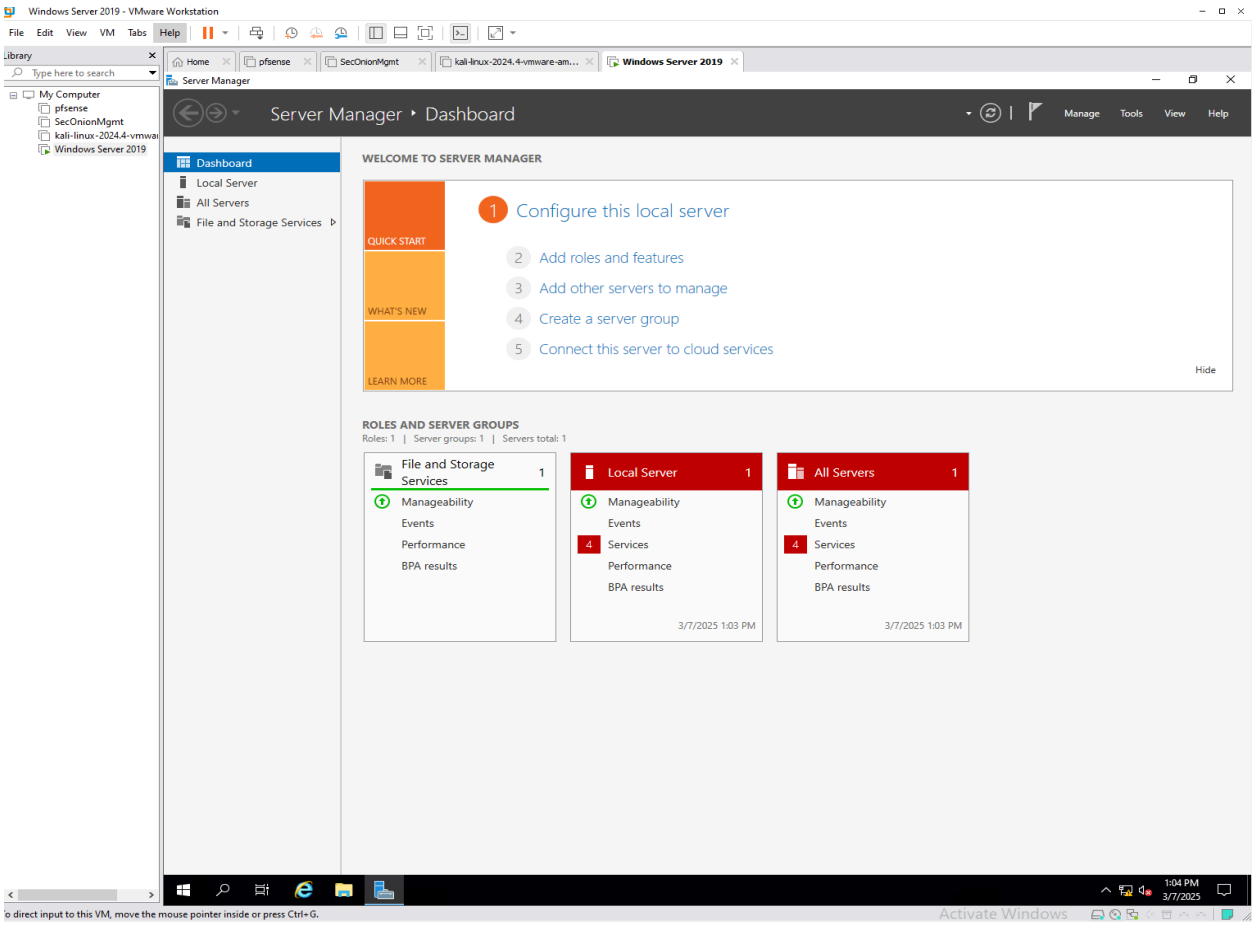
-Waiting for installation of windows



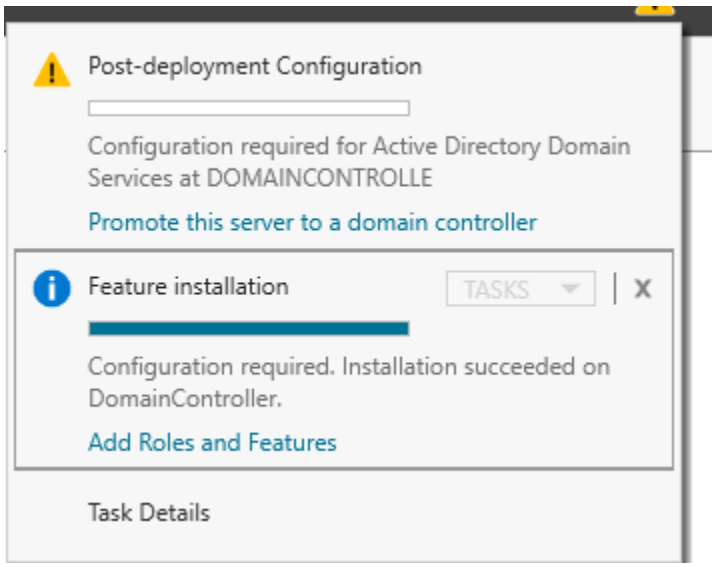
-Creating a new password



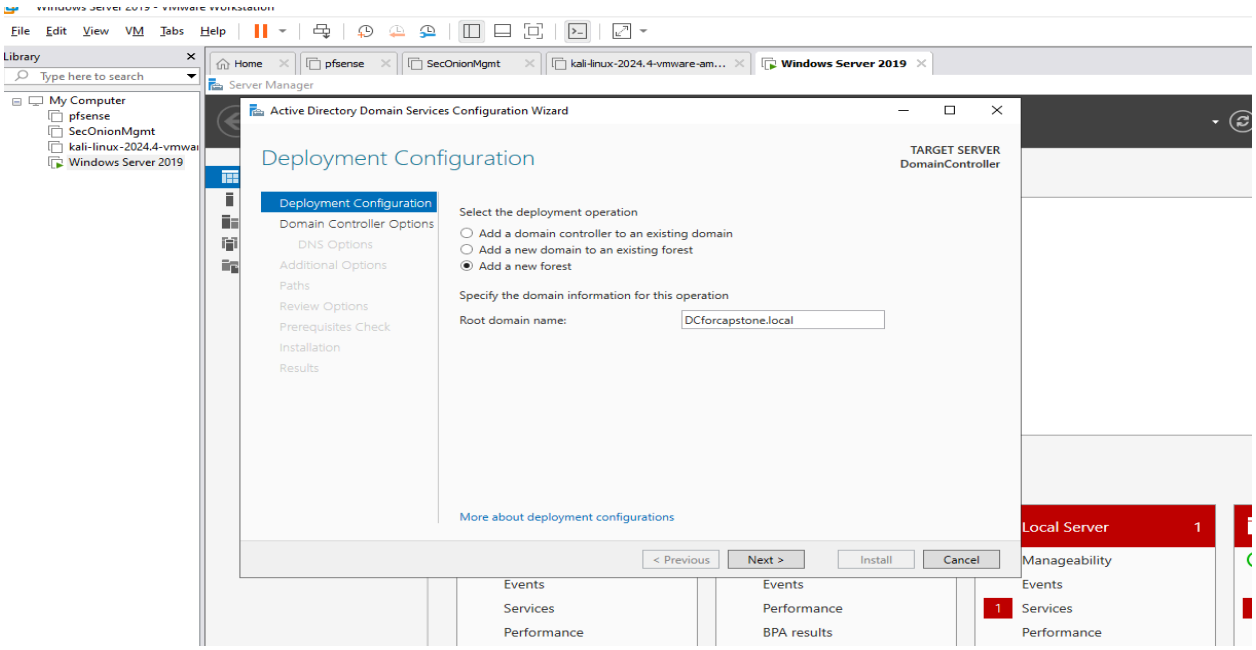
-After entering the password we are sent to the server manager dashboard



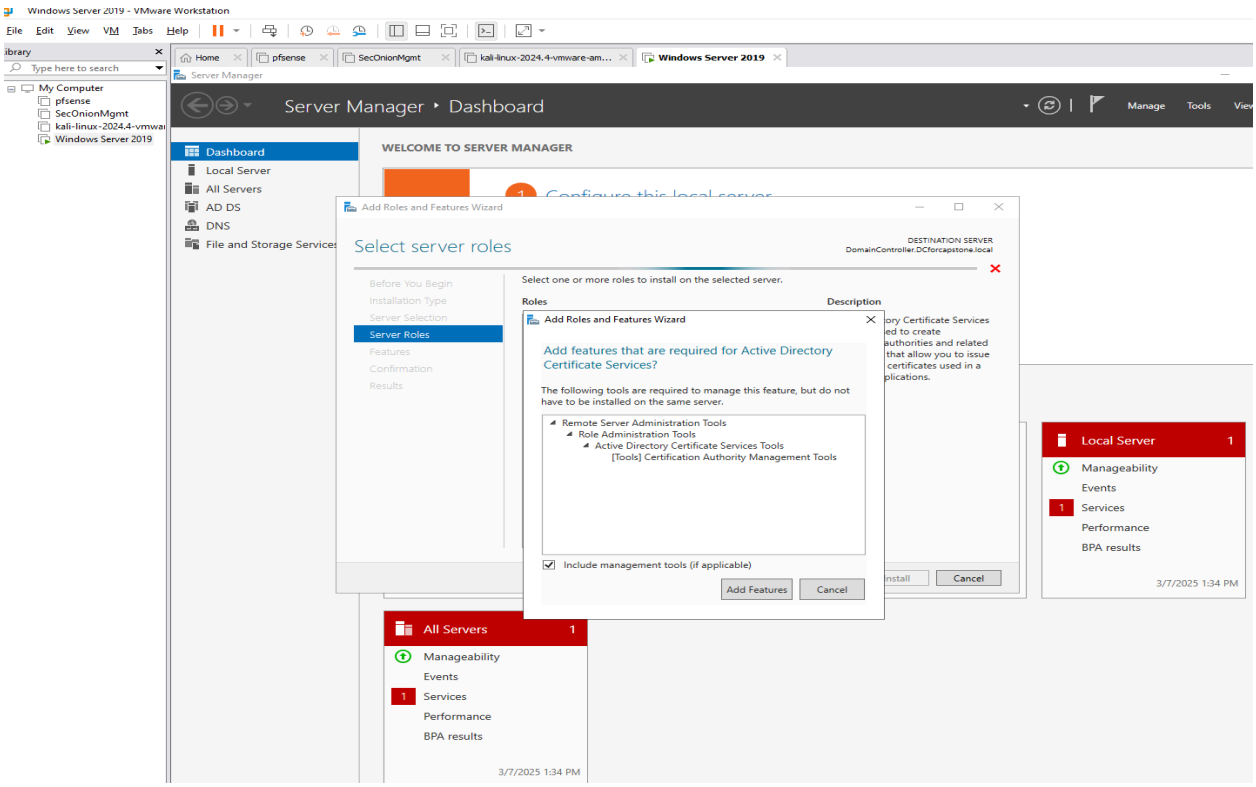
-Going to manage then add roles and features to then add the active directory domain service roles. Then we get a flag to add the server to domain controller



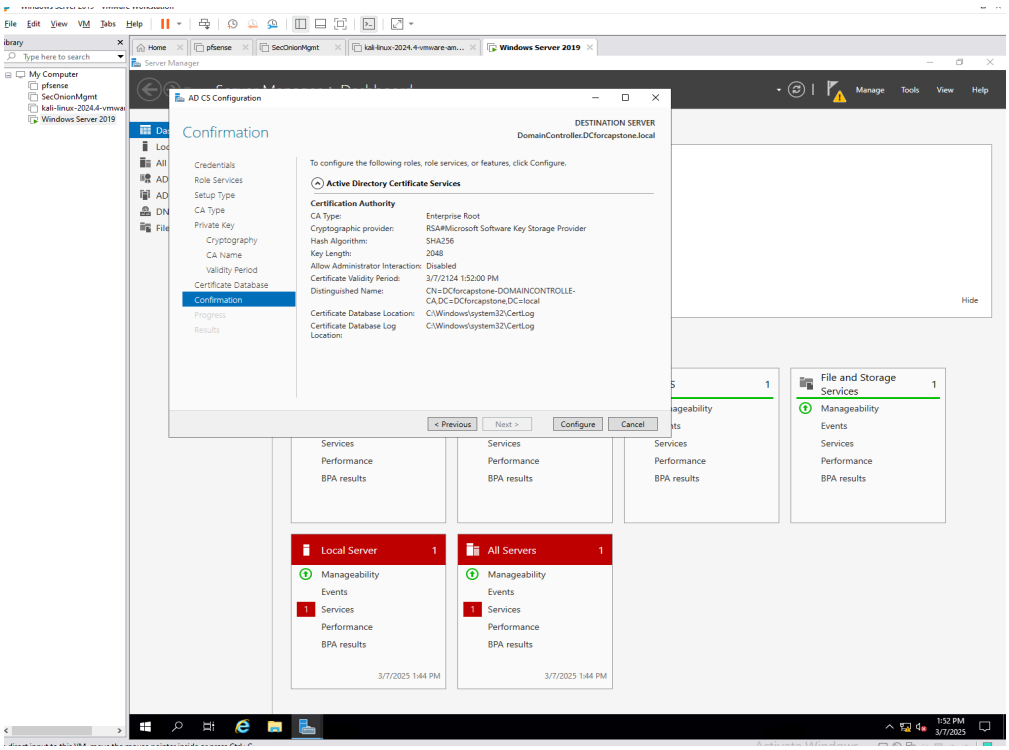
-We can now add the domain controller with a root name and password. We will then install and wait for the reboot



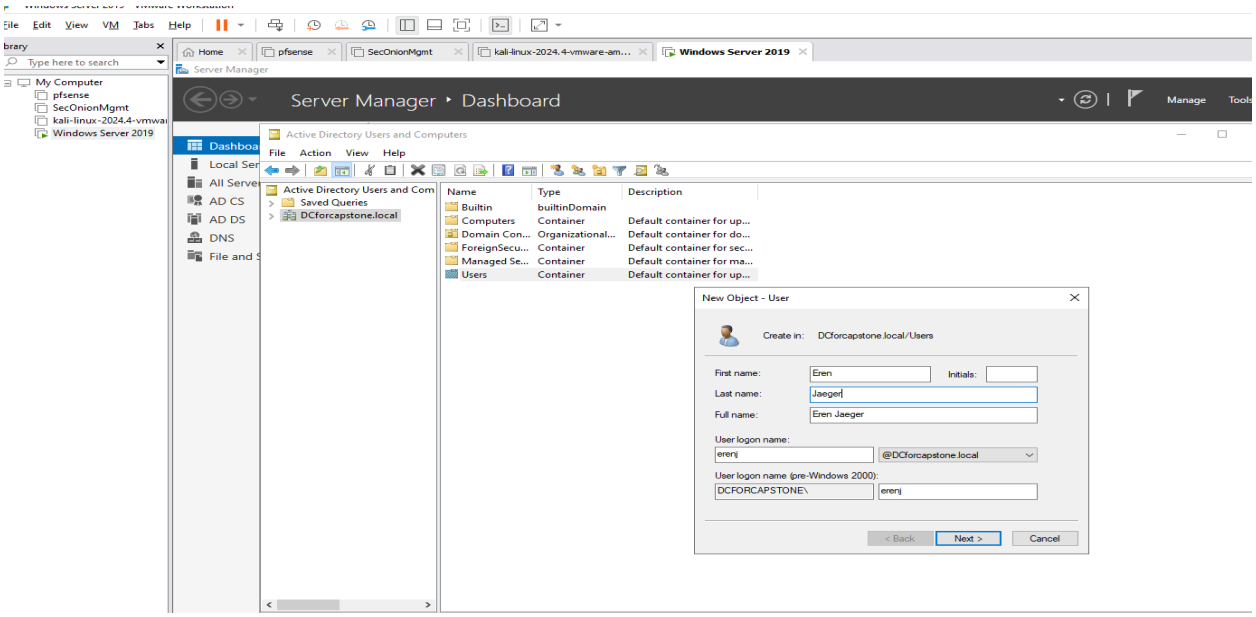
-we will now add the active directory certificate service to the server roles



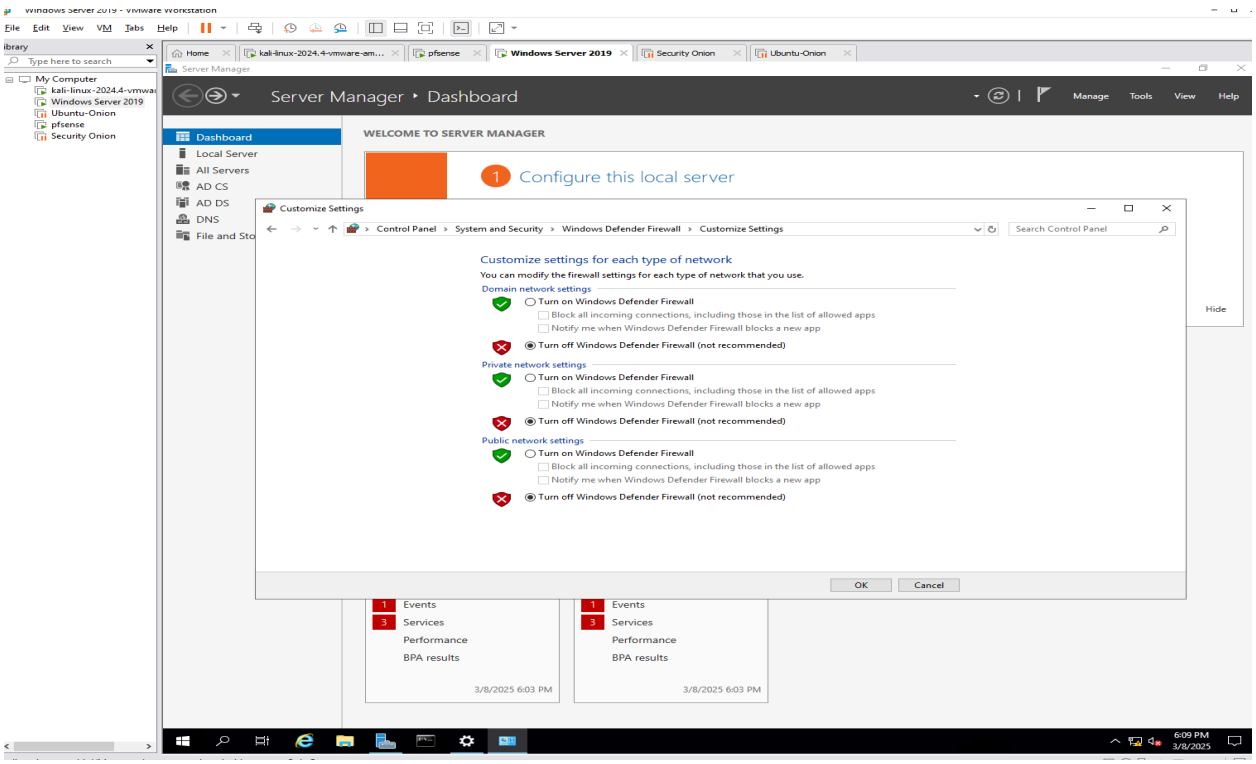
-We then enter the flag for the certificate services and enter credentials to establish the certificate. Then after restarting it to initialize the change.



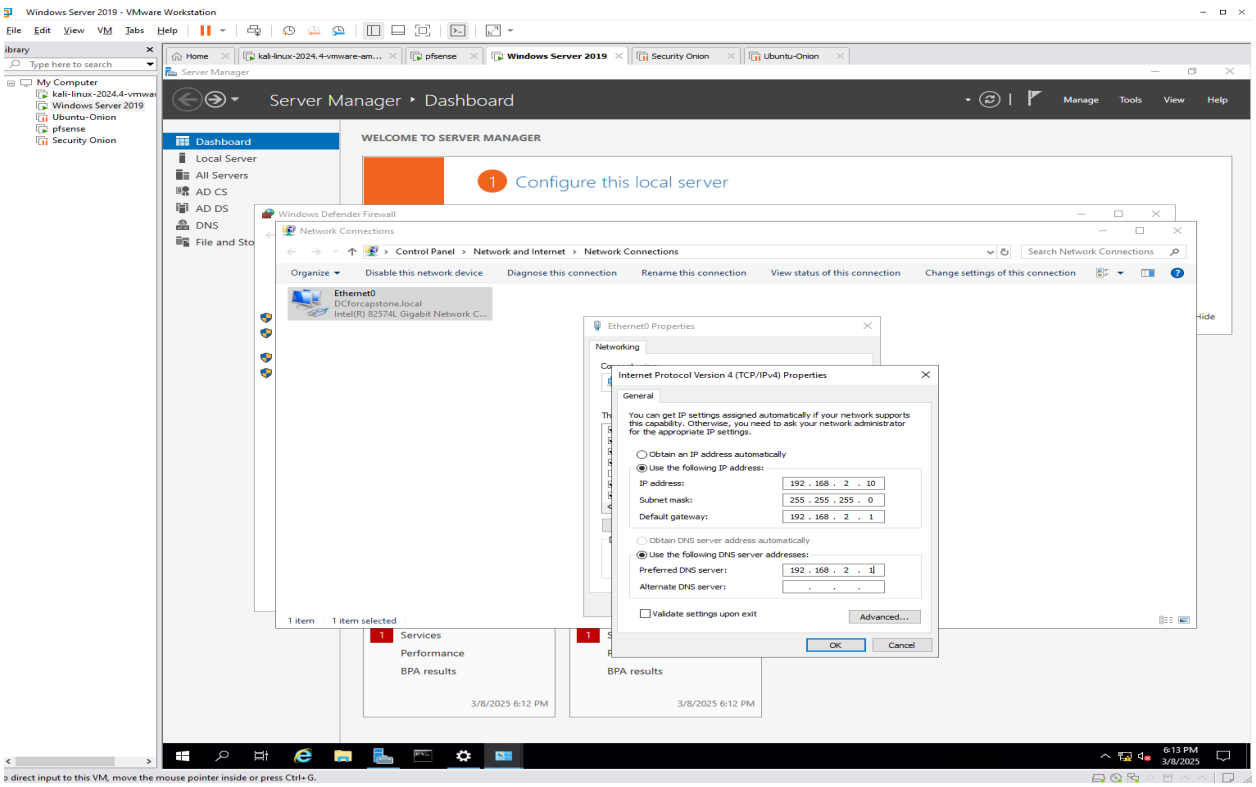
-Entering Tools-DC-Users-to create a new user called Eren Jaeger and creating a password



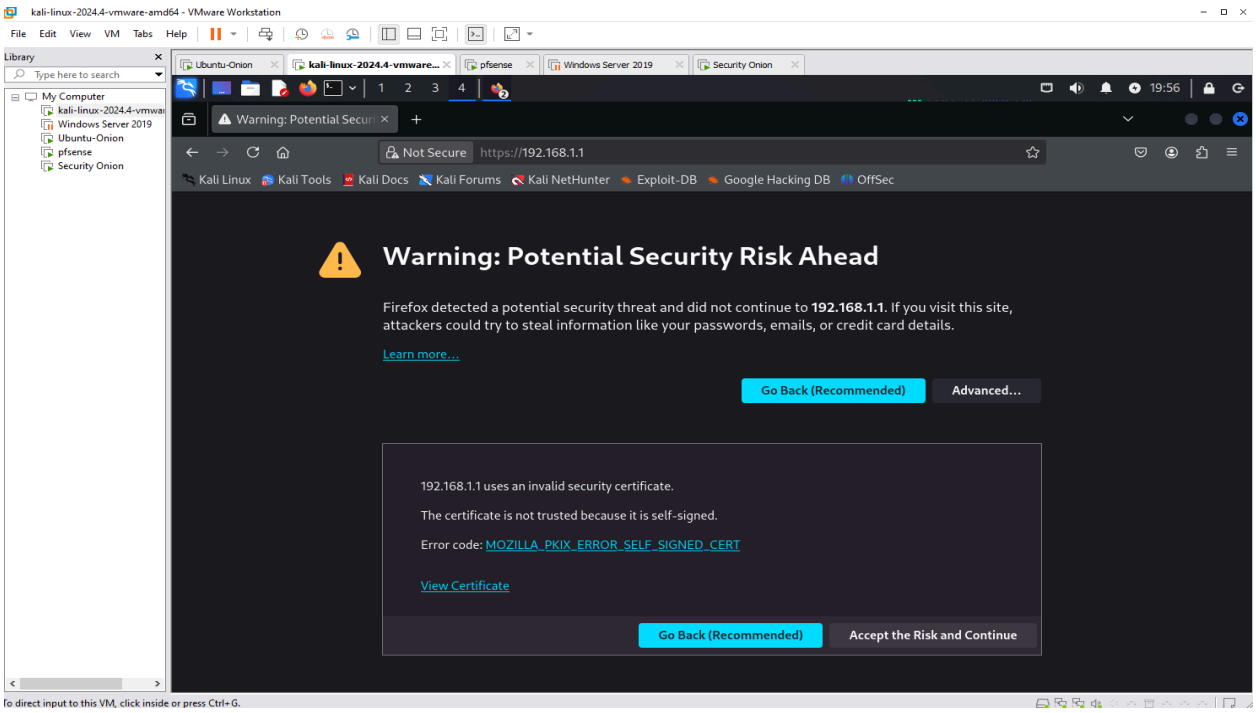
-Since a lab environment we will turn off the windows firewall



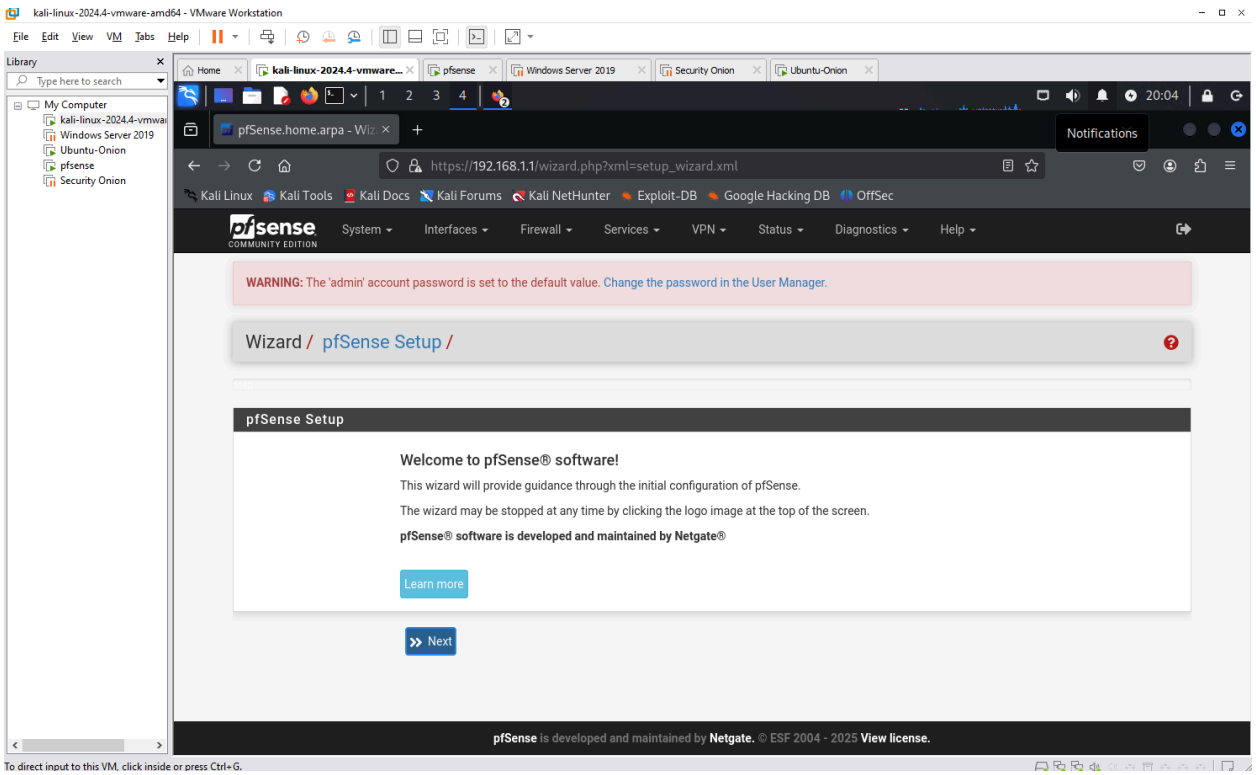
-Entering the control panel to create the TCP/IP properties



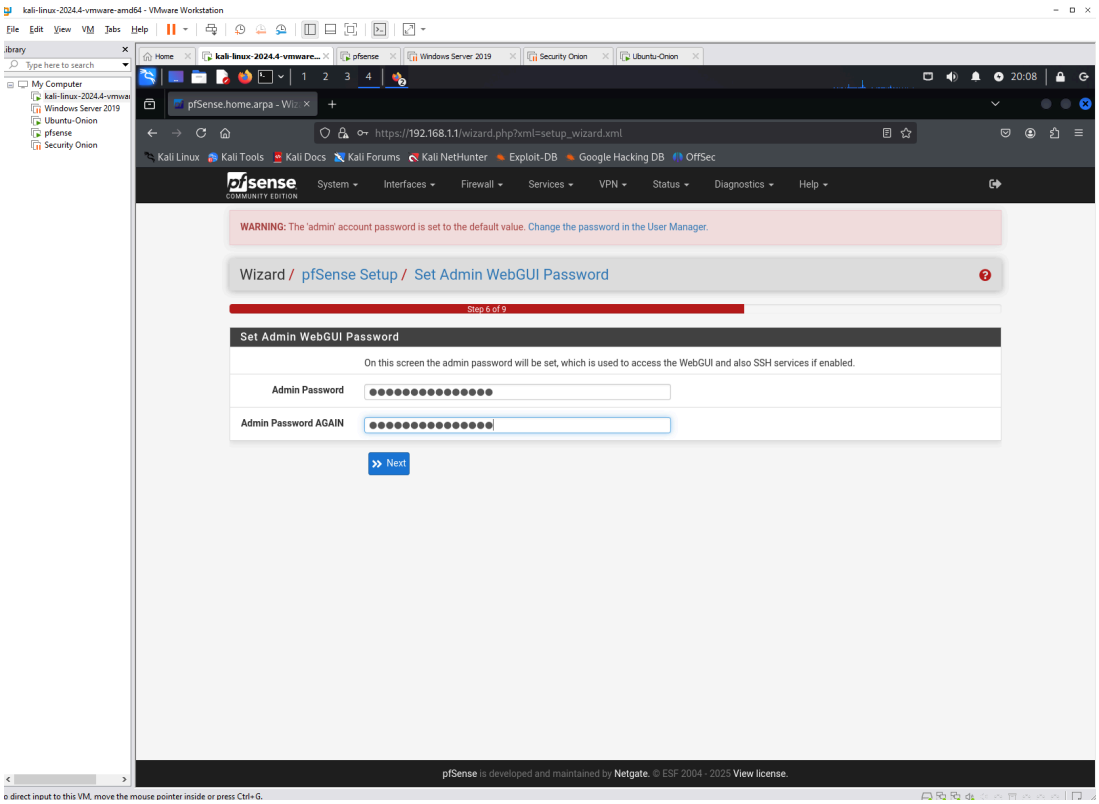
-Now we will move to pfsense settings with kali by logging in and opening firefox and entering the ip address: 192.168.1.1 that we configured on our pfsense and accepting the risk and continuing.



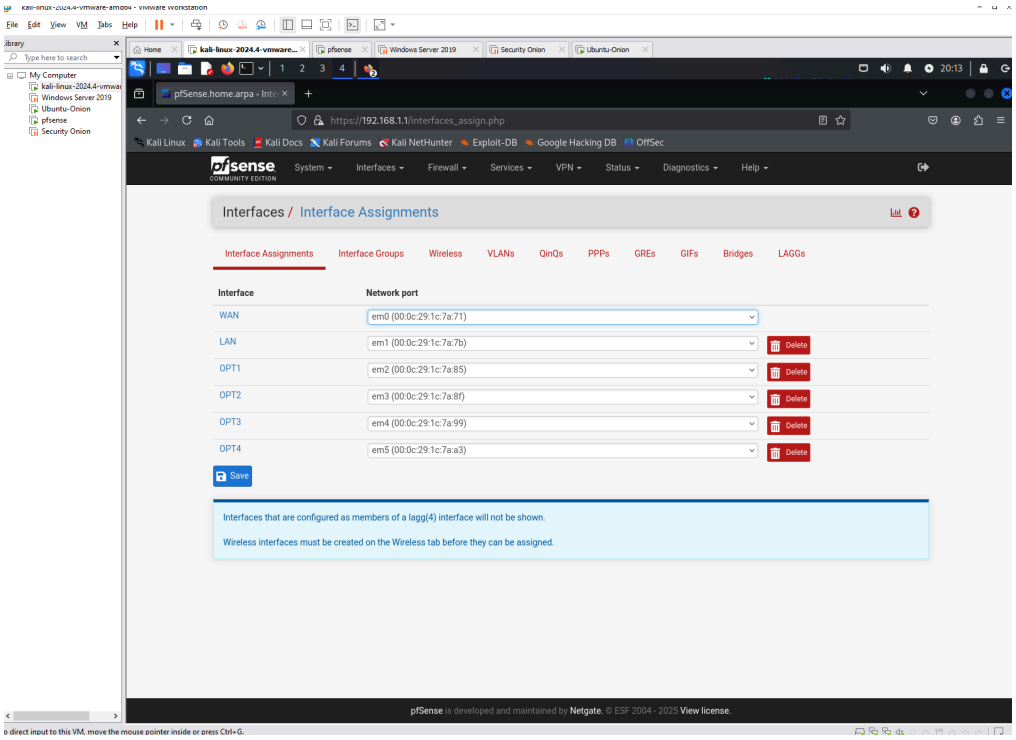
-Entering the username and password to access the setup



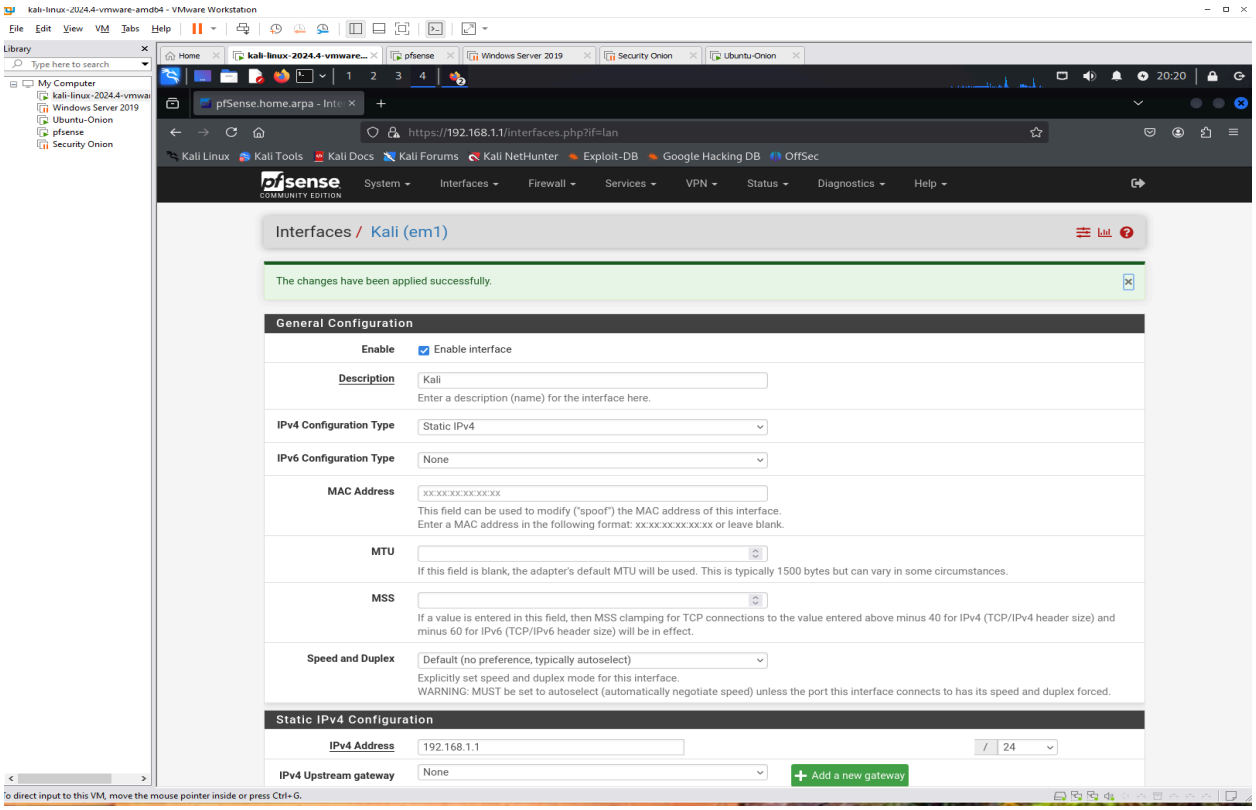
-Following the setup with accepting the defaults/only option on clicking next til entering new password and it will reload



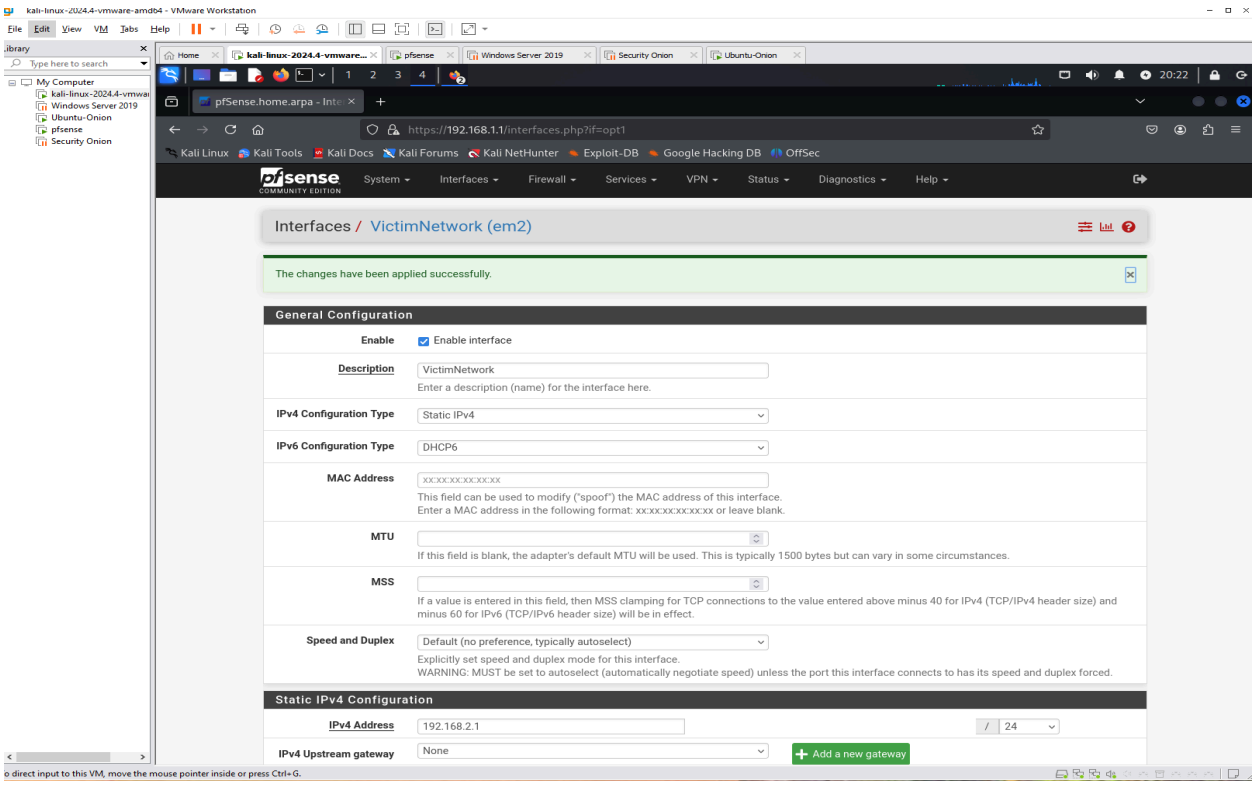
-Now we are going to configure the interfaces



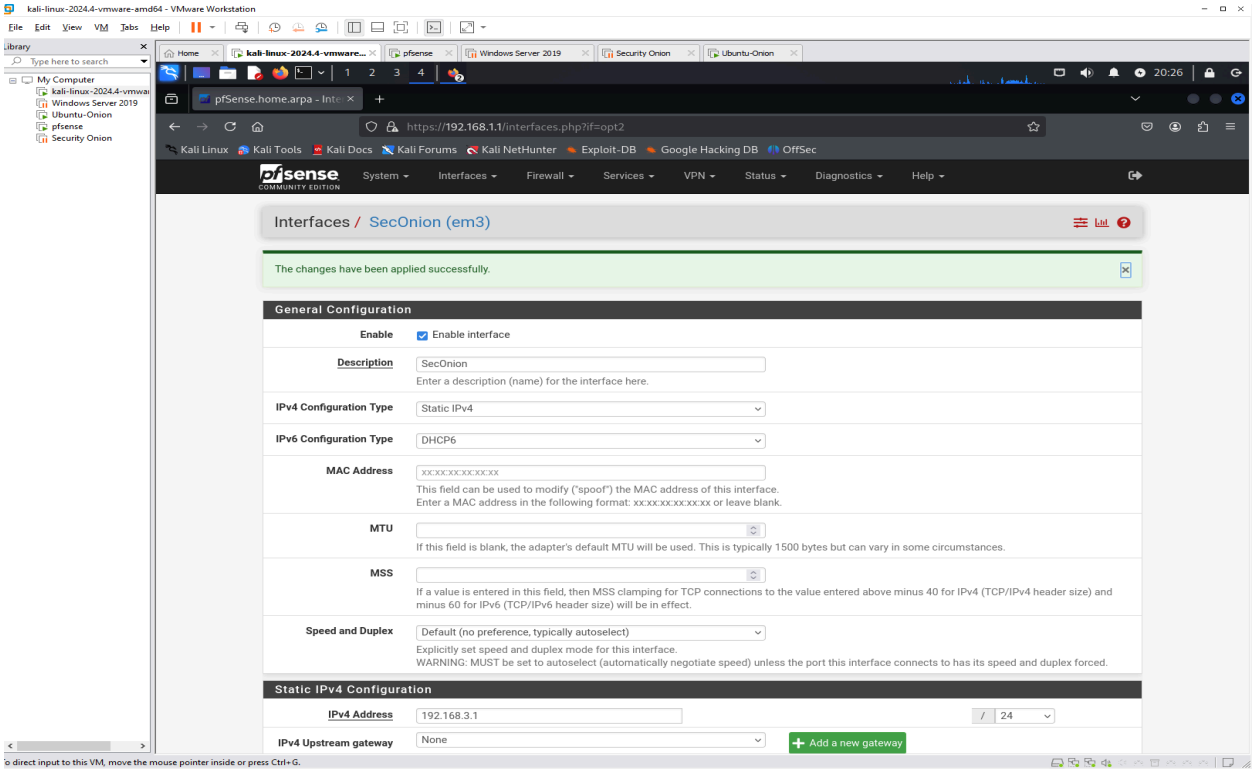
-First I changed the LAN to Kali and checked to make sure the ip address was corect



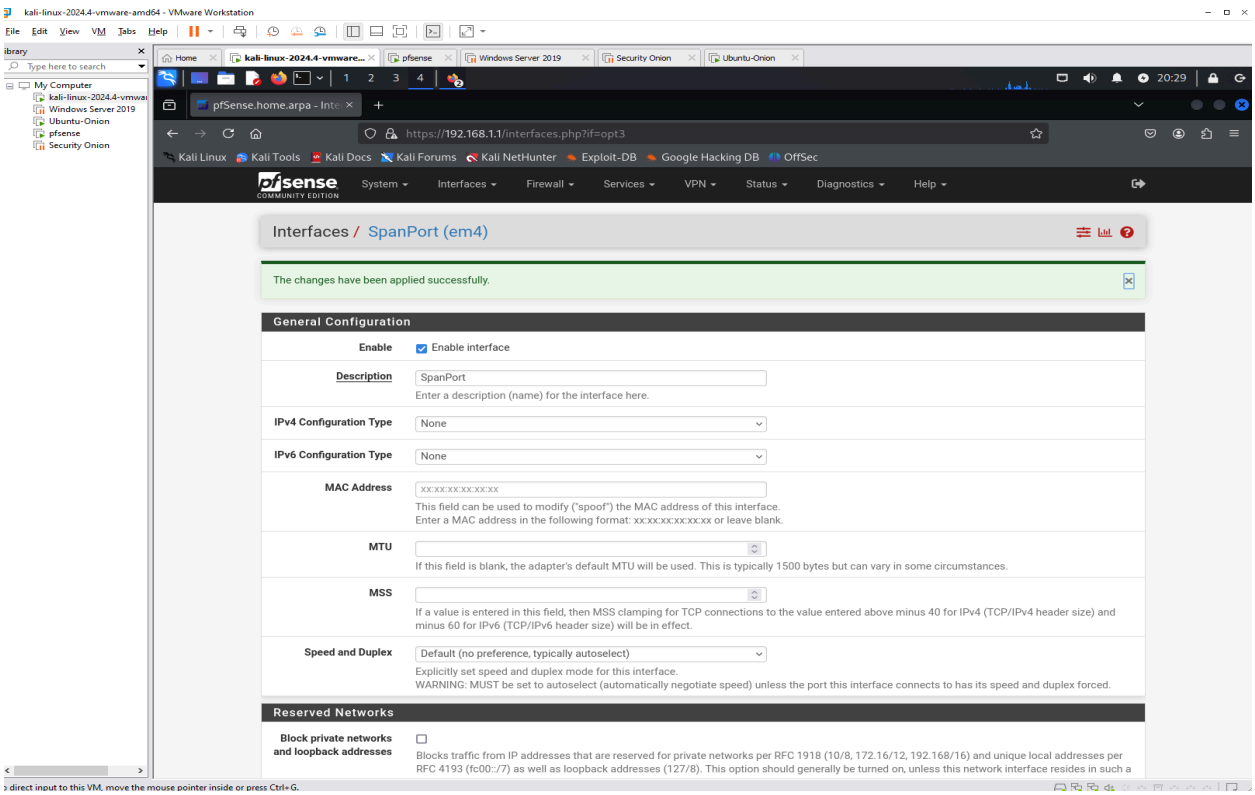
-Changed opt1 interface to Victim network again checking the ip was correct



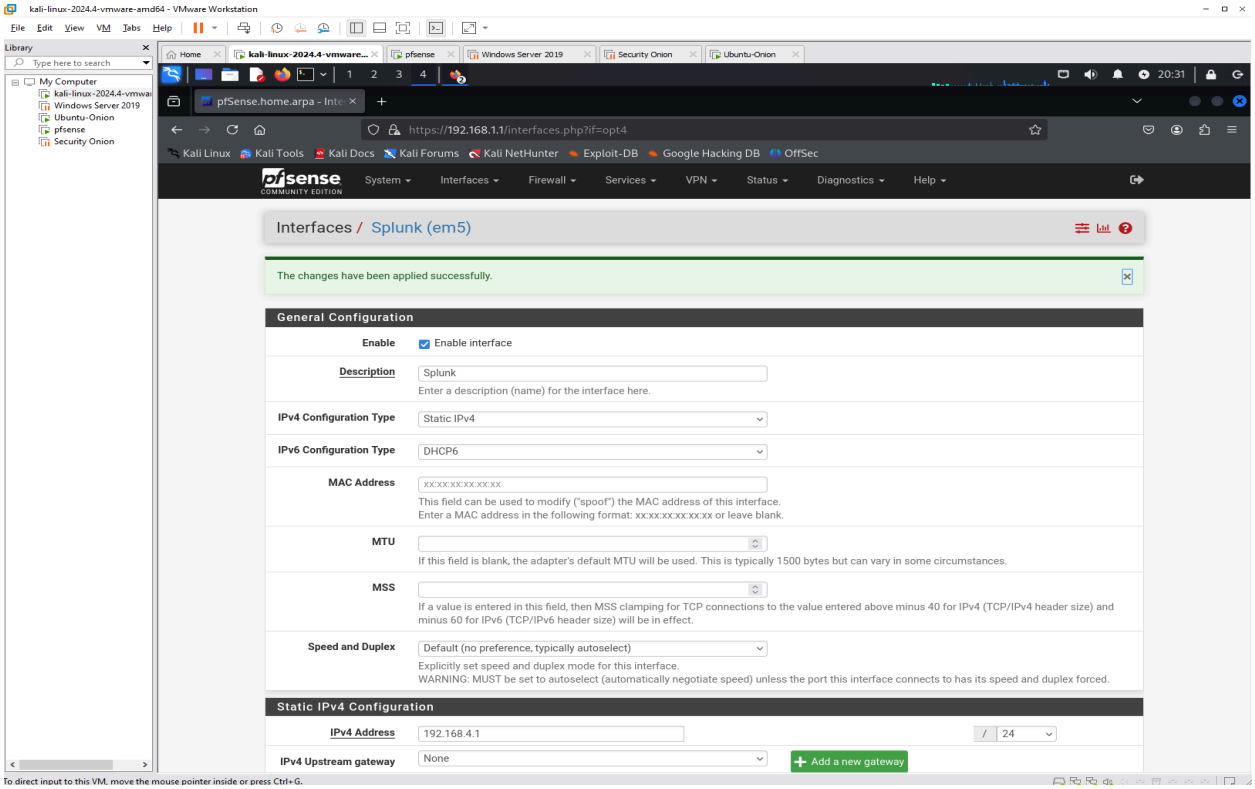
-Setting the opt2 interface to SecOnion again checking the ip was correct



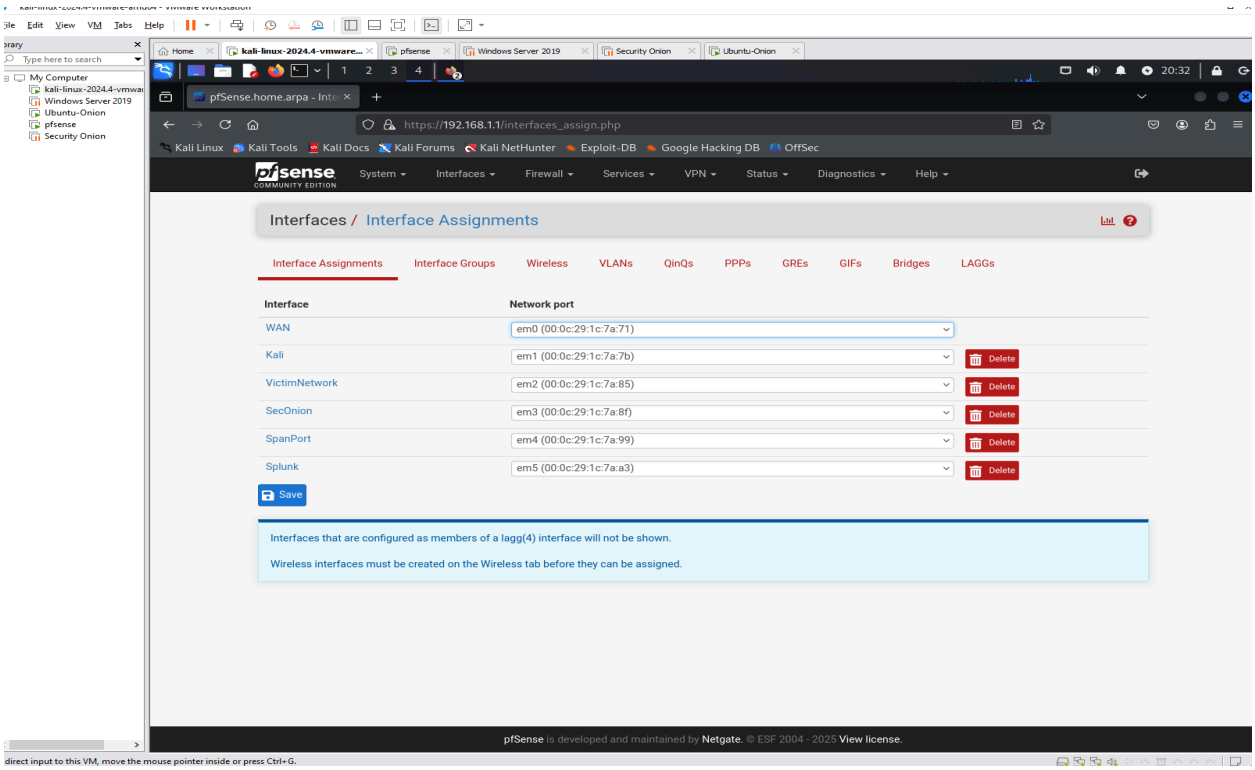
-Since we didn't set ip for opt3 we have to enable the interface after naming it SpanPort



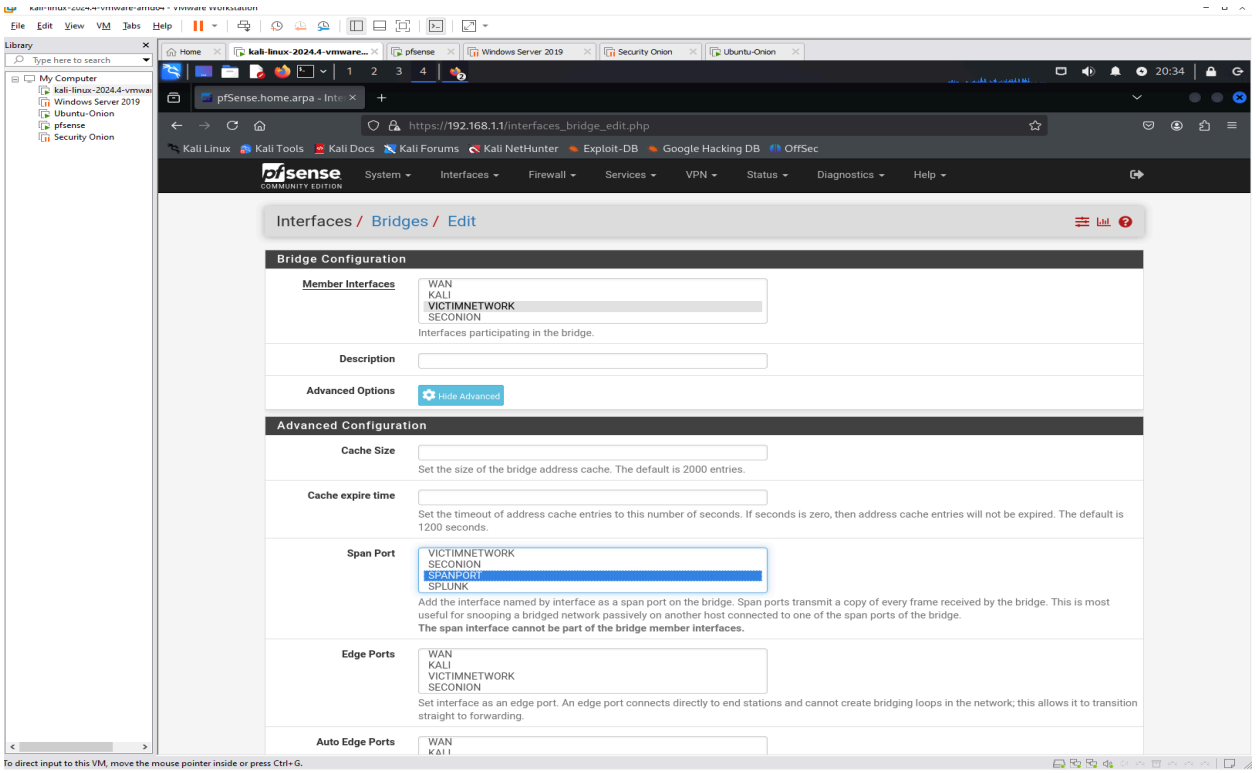
-Now opt4 will be named Splunk and checking the ip address



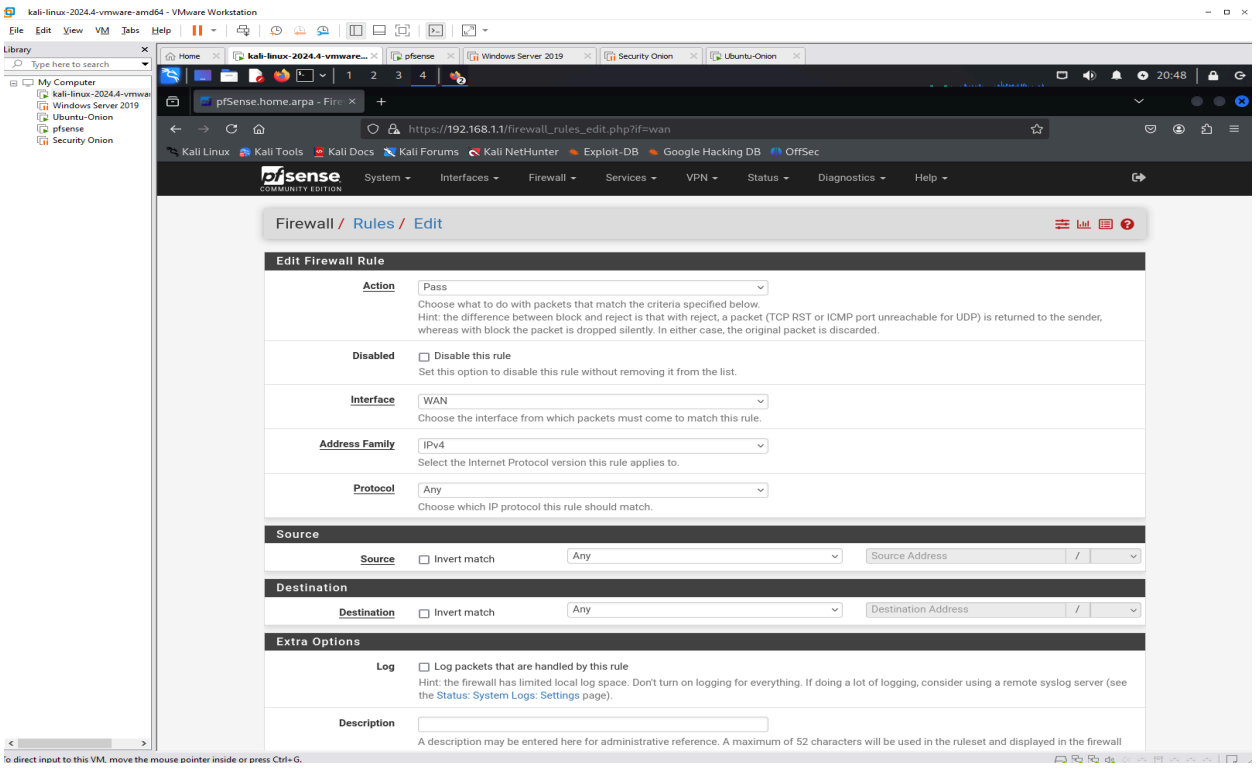
-Finalized assignments



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



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



Resources

Damon, Joseph. “Virtual Home Lab for Blue Team Security – Network Topology – Section 2.” *Joseph Damon* |, 28 Aug. 2023, josephmdamon.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/

O’Brien, Gerard. “Gerard O’Brien.” *YouTube*, YouTube, 15 Feb. 2023, www.youtube.com/@gerardobrien