DATA SPELUNKING

Project Report
CY 5-1

Date:

09/06/2022

Course title:

Computer Networks

Document Code	DS/PR-CN
Version	1.0
Date of version	09/06/2023
Approved by	Engr. M Ahmed Nawaz
Confidentiality level	Internal – Confidential

Document Change History

Date	Version	Edited By	Description of Change

Table of Contents

Data Spelunking using Splunk 4
- Scenario 4
- Lab Environment 4
- Download Links 4
- Proof of Concepts 5
  - Virtual Machine for PfSense 5
  - Kali and PfSense Configuration 10
  - SecOnion Configuration 16
  - SecOnion Management 22
  - Windows Server 2019 26
  - Windows 10 Virtual Machine 36
  - Virtual Machine for Splunk 40
  - Ubuntu Server Installation 41
  - Splunk Installation 44
  - Splunk Universal Forwarder 47
- Lab Analysis 50

Data Spelunking using Splunk

Scenario

The exponential growth in machine data over the last decade was primarily due to the growing number of machines and increased use of IoT devices. This machine data contains hidden insights crucial for optimizing businesses and reshaping current as well as future products. We can feed this data to Splunk, which in turn does the data processing for us. So, Splunk is basically a software platform that helps us search, analyze and visualize big data. Eventually, this leads to better decision making.

Lab Environment

To complete this lab we used:

- 3.8 GHz 8-Core Processor
- 32 GB (DDR4 Memory)
- 256GB M.2-2280 NVME SSD
- Windows 10/11

Download Links

VMware	https://www.vmware.com/products/workstation-pro.html
Pfsense	https://www.pfsense.org/download/
SecOnion	https://github.com/Security-Onion Solutions/securityonion/blob/master/VERIFY_ISO.md
Ubuntu Desktop	https://ubuntu.com/download/desktop
Ubuntu Server	https://ubuntu.com/download/server
Kali Linux	https://www.kali.org/get-kali/#kali-platforms
Windows Server	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
Windows Desktop	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
Splunk	https://www.splunk.com/en_us/download.html
Universal Forwarder	https://www.splunk.com/en_us/download/universal-forwarder.html

Virtual Machine for PfSense

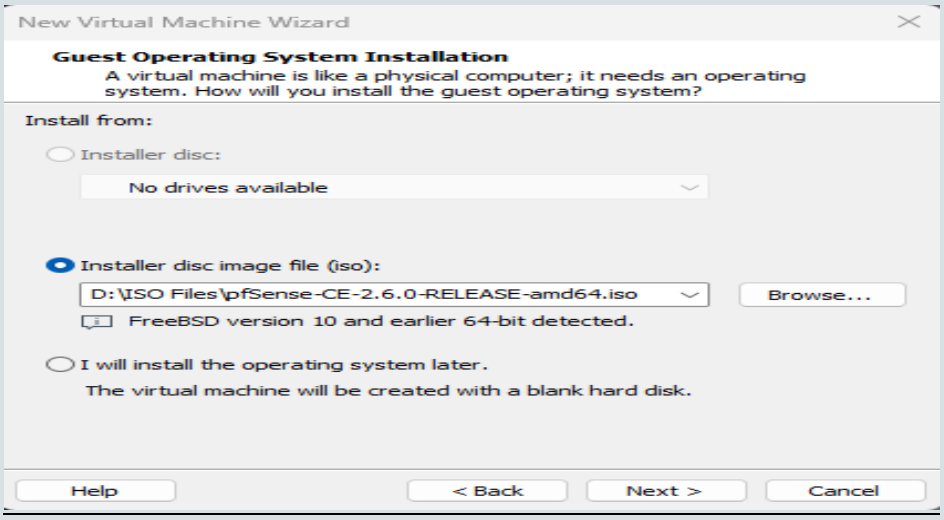

Figure 1

- Open VMware and select ‘create a new virtual machine’, select ‘typical configuration’ and click on ‘next’ and select the PF sense ISO image file click on ‘next’ to proceed.

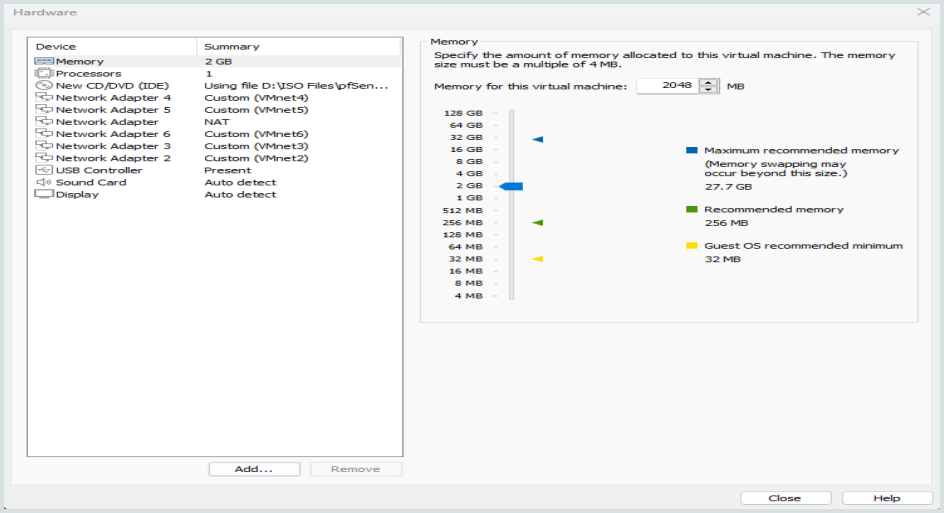

Figure 2

- Now configure the following below VM settings for configuring PF sense.

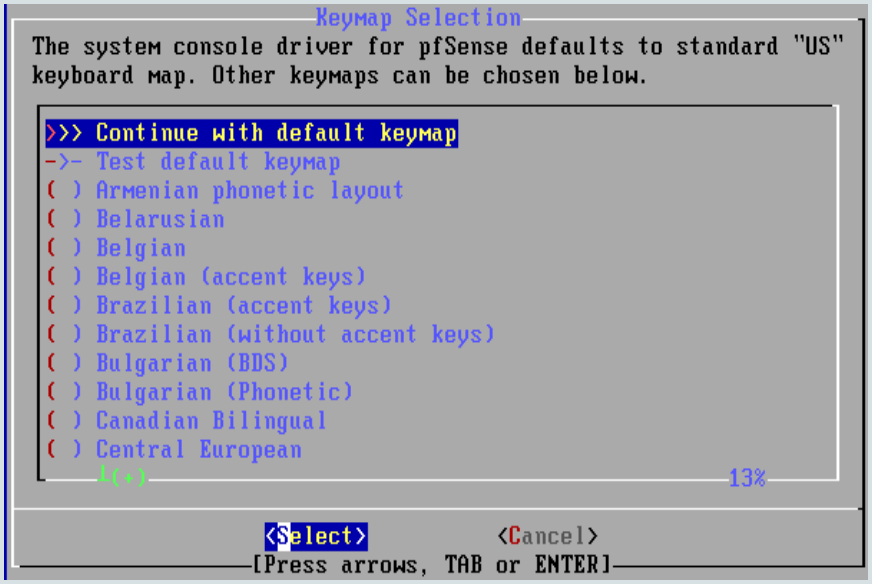

Figure 3

- 'Power on' the PF sense VM and 'accept' the terms, select 'install PF sense' option and click on 'OK'. After that select 'continue with default keymap'.

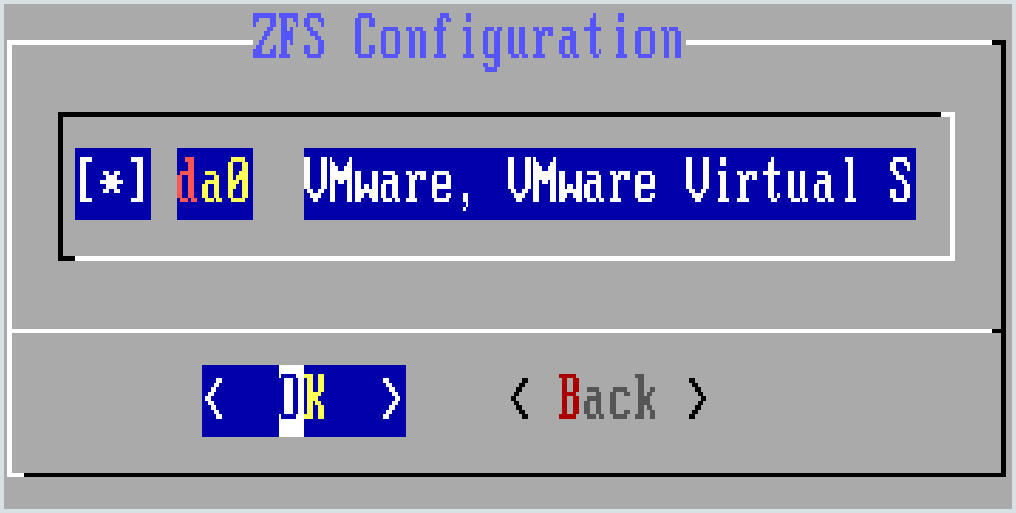

Figure 4

- After that, click on 'guided root disk partition' and click 'ok'. Then click on 'proceed with installation' and then select virtual disk type as 'strip no redundancy'. Select 'VMware Virtual option' and click 'OK'.

Figure 5

- After that click on '**Yes**' option to proceed further and then you can see the installation process is started, will take few seconds to complete.

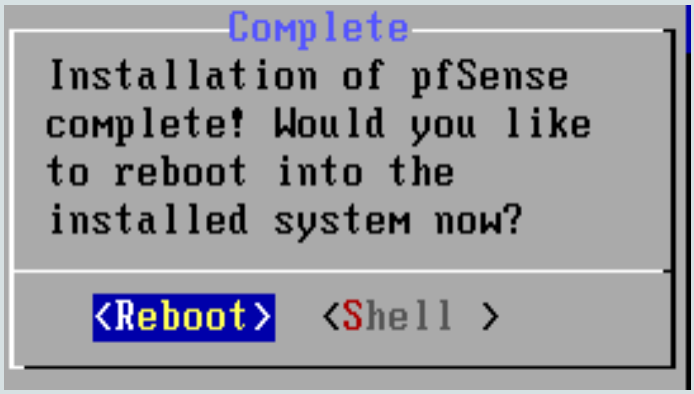

Figure 6

- After that a manual configuration dialog box appears, click on 'No' to proceed further and then click on reboot to restart the PF sense.

Figure 7

- At the next start-up we should be met with the screen below where we will 'press 1' to go to the interface mappings.

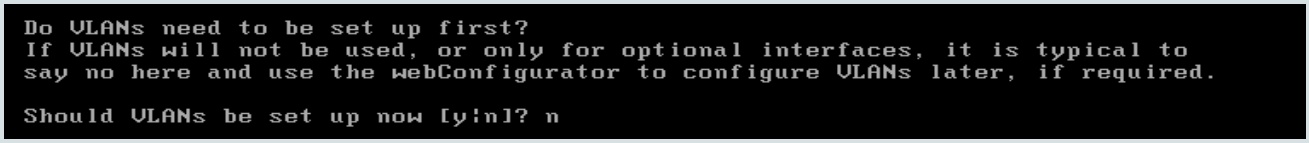

Figure 8

- It displays valid interfaces available and then ask the prompt below to which we will say 'no'.

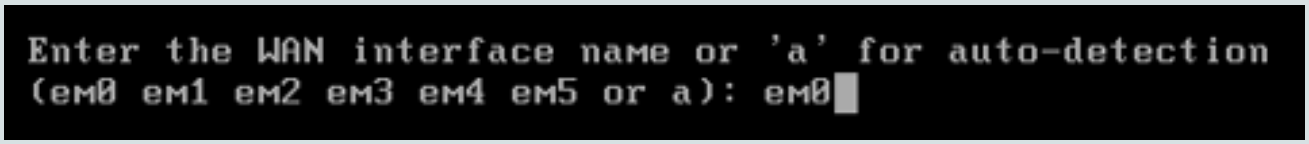

Figure 9

- In next prompt we will enter the interface names for the network adapters.

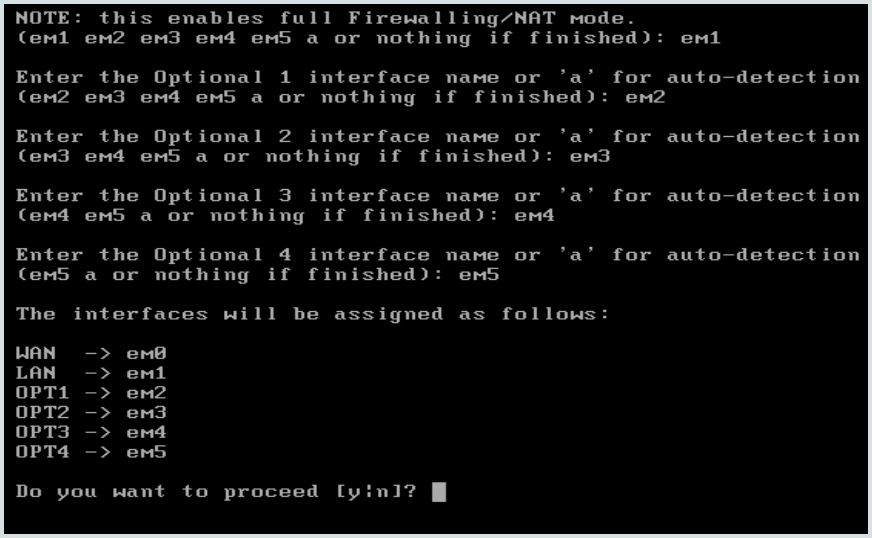

Figure 10

- Continue to respond to the prompts such that the interfaces will be assigned.

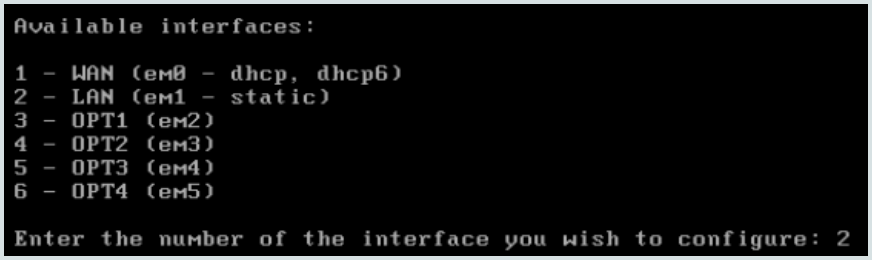

Figure 11

- Now, we are going to configure the interface IP addresses by entering '2' at the PF sense menu. It will ask us to enter the number of the interface that we wish to configure and we will begin with LAN (em1) by entering '2' on the list of available interfaces.

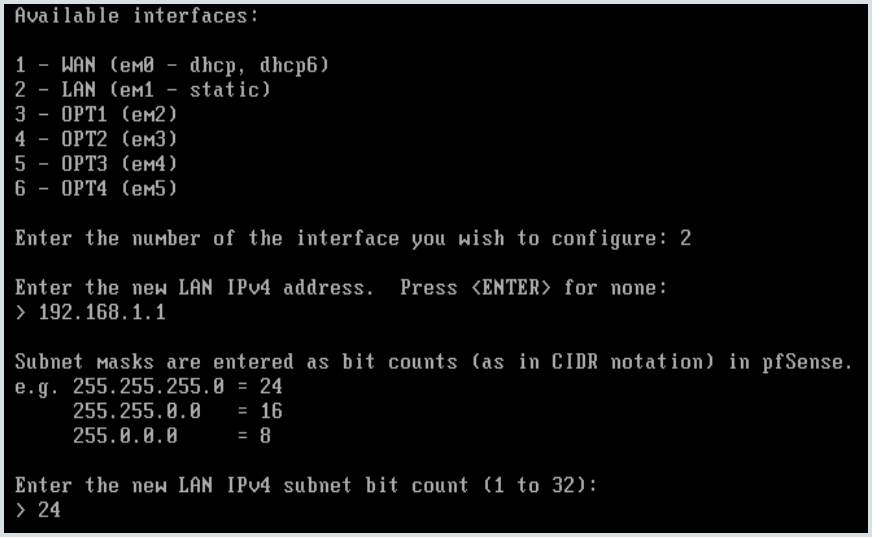

Figure 12

- Now we will assign 'IP address' to selected interface and also the subnet count according IP address class.

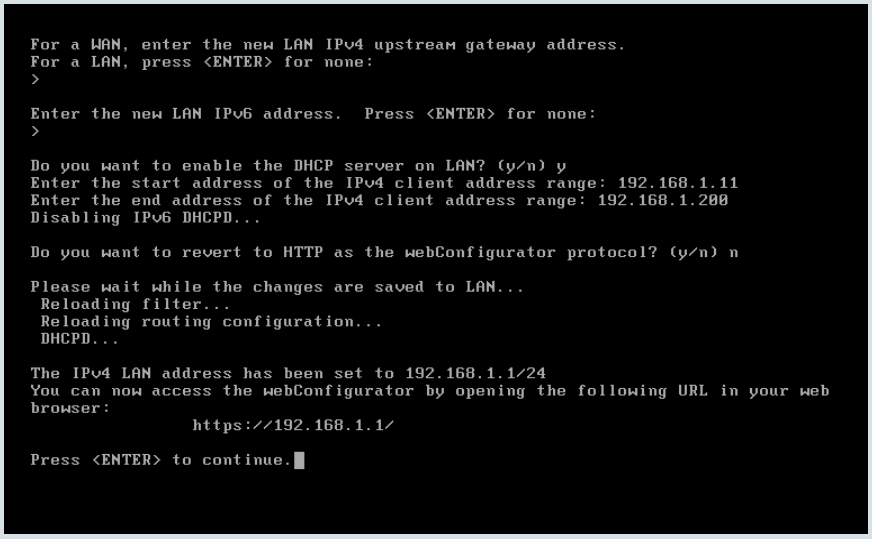

Figure 13

- After that we give the 'starting' and 'ending' IP address.

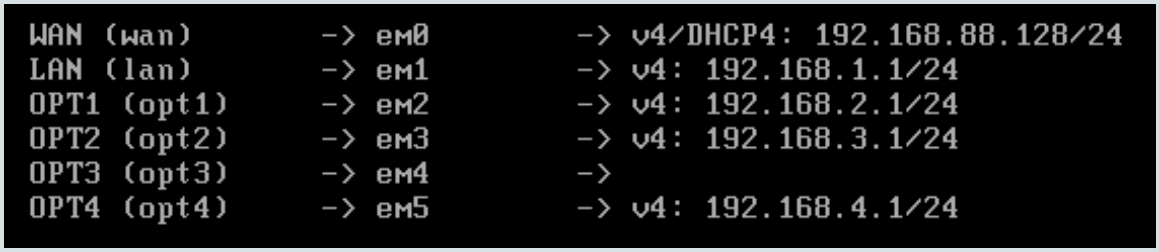

Figure 14

- After that, we will leave 'em4' which is on vmnet5 for now because it will be configured as a span port. Then will continue assigning in the same pattern of giving each adapter its own /24 subnet.

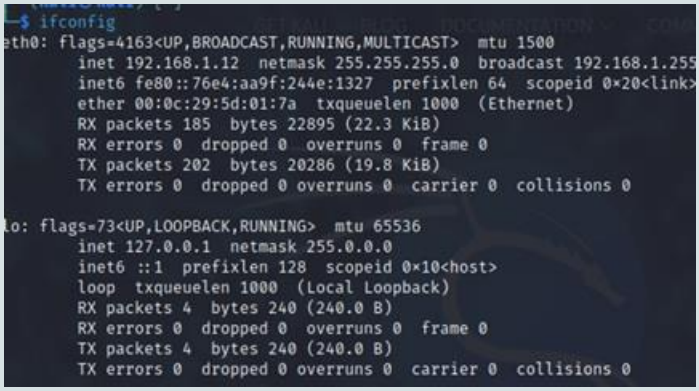

Figure 15

- Open VMware and select 'open a new virtual machine'. Change the network adapter from NAT to VMnet2. Then power on the VM and allow it to load. Open terminal, run ifconfig command and you should have received an IP from the pfSense.

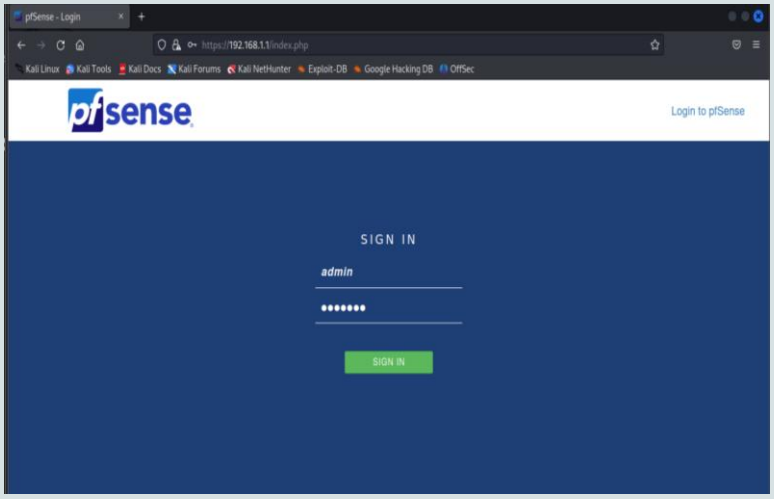

Figure 16

- Now remember that we want to use this machine to access pfSense web portal so open Firefox and type in the IP to access pFsense.

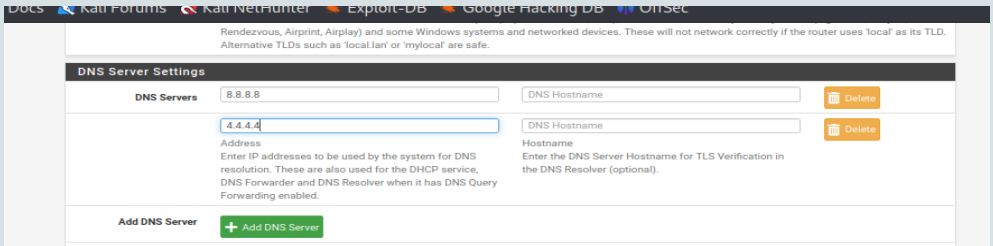

Figure 17

- We will now configure the rest of pfsense through the presented wizard. Add the primary and secondary DNS servers as 8.8.8.8 and 4.4.4.4 respectively. On the next page, choose your 'timezone'.

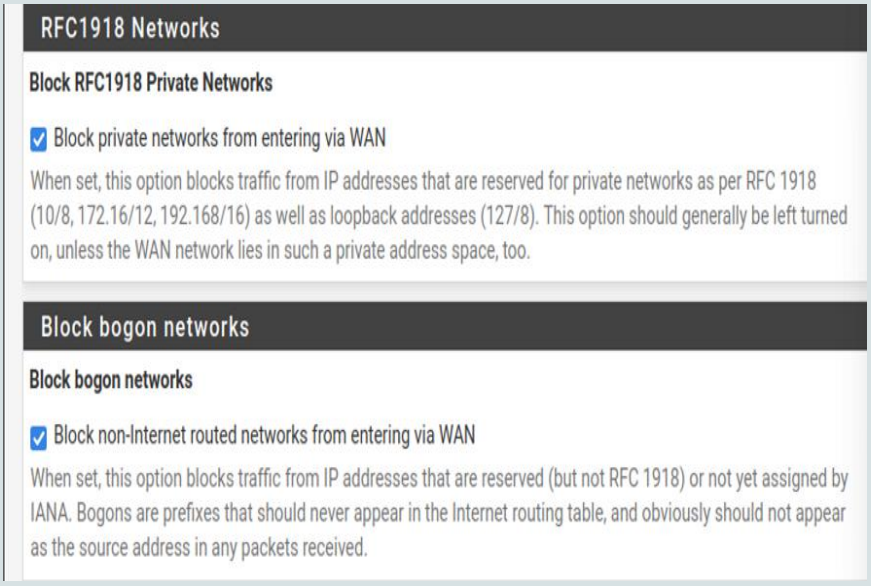

Figure 18

- Then we go to the next page, 'Configure you WAN Interface' and scroll down to the bottom. We can scroll down to the bottom and '**untick**' these options and click on 'save'.

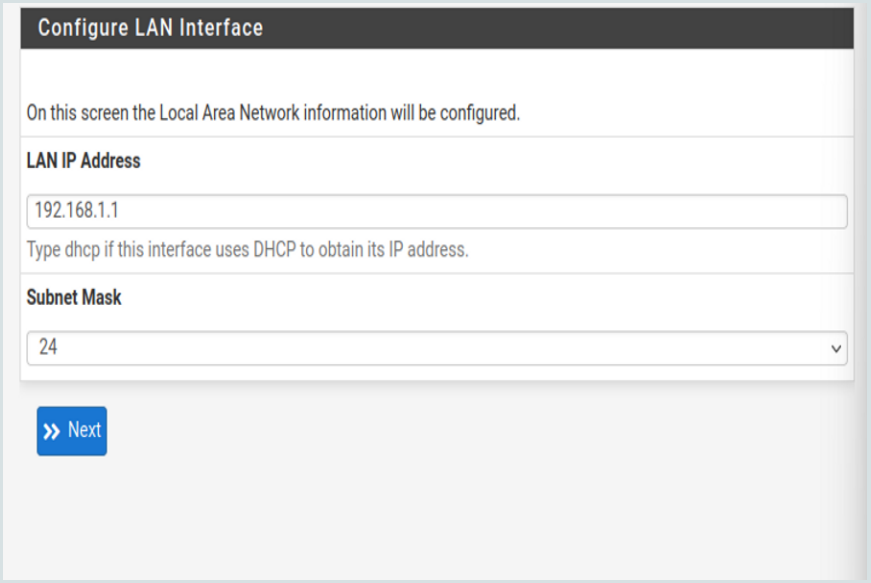

Figure 19

- We leave the default on the 'Configure LAN interface' page and click on 'next'.

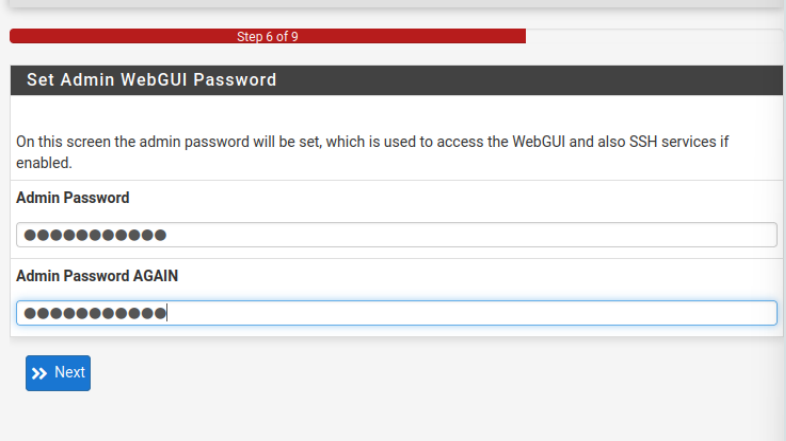

Figure 20

- On the next page we want to set a new password and then click on ‘next’. Then click ‘reload’, to reload pfSense with new changes.

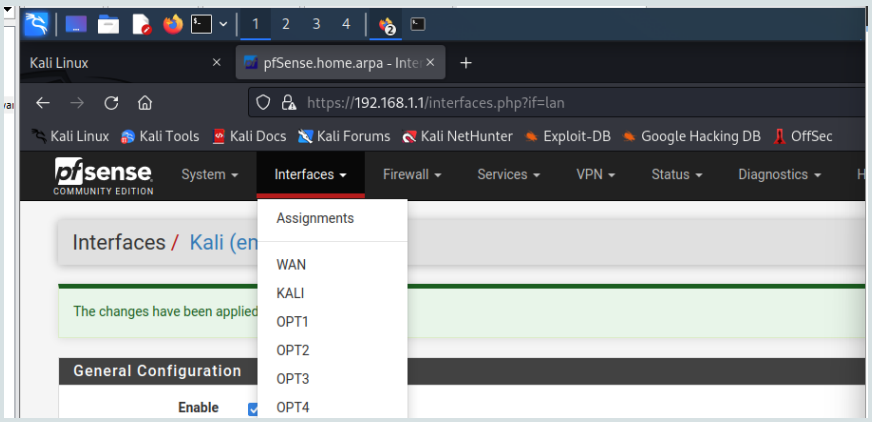

Figure 21

- We will now begin further configuring the interfaces in the web configurator. To do this we will navigate to Interfaces in the top menu and we will start with LAN which would be KALI. We will change the interface name from ‘LAN’ to ‘KALI’, since it is for the kali machine. ‘Save and apply configuration changes’.

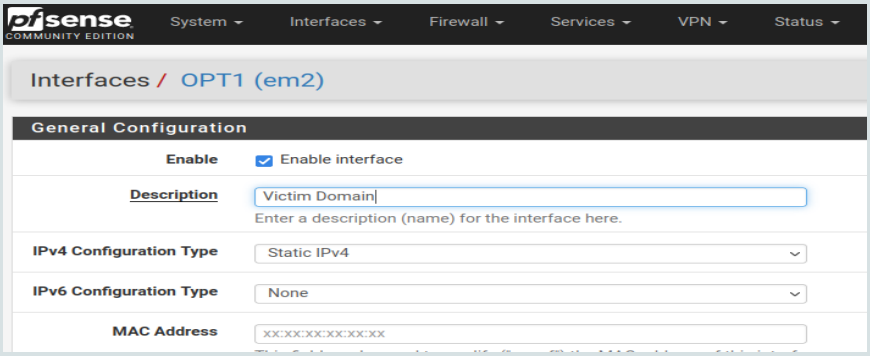

Figure 22

- We will then configure OPT1 which is interface 2 (em2) by naming it Victim Domain.

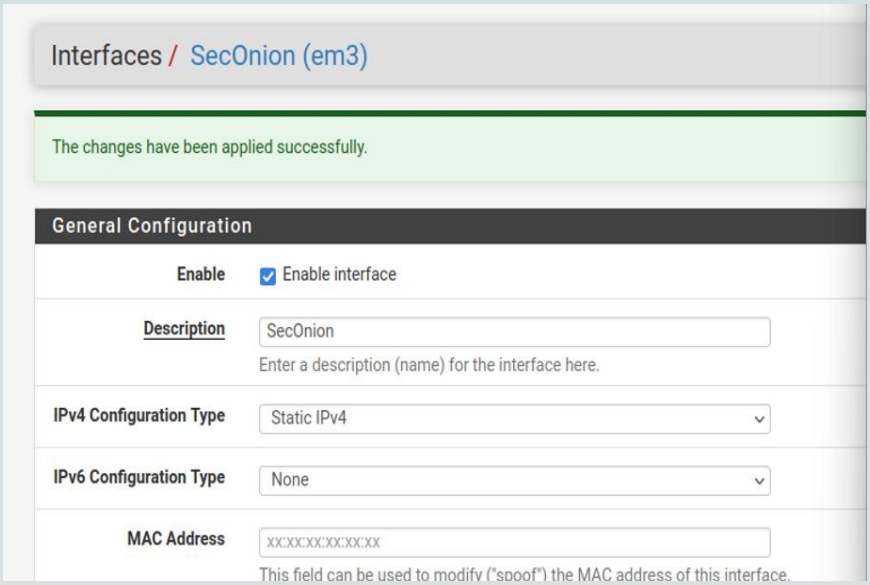

Figure 23

- In accord with the network topology, interface 3 (em3) is on vmnet4 which connects to security onion. Therefore we name it that.

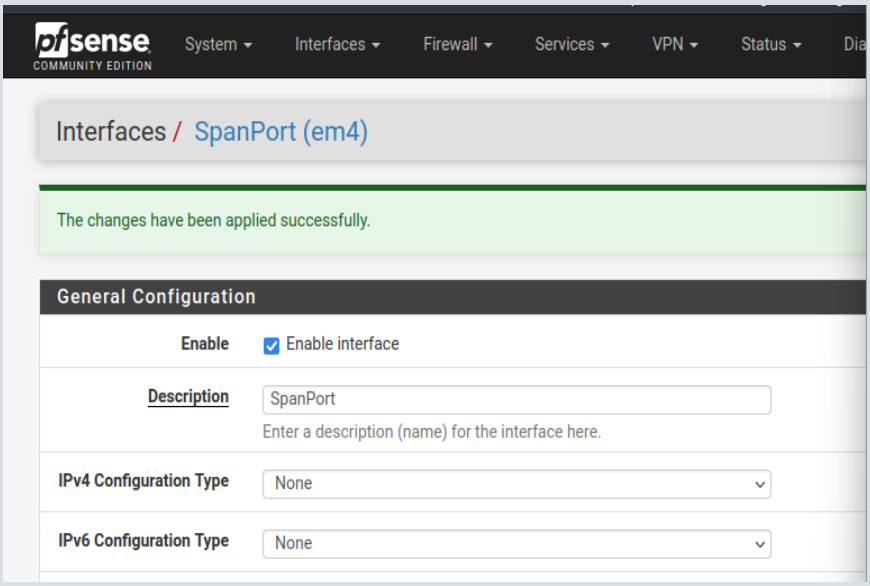

Figure 24

- As we go over to 'opt3' you would realize we do not have an IP address. This is because we did not set interface IP address for it like we did with the others. Therefore, we will have to 'enable it' and 'name it'. This will be our 'span port' on vmnet 5.

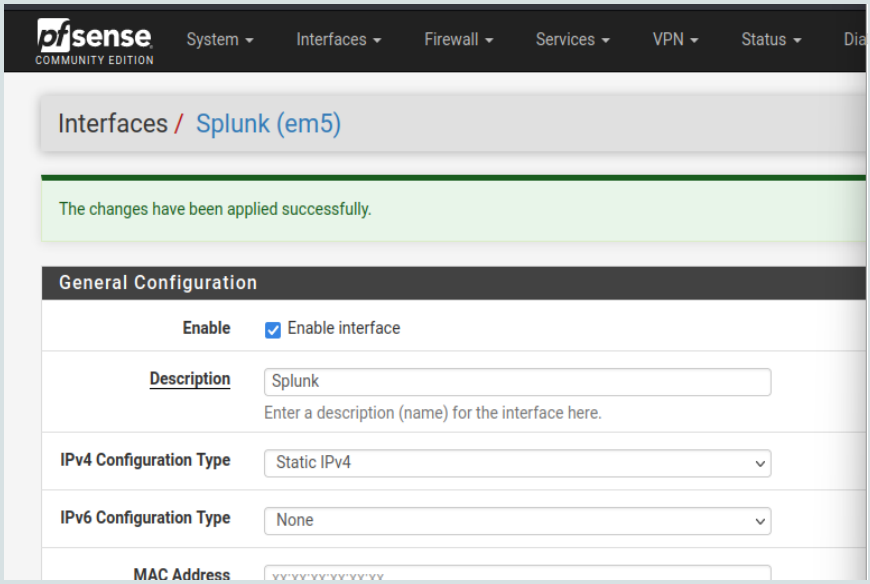

Figure 25

- The last one we will configure will be splunk. Which is our vmnet on interface 5 (em5). As the name suggests we will be connecting our splunk instance to our network from this interface.

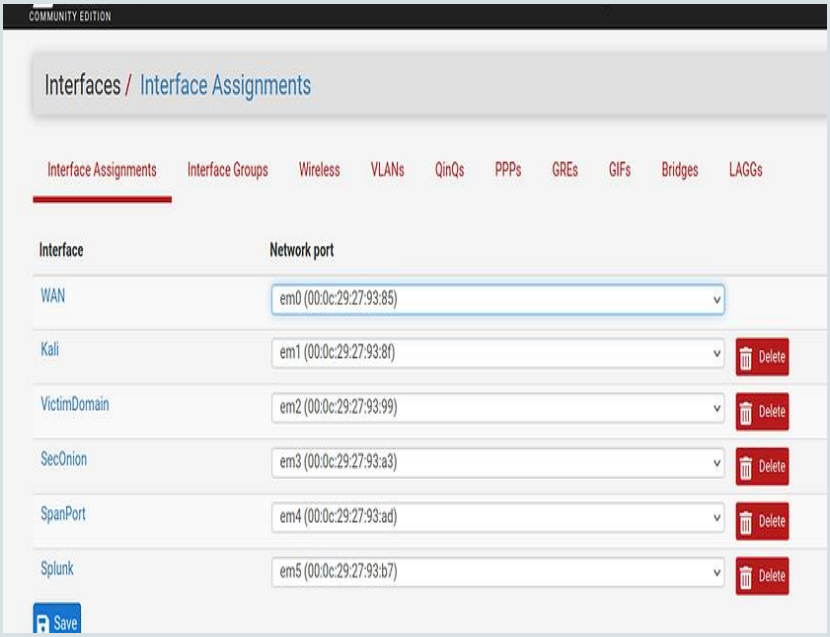

Figure 26

- You can verify the assignment by clicking on interfaces then navigating to interface assignments. It should look like this below

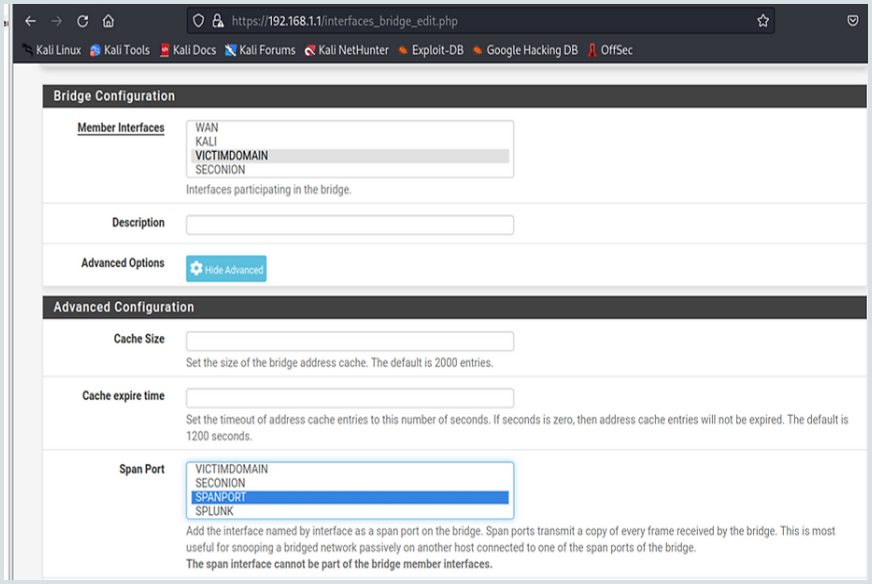

Figure 27

- Next, we want to add a 'bridge' by clicking bridges option in 'interfaces'. Click ADD. We will now select the victim domain as our member interface for the bridge and the click display advanced go to span port and select SPANPORT as the span port.

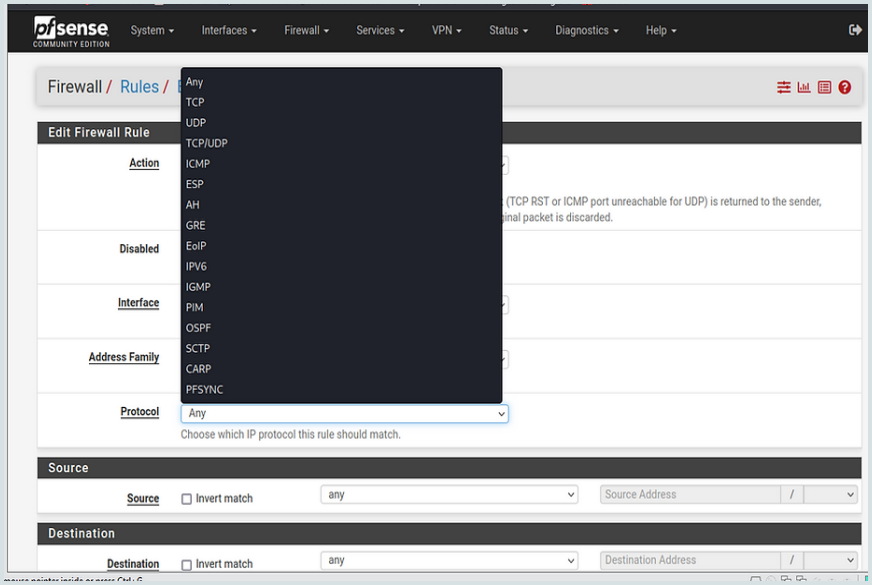

Figure 28

- Next we will go to firewall > rules > Under WAN select > add(top of the list) > then edit the protocol to allow any. Make sure the action is set to Pass > Apply changes. The reason why we are opening up the firewall is to make It more vulnerable so that we can see some alerts in action.

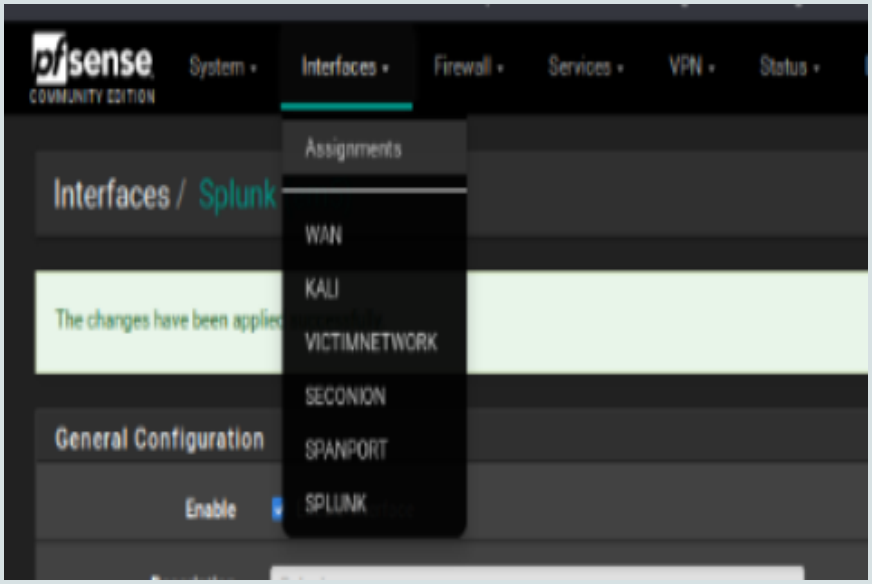

Figure 29

- Do the previous rule we add for all interfaces you see above you are trying to establish connections for now.

SecOnion Configuration

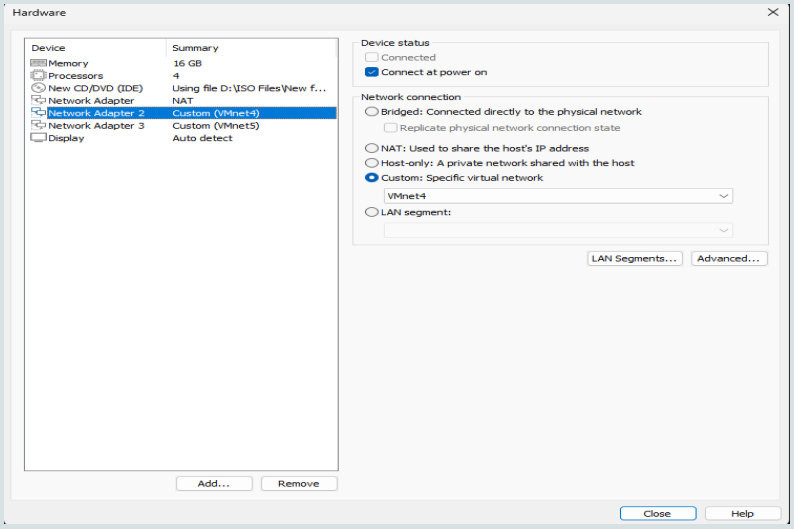

Figure 30

- In the wizard we click customize hardware and set memory to the minimum, set the processor cores to 4 and add 2 additional network adapters and connect them to vmnet 4 and 5, respectively. We ended up provisioning more RAM carrying it up to 16GB of RAM.

Figure 31

- 'Power on' the machine and install security onion with basic graphic interface.

Figure 32

- Type yes when you see this screen.

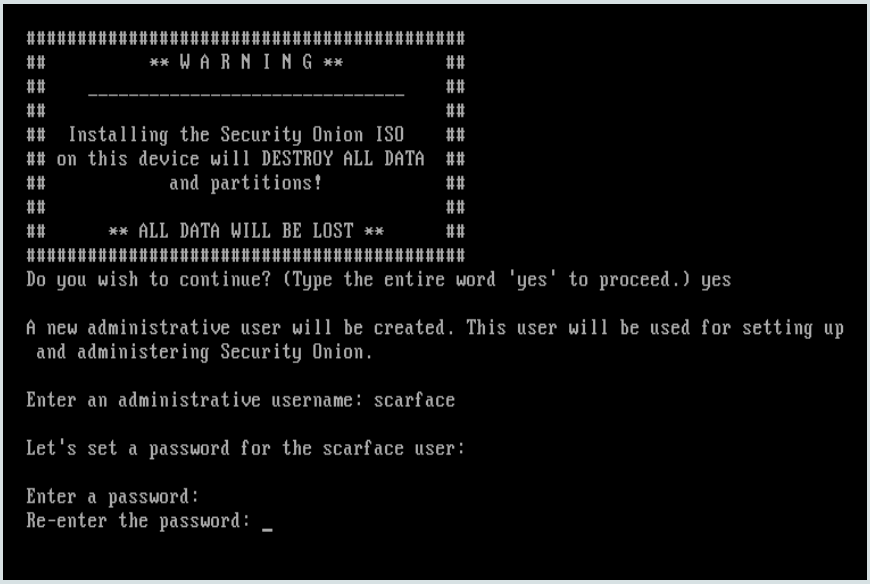

Figure 33

- Type yes when you see this screen. Follow the other prompts and enter username and password. It will reboot when finished.

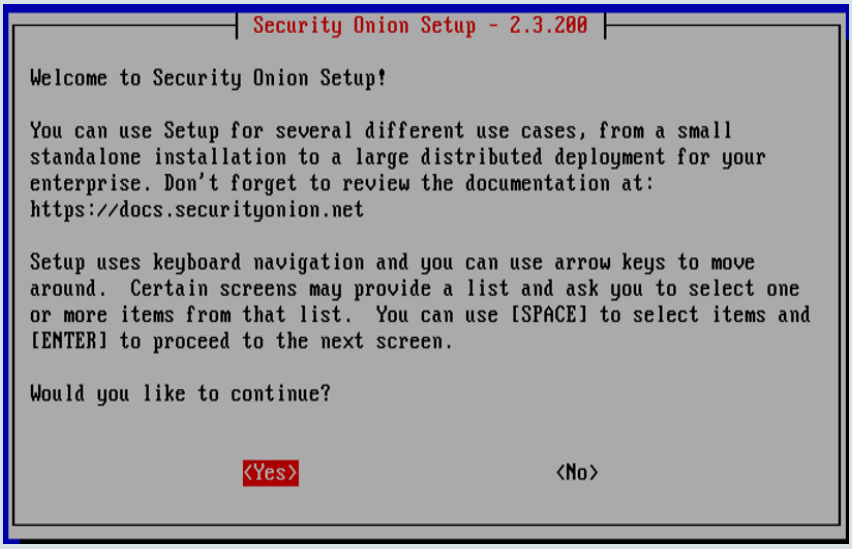

Figure 34

- Click Yes > Install > Select Eval version > Agree for the Elastic License > Give it a non-default hostname > Give it a description > Then we will be using the second Interface (ens33) as a management interface so we click space bar to select it.

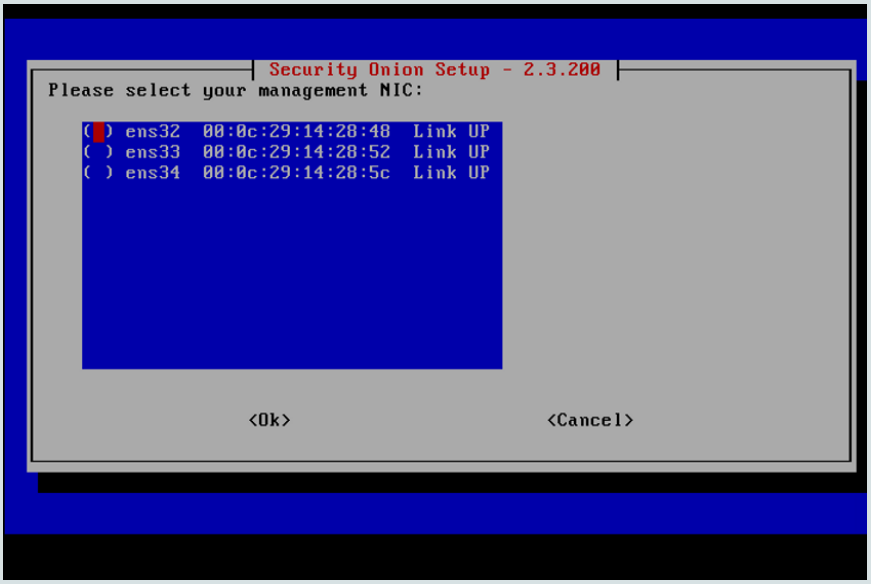

Figure 35

- Choose to use ens33 as the management interface for Security Onion.

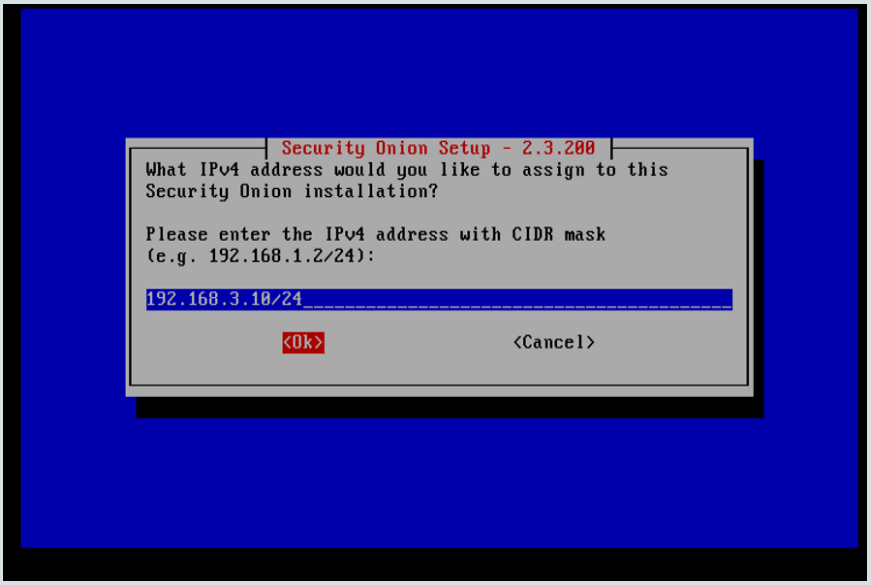

Figure 36

- Configured ens33 with a static IP address of 192.168.3.10. This approach avoids problems with changing the web access URL when the IP address lease expires.

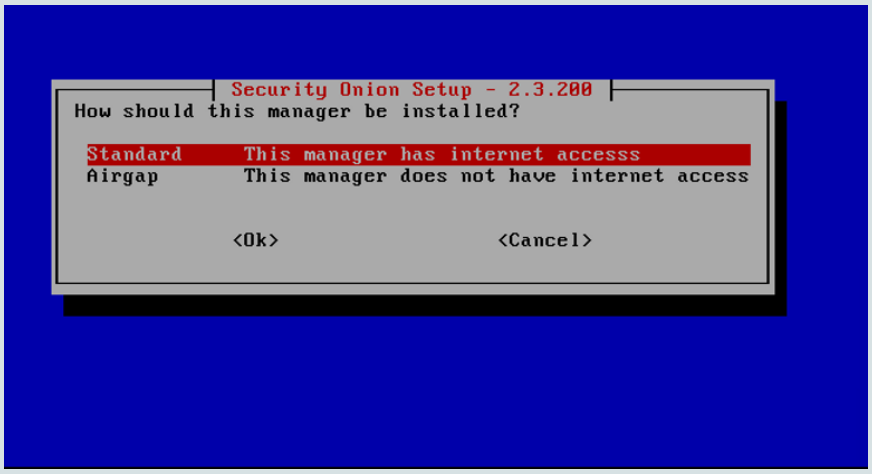

Figure 37

- For gateway enter the IP address for the interface at the firewall connection. Which in this case would be 192.168.3.1. For search domain enter the domain name of your victim network. Next we select ‘Standard’

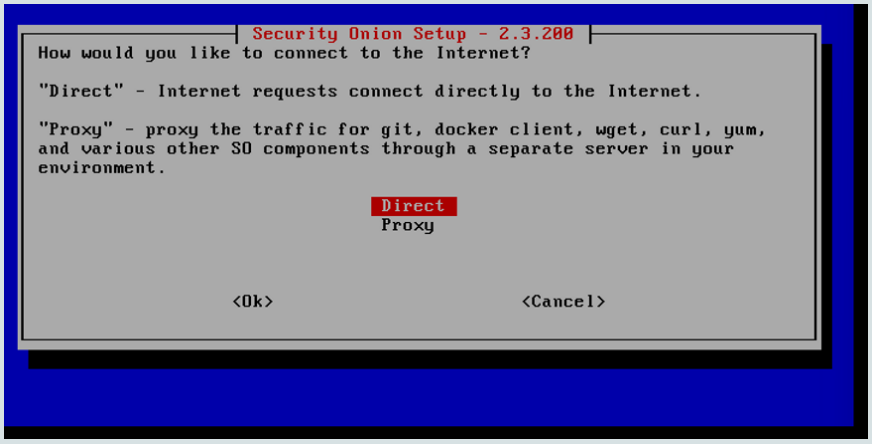

Figure 38

- We select ‘direct’ connectivity to the internet.

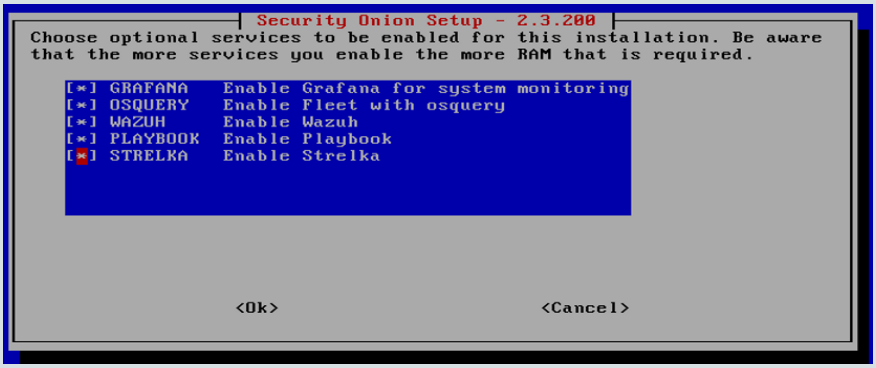

Figure 39

- We will next setup the monitoring interface which will be ens 34 on vmnet5. The next page we canleave as default since it already contains all the private IP’s. On the page After that in above screenshot if there is something you won't be using we can unselect it. However, we leave everything selected.

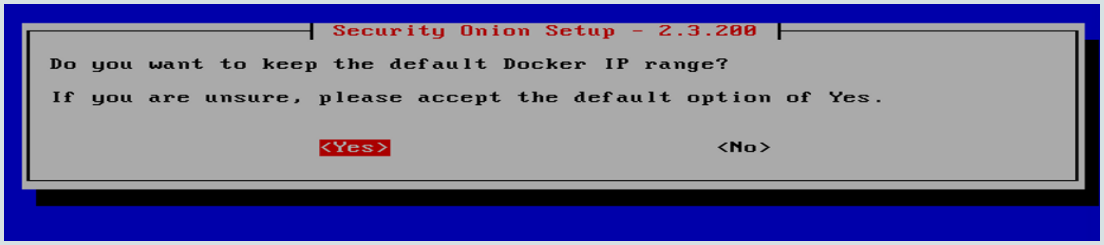

Figure 40

- We also want to keep the default Docker IP range, so we click on 'yes' and proceed further.

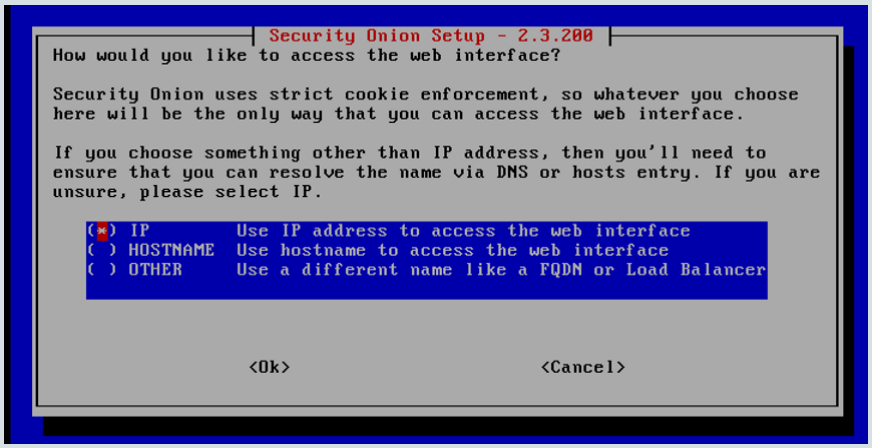

Figure 41

- The next slide prompts us to create an email address to access the web interface. It does not have to be legitimate. Just ensure you do not forget it. The page after that then asks us how we would like to access the web UI. You can leave this as 'IP'.

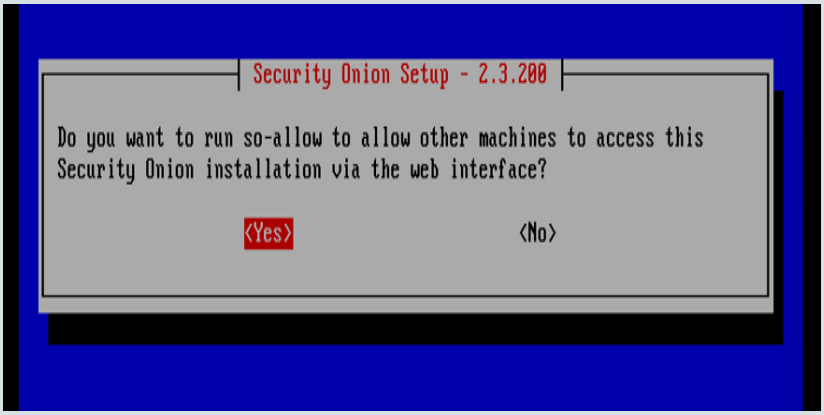

Figure 42

- On the next page we will be asked to allow NTP service ensure to select 'Yes' and then leave the default on the following page. We will next be prompted with the follow but we don't want to run 'so-allow' right now because we need to do something else before running it so-allow.

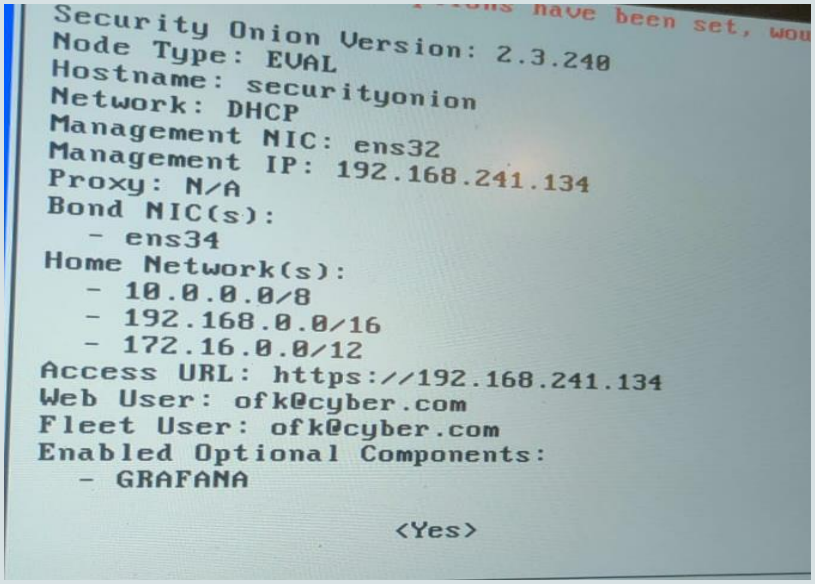

Figure 43

- On the summary page, take note of the access url. This is what you will enter to access Security Onion through the web interface.

SecOnion Management

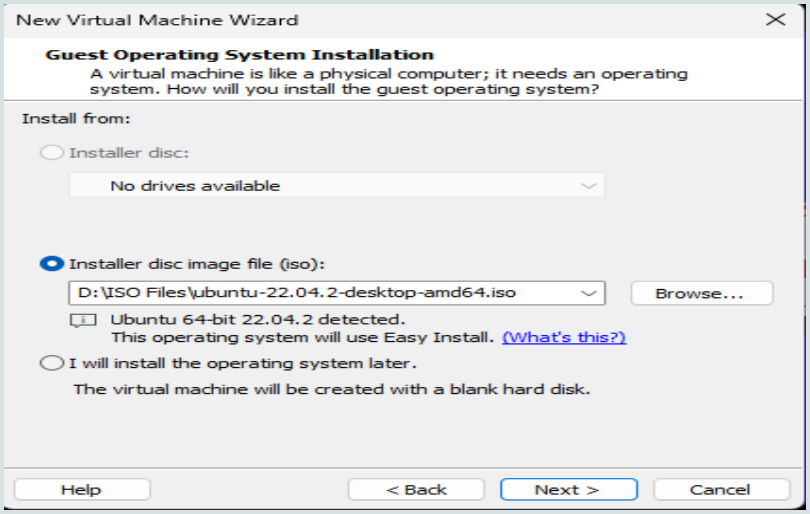

Figure 44

- Click on File and click New Virtual Machine. Select ‘typical configuration’ and click on ‘next’ and select the Ubuntu desktop ISO image file click on ‘next’ to proceed.

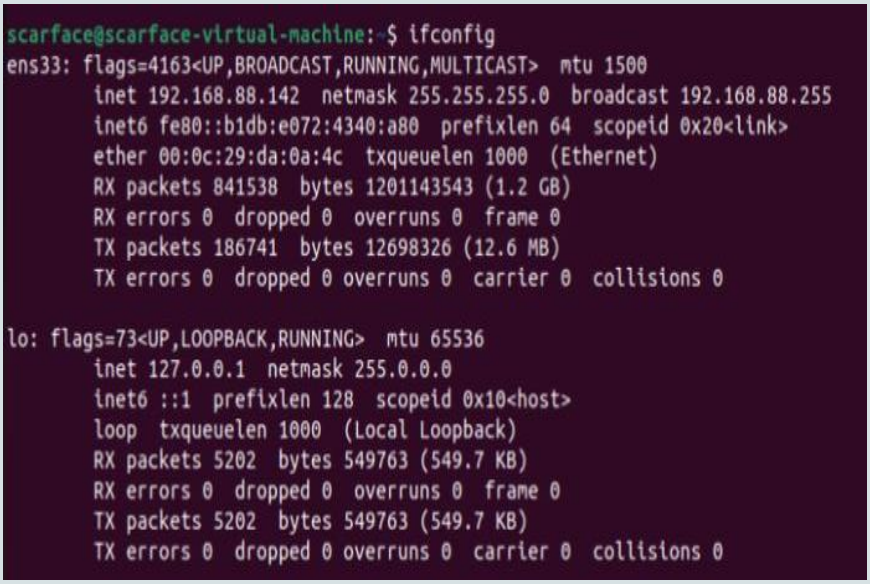

Figure 45

- After this installation, run the ifconfig command on the Ubuntu machine and take note of its IP Address.

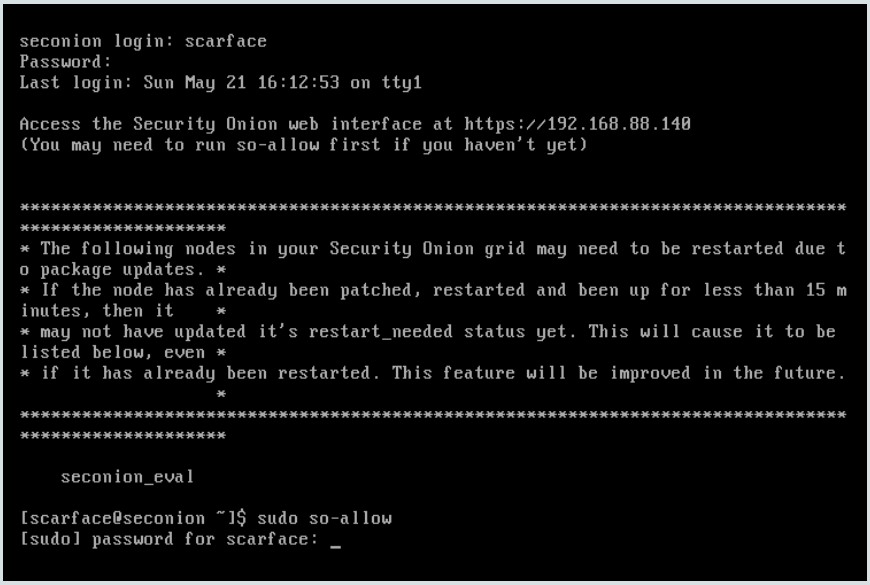

Figure 46

- Now, head back to your Security Onion instance and run the following command 'sudo so-allow' and then enter your password to proceed.

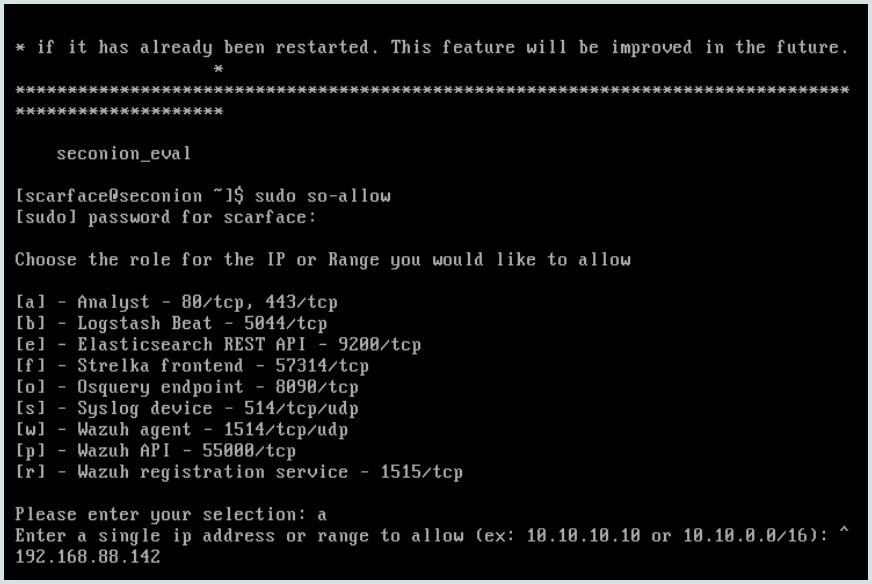

Figure 47

- Now, head back to your Security Onion instance and run the following command 'sudo so-allow' and then enter your password to proceed. After that type in the IP Address from the Ubuntu Desktop.

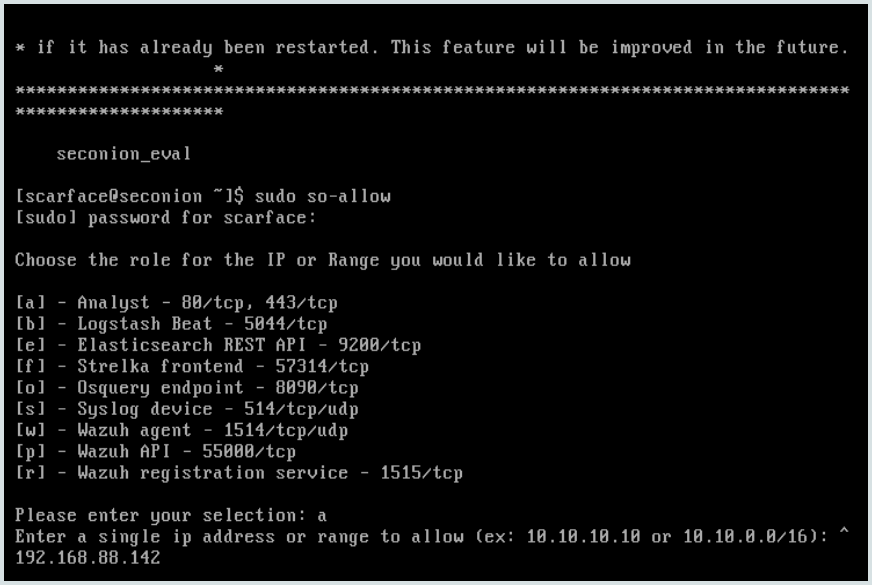

Figure 48

- Head back to your Security Onion instance and run the following command 'sudo so-allow' and then enter your password to proceed. Then type in the IP Address from the Ubuntu Desktop. It will allow you to have web access from your Ubuntu Desktop

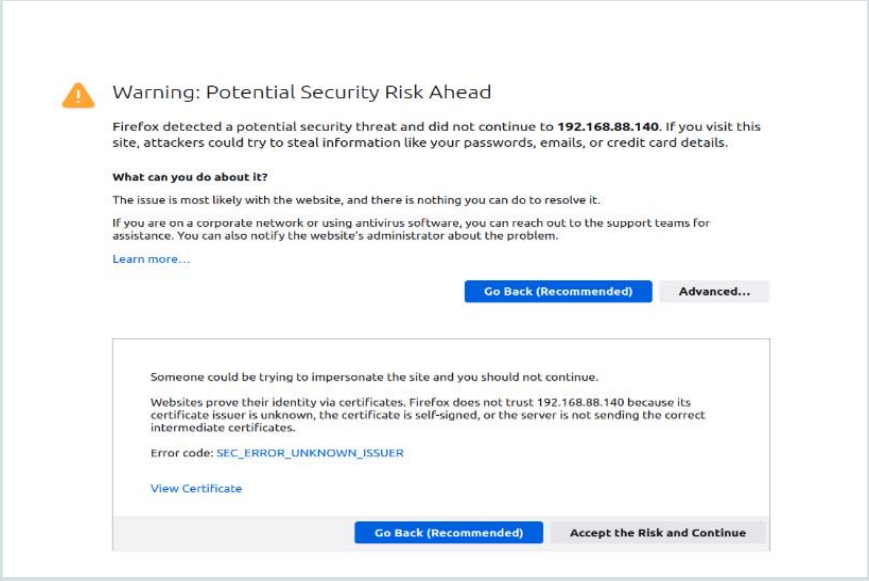

Figure 49

- Now, open Firefox in Ubuntu desktop and type in IP address that we noted at end of SecOnion configuration. Then click on 'Advanced' and click 'Accept the risk and continue'

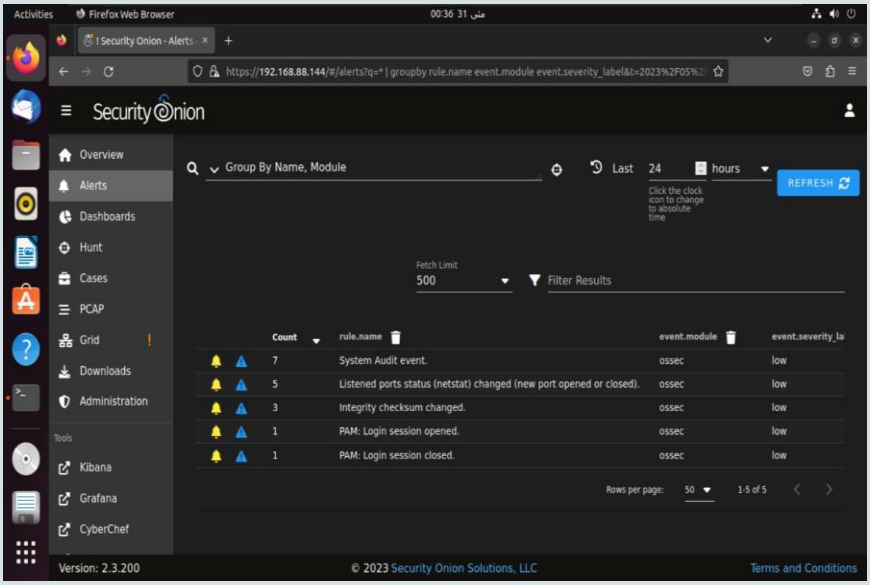

Figure 50

- In the above you can see the web interface of the SecOnion WebGUI. This ends the configuration of the SecurityOnionMgmt VM.

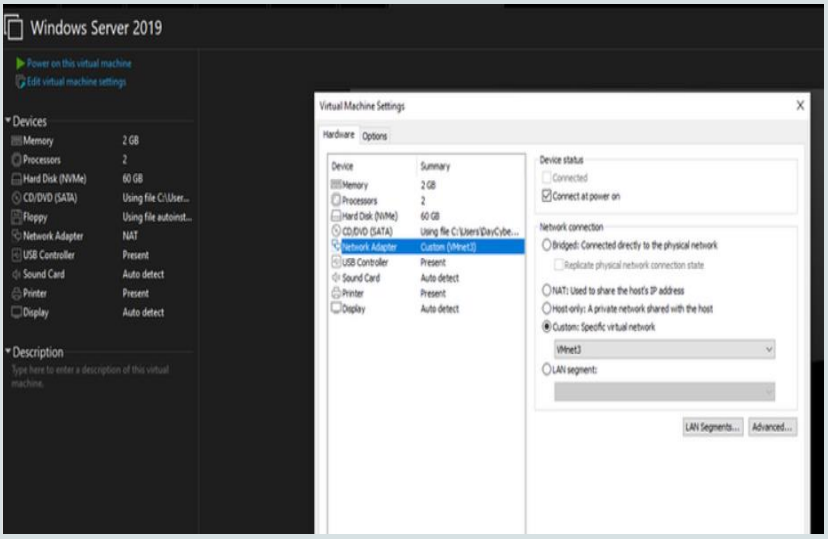

Figure 51

- Install in VMware as usual with defaults, do not worry about a product key, simply click Next. At the end of the installation, be sure to change the Network Adapter to Vmnet3. Make sure to UNCHECK 'Power on this virtual machine after creation'.

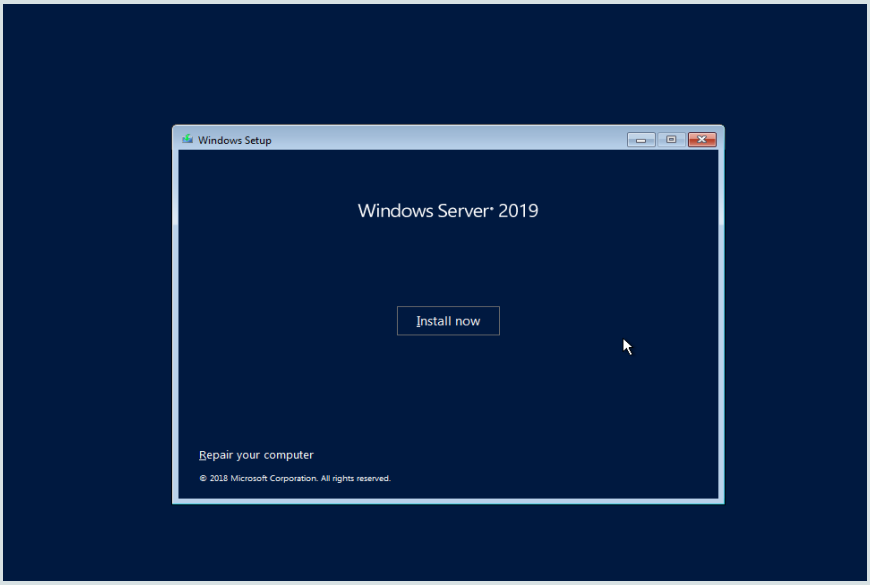

Figure 52

- Power on the Virtual Machine and immediately click any key. Click 'Next' and then click 'Install Now'.

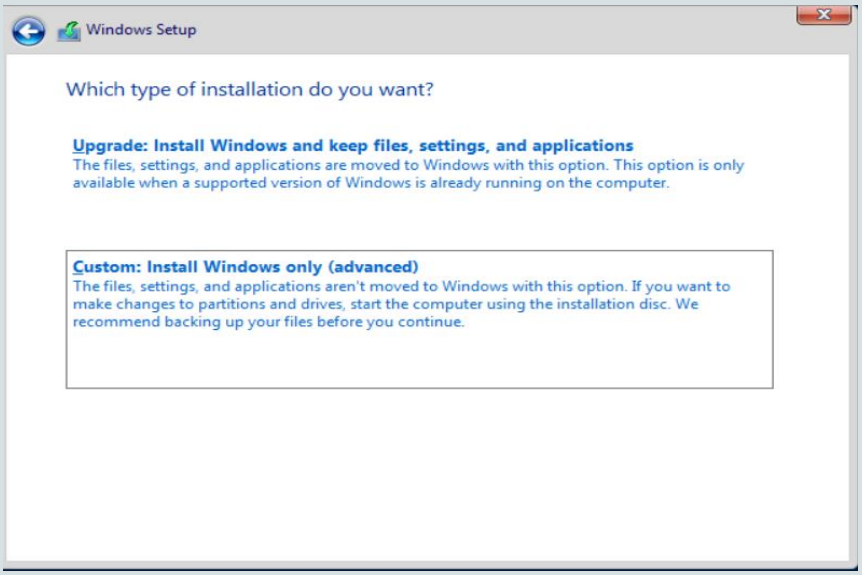

Figure 53

- Select the Windows Server 2019 standard Evaluation (Desktop Experience). Accept the License Terms. Then Click Next and Select the Custom Install.

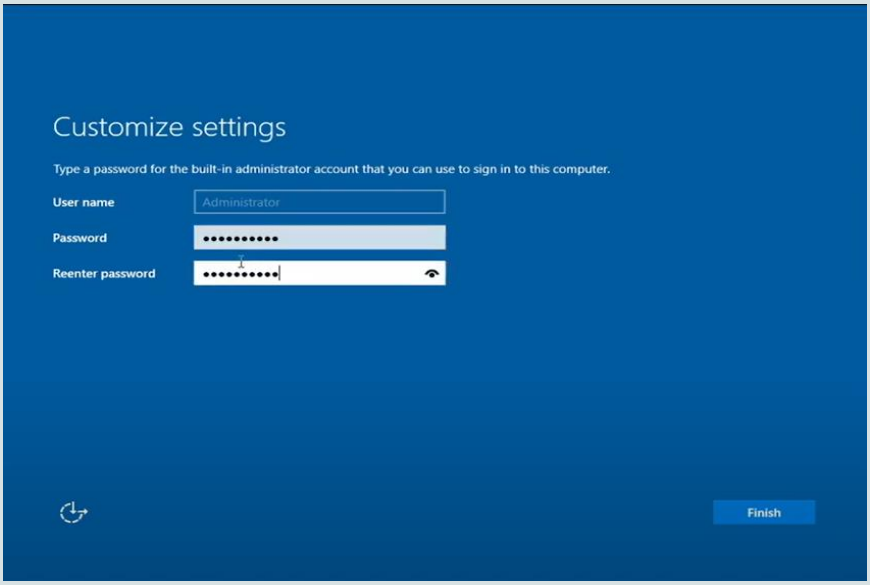

Figure 54

- When the installation is complete, above screen appears then create a password and click 'finish'.

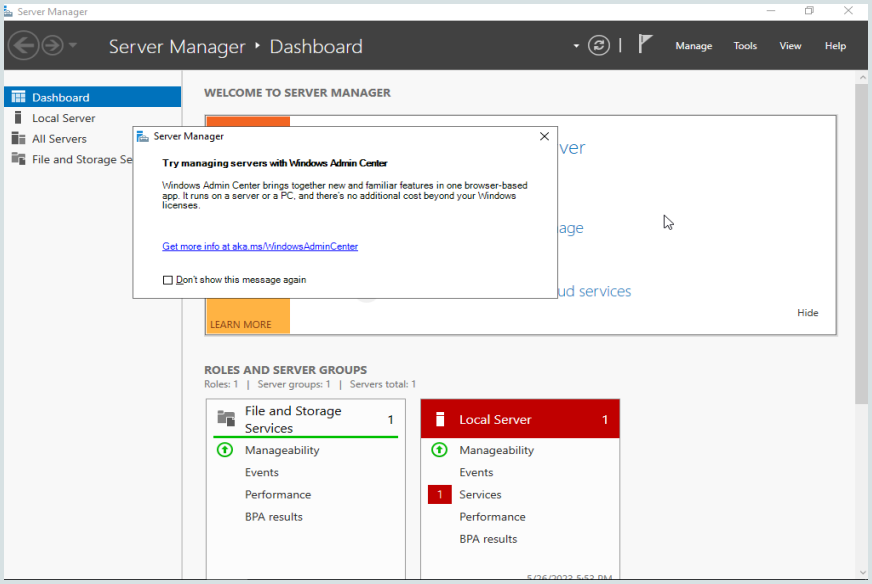

Figure 55

- After the installation, you should end up with this screen.

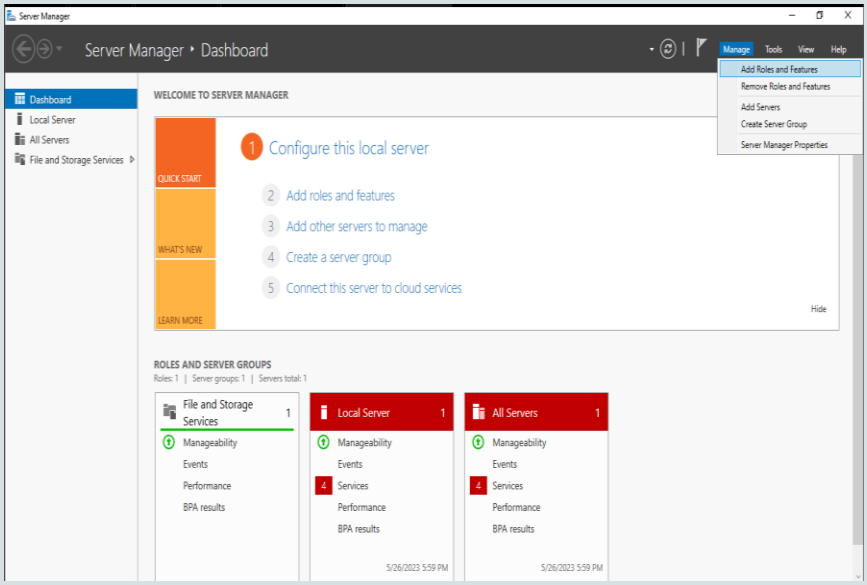

Figure 56

- After the reboot, on the Server Manager Dashboard, Click Manage >> Add Roles and Features

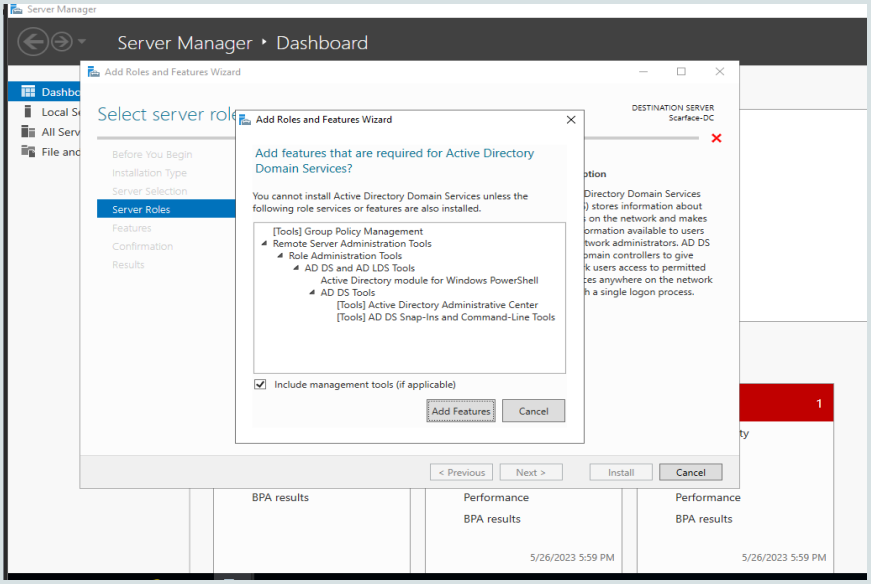

Figure 57

- Keep clicking 'Next' till you get to the 'Server Roles' menu. Then select 'Active Directory Domain Services' and then select "Add Features".

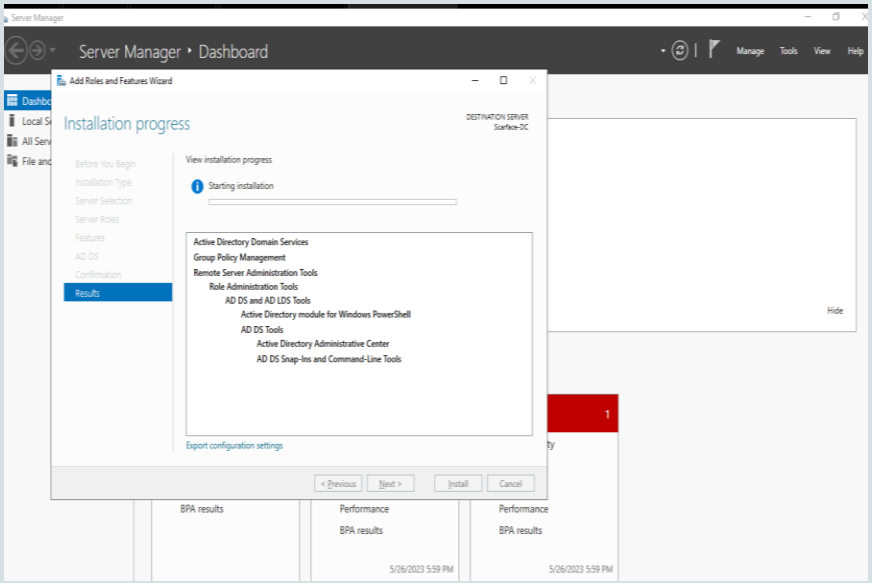

Figure 58

- Click on 'Next' till you get to the Confirmation menu, then click 'Install' After the Install, Click 'Close'.

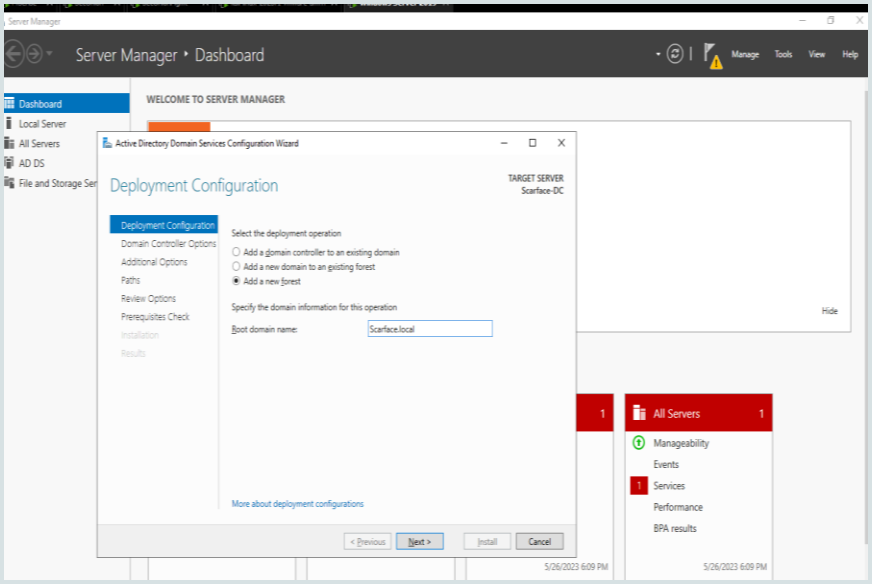

Figure 59

- Click on the flag with the yellow caution triangle. Select ‘Promote this server to a domain controller’ and then select ’Add a new forest’, then specify a domain name. After that Click ’Next’ and then ‘Set a Password’.

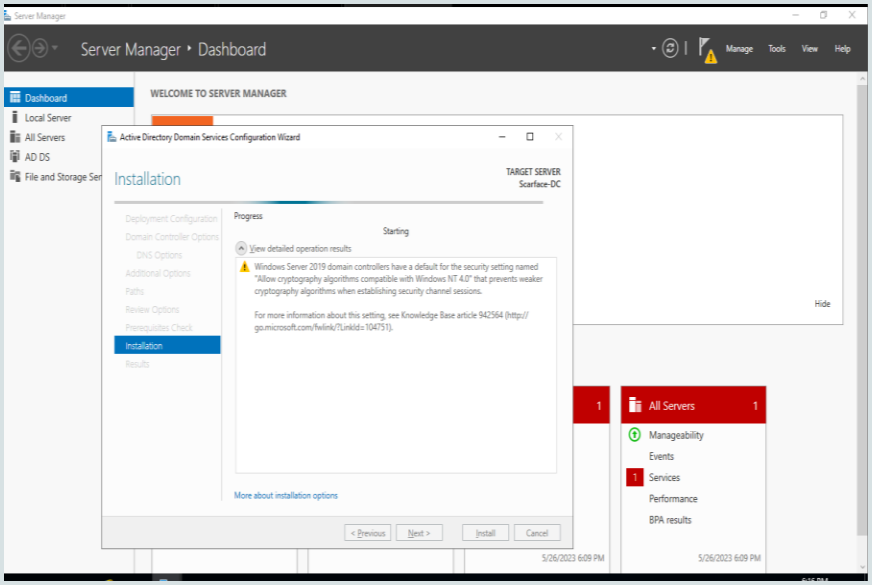

Figure 60

- Click Next till you get to the Prerequisites Check Menu and then click ’Install’. After that Wait for the Reboot

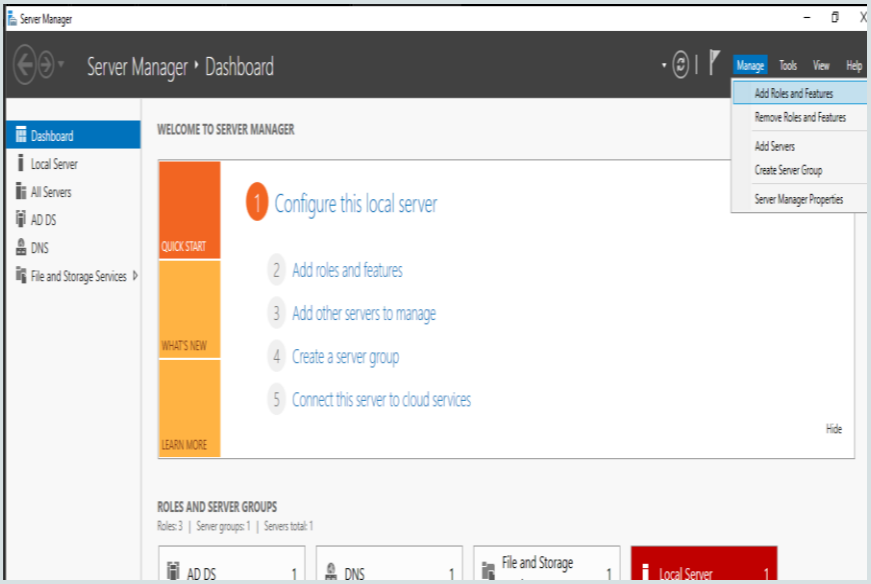

Figure 61

- After the Reboot, Log back in Select Manage >> Add Roles & Features again on the Server Manager and then click 'Next' till you get to 'Server Roles'.

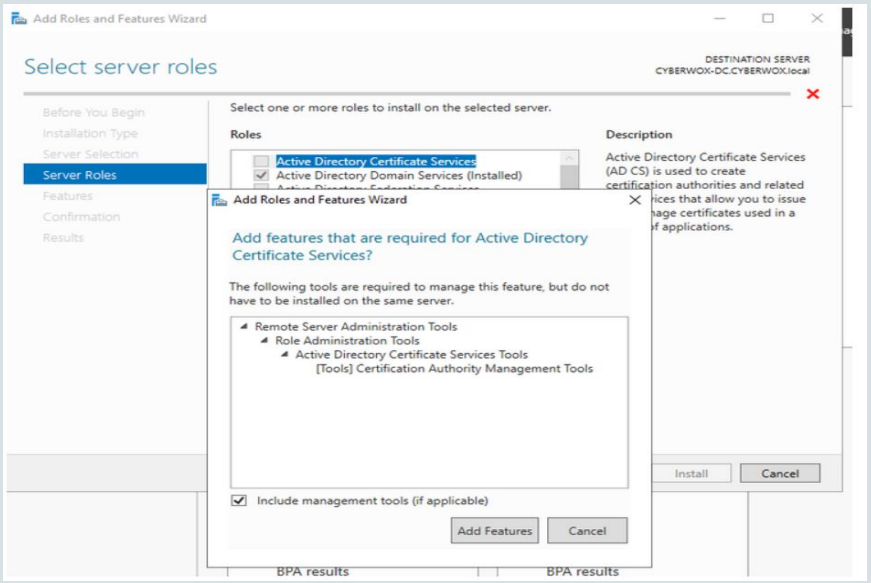

Figure 62

- Select 'Active Directory Certificate Services' and then select 'Add Features'.

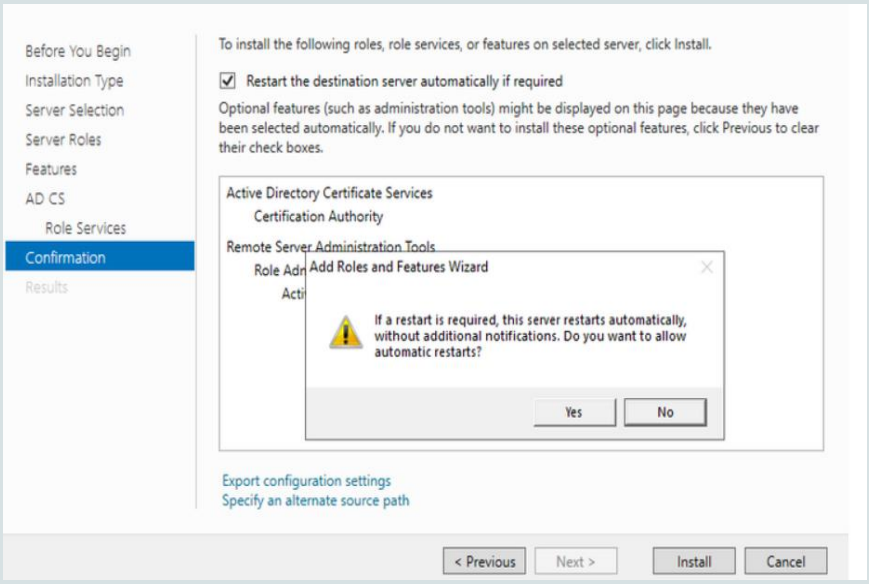

Figure 63

- Click Next till you get to the 'Confirmation' menu and then check 'Restart the destination server automatically if required' and then select 'Yes'. After that select 'Install' and then click 'Close'

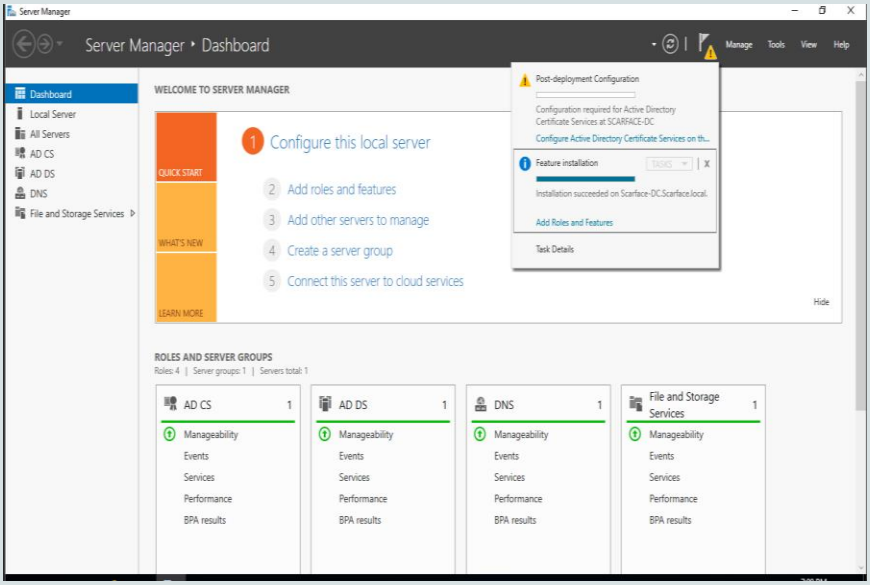

Figure 64

Click on the flag with the yellow caution triangle. Select 'Configure Active Directory Certificate Services on the destination server'

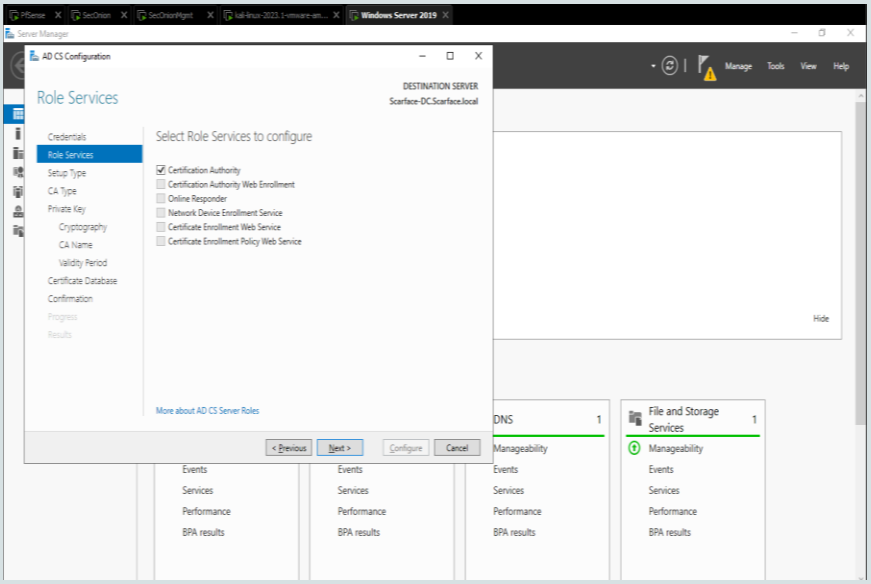

Figure 65

- Click 'Next' on credentials. On the 'Role Services' menu, check 'Certification Authority'.

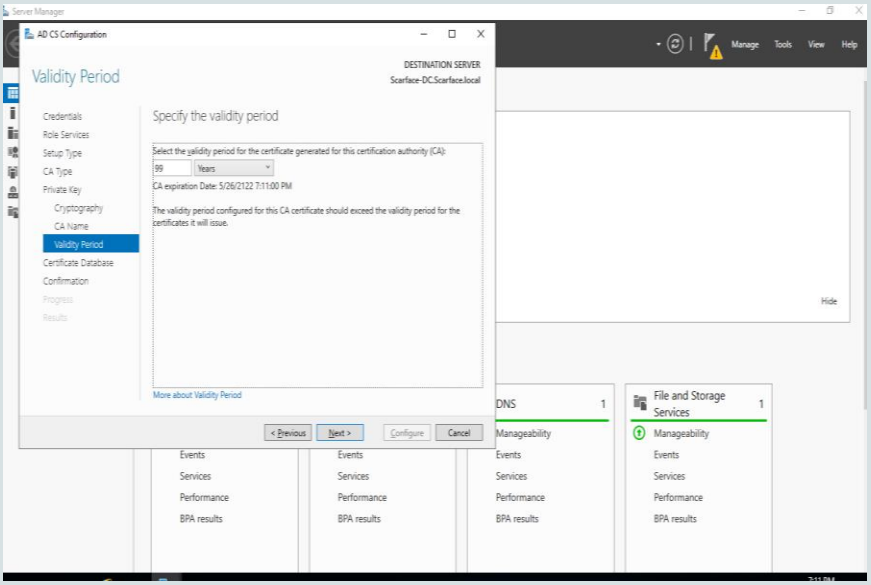

Figure 66

- Click Next till you get to the Validity period menu and change it to 99 years. Click 'Next' till you get to the Confirmation menu, then select 'Configure'.

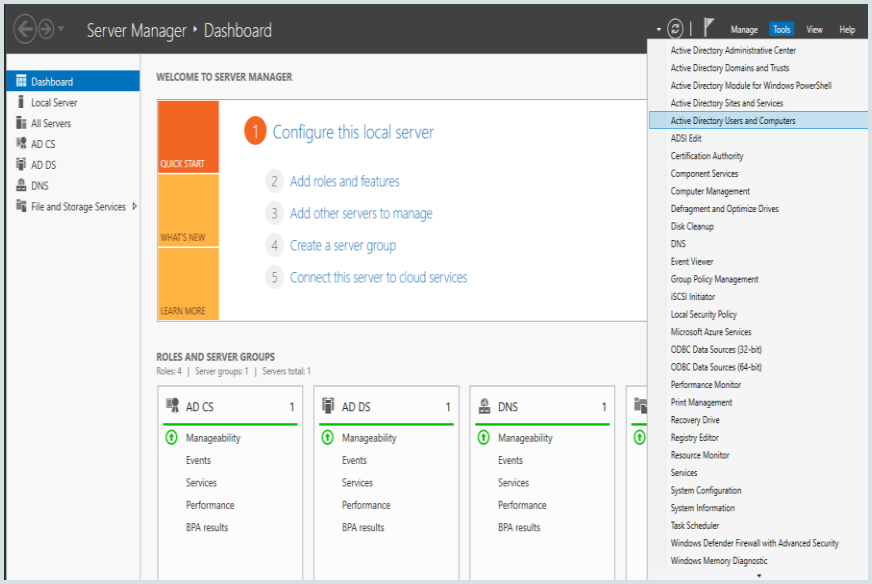

Figure 67

- Manually restart the server in order for all the settings to take effect. Now add some Users. Back at the Server Manager Select 'Tools > Active Directory Users and Computers'.

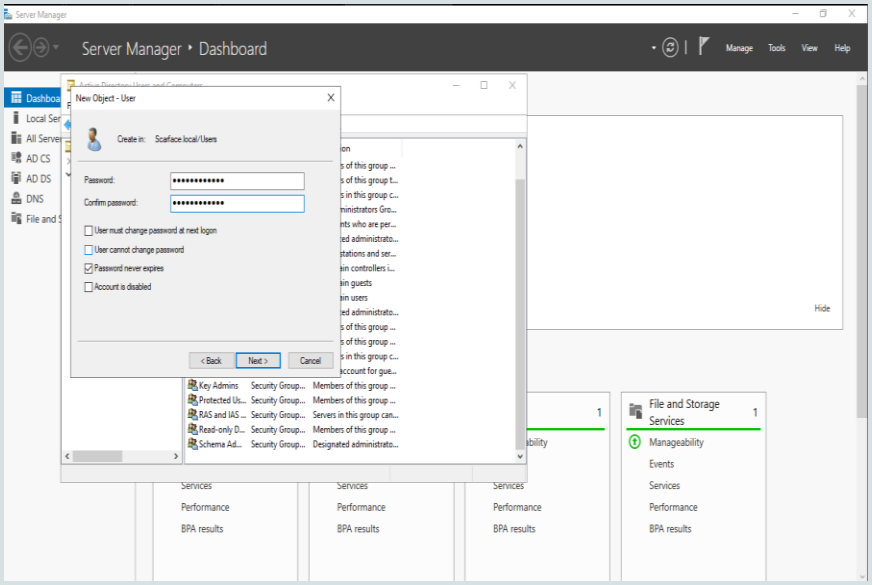

Figure 68

- Select your Domain Name > Users, Right Click & Select New > User. Enter a First, Last & User logon name for the user. Set a password that never expires. Select 'Finish'.

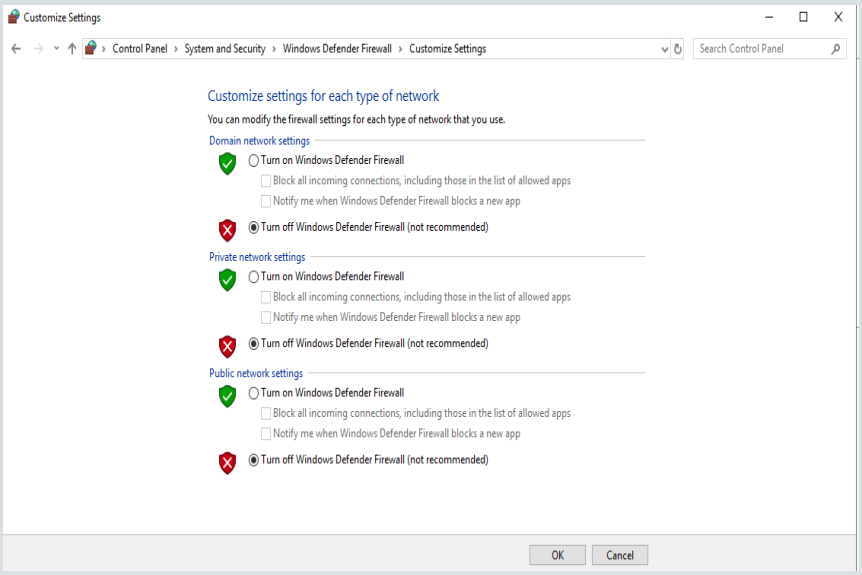

Figure 69

- Search for 'Windows Defender Firewall' > Turn Windows Defender Firewall on or off. Turn off the firewall for all Networks

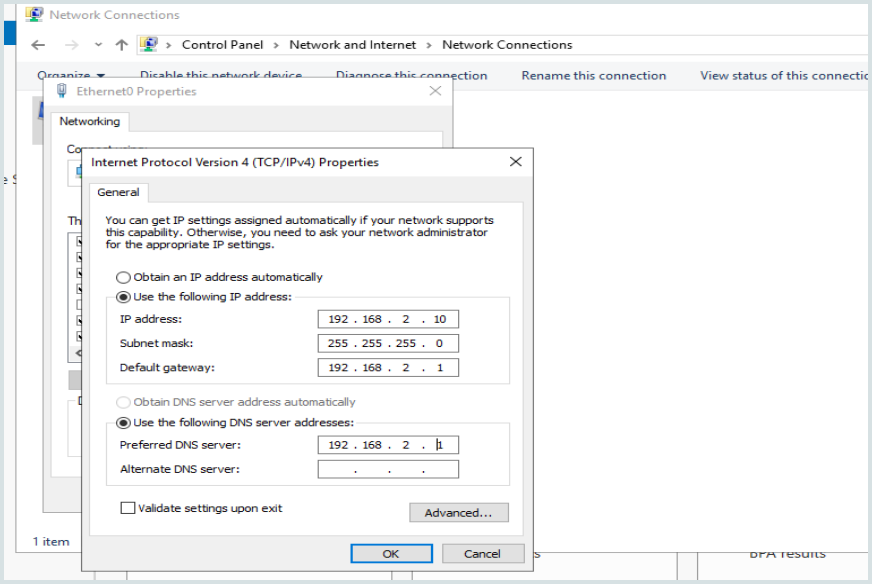

Figure 70

- Now Use Pfsense as the default gateway for the Domain Controller. Navigate to Control Panel > Network and Internet > Network Connections. Enter the above configuration

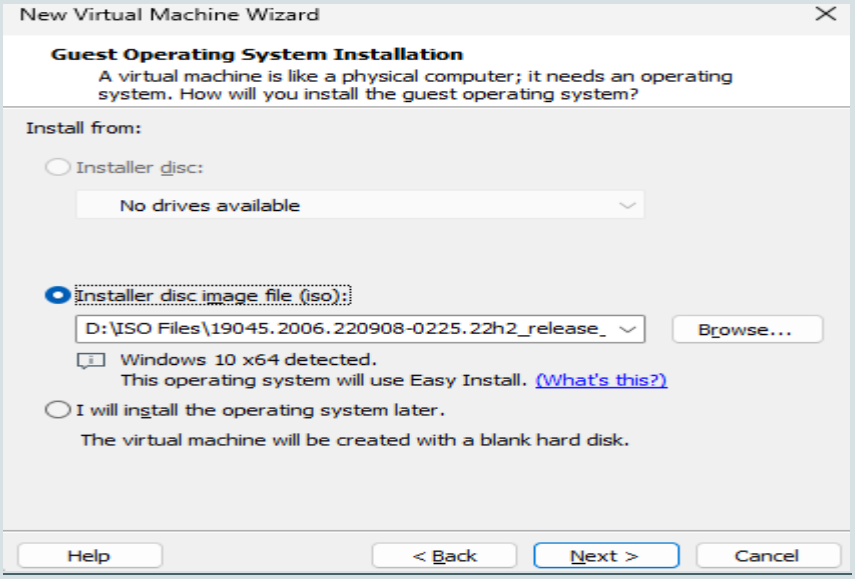

Figure 71

- Open VMware and select 'create a new virtual machine', select 'typical configuration' and click on 'next' and select the PF sense ISO image file click on 'next' to proceed.

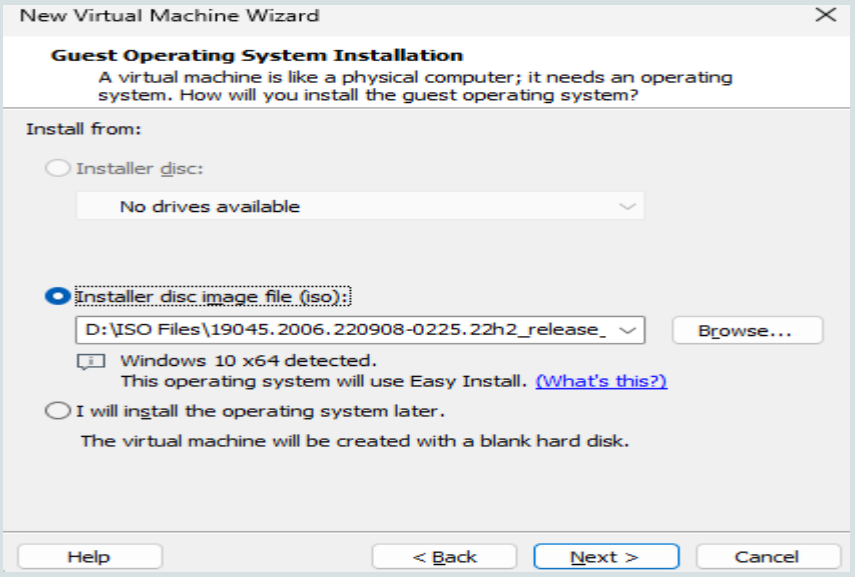

Figure 72

- Open VMware and select 'create a new virtual machine', select 'typical configuration' and click on 'next' and select the PF sense ISO image file click on 'next' to proceed.

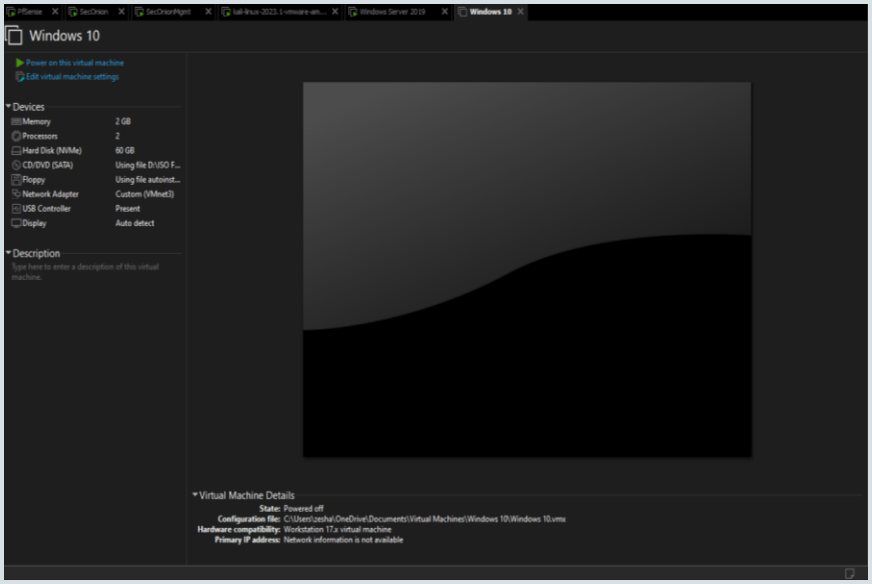

Figure 73

- Name the virtual machine the first user you set in your DC. At the end of the installation, be sure to change the Network Adapter to Vmnet3. Make sure to UNCHECK 'Power on this virtual machine after creation'. After VM has been installed, click 'Edit virtual machine settings' and remove the Floppy drive.

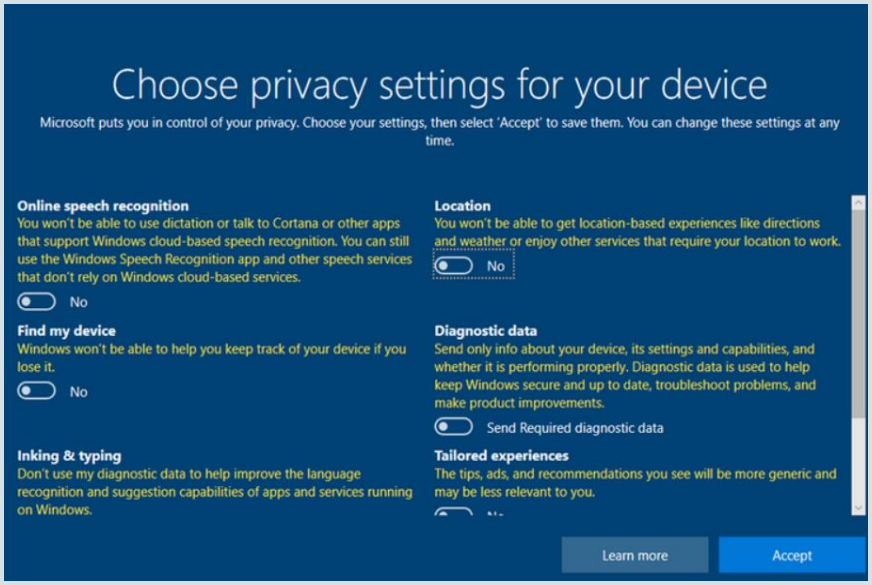

Figure 74

- Uncheck ALL the privacy settings then select Accept.

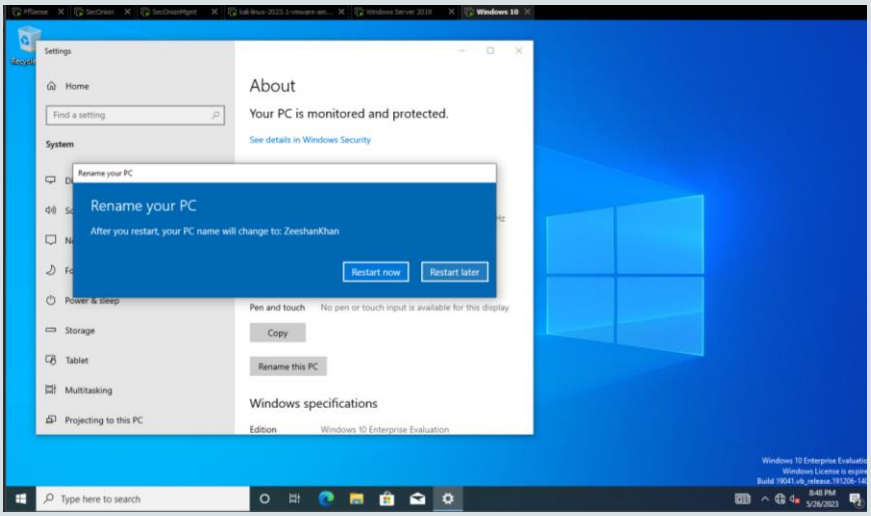

Figure 75

- Choose ‘Not Now’ for Cortana. Search ‘pc name’ and change the PC Name according to the designated users. Restart the PC

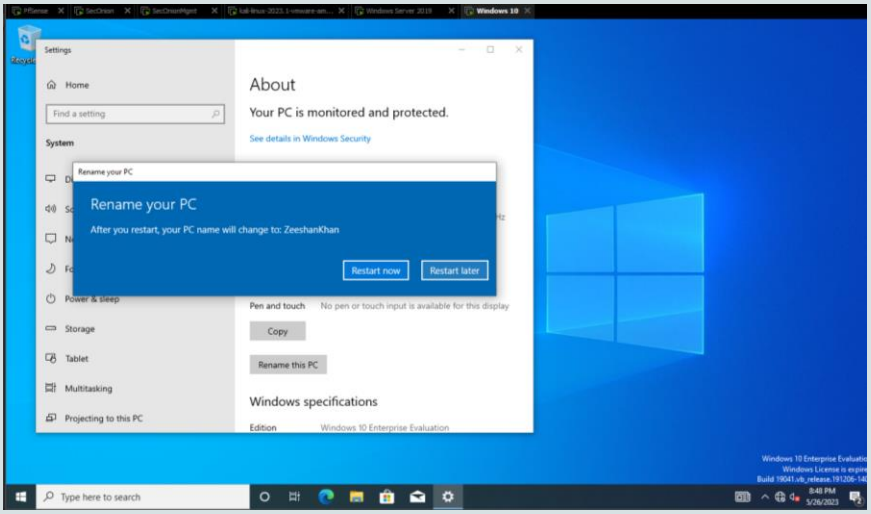

Figure 76

- Navigate to Network Adapter settings, then right-click on Etherneto and select properties and select IPV4 add an IP Address(192.168.2.21) & Use 192.168.2.1 as the default gateway. Use 192.168.2.10(Victims Network) as the DNS Server

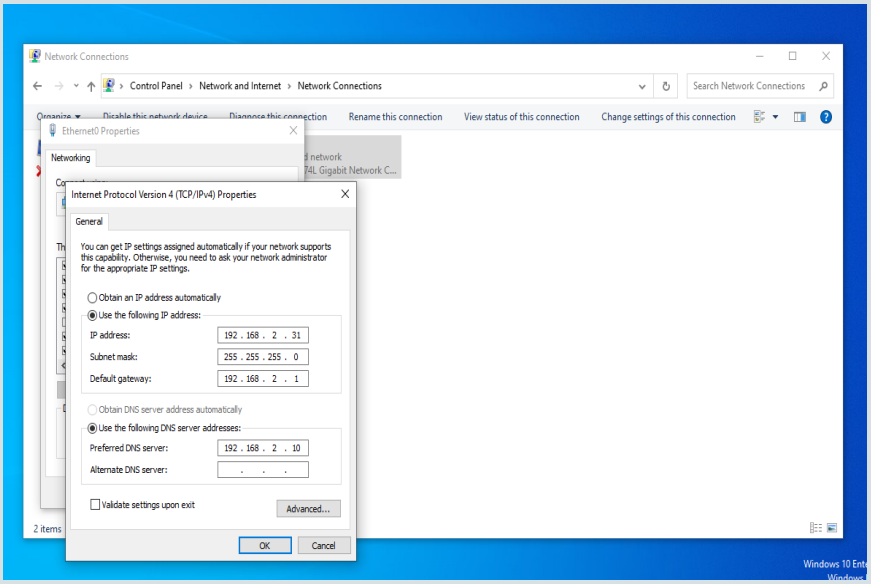

Figure 77

- Navigate to Network Adapter settings, then right-click on Etherneto and select properties and select IPV4 add an IP Address(192.168.2.21) & Use 192.168.2.1 as the default gateway. Use 192.168.2.10(Victims Network) as the DNS Server

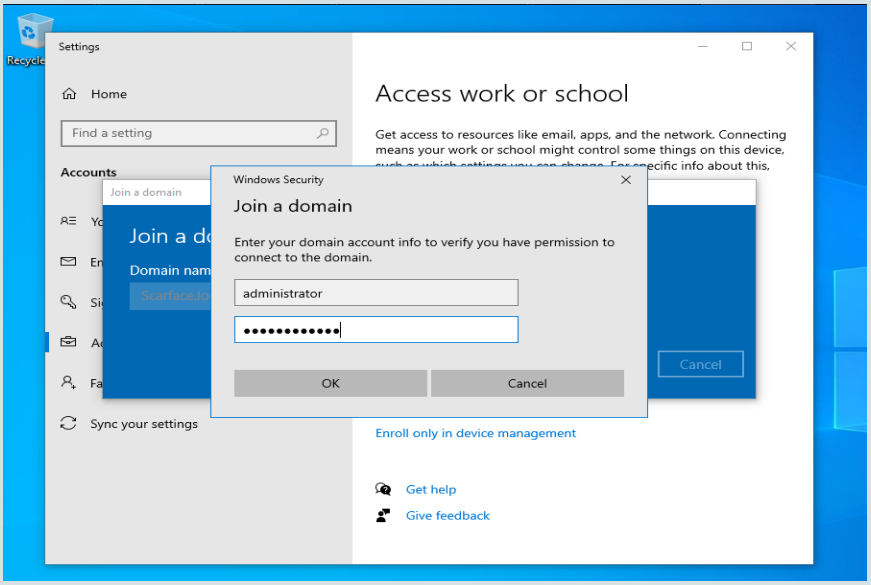

Figure 78

- Search ‘domain’ and select ‘Access work or school account’. Select Connect > Join this device to local Active Directory Domain Enter your domain name.local

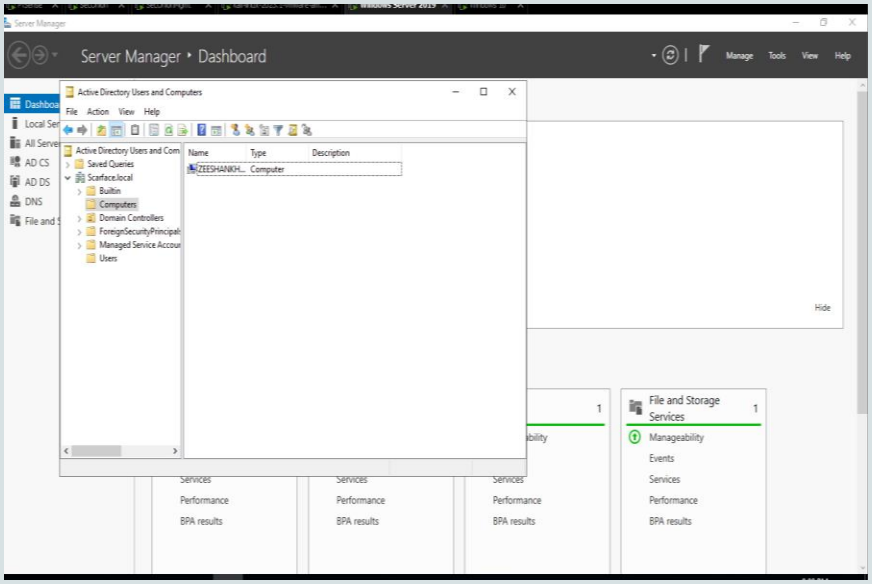

Figure 79

- Now head back to windows server, you can see in active directory and users the pc, we connect domain controller in previous step.

Virtual Machine for Splunk

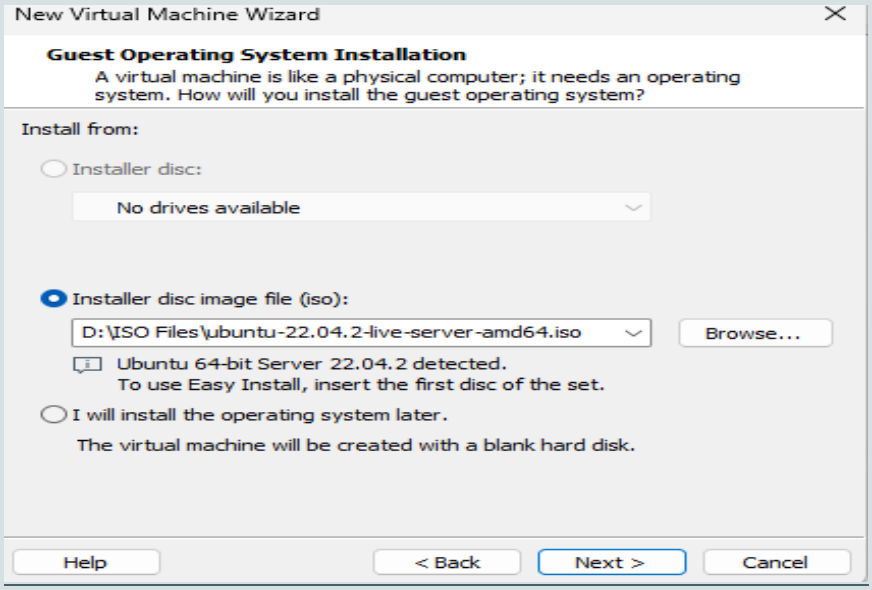

Figure 80

- Open VMware and select ‘create a new virtual machine’, select ‘typical configuration’ and click on ‘next’ and select the Ubuntu Server iso file and click on ‘next’ to proceed.

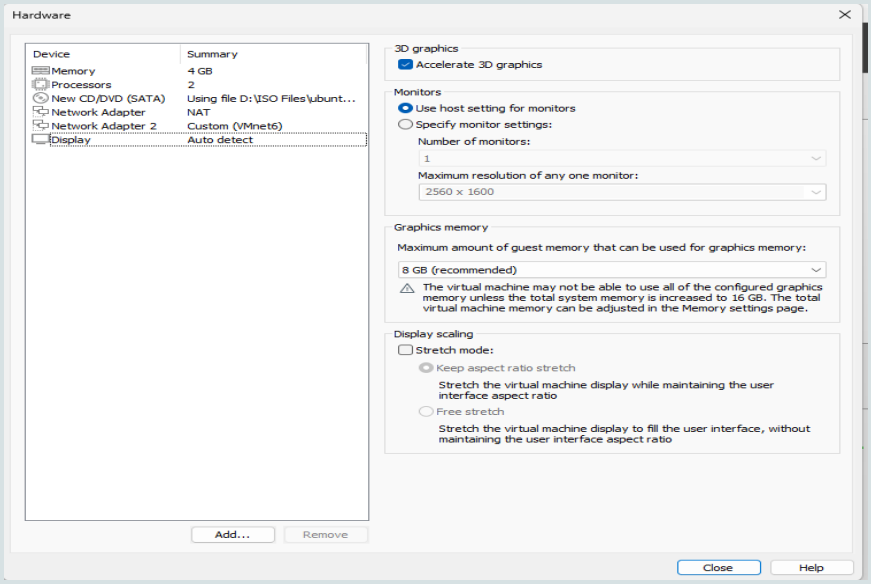

Figure 81

- Before powering on the machine, enter the Virtual Machine Settings and remove the Floppy drive with the file autoinst.flp

Ubuntu Server Installation

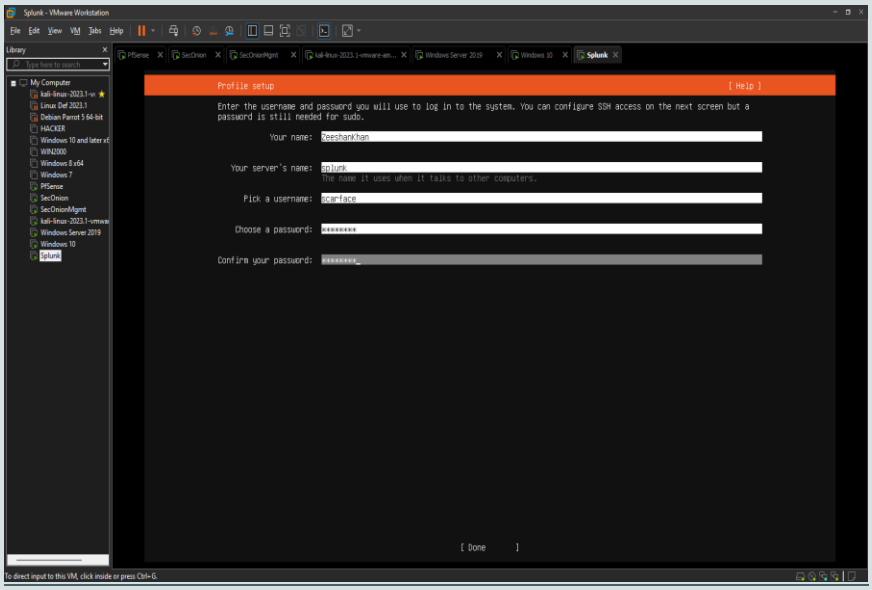

Figure 82

- Install the server using all the default settings and create a profile.

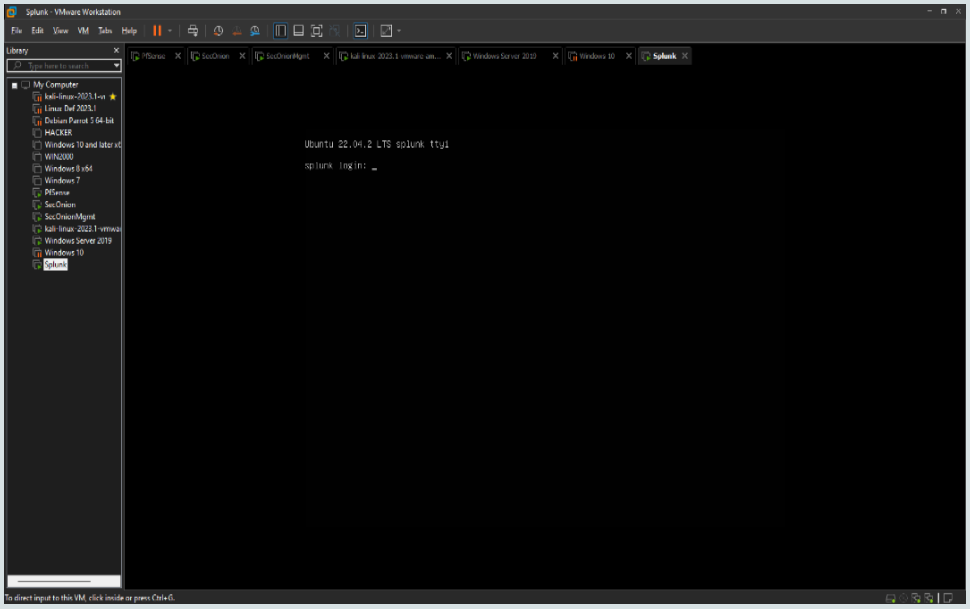

Figure 83

- During the installation, you'll be prompted to remove the CD(ISO) remove it and then reboot the VM.

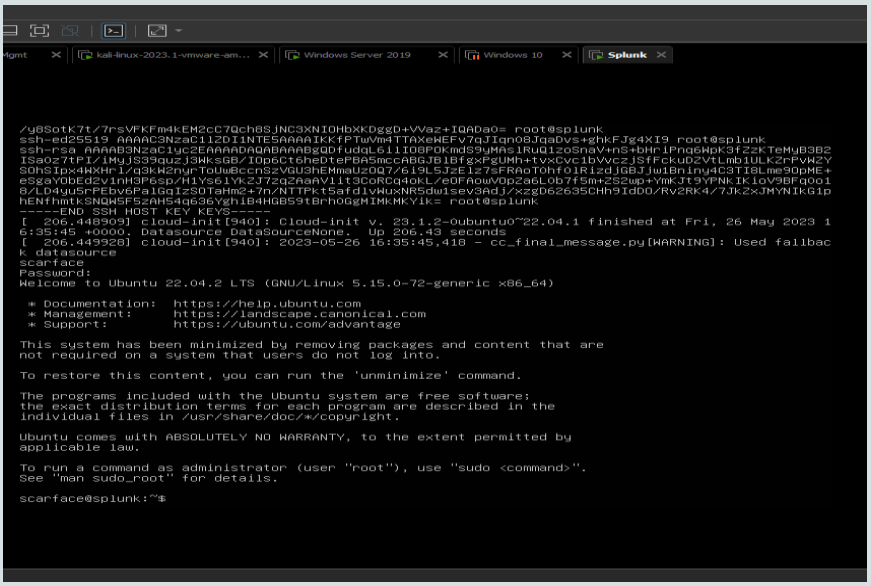

Figure 84

- After the VM has rebooted, your sign-in screen should look something similar to this.

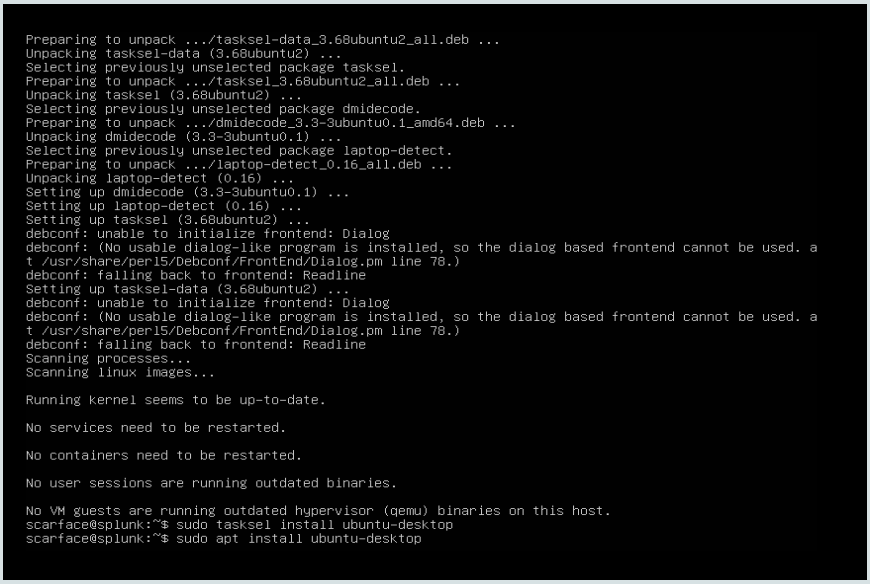

Figure 85

- For the Splunk server, we will install a GUI on the Ubuntu Server using the command sudo apt install ubuntu-desktop.

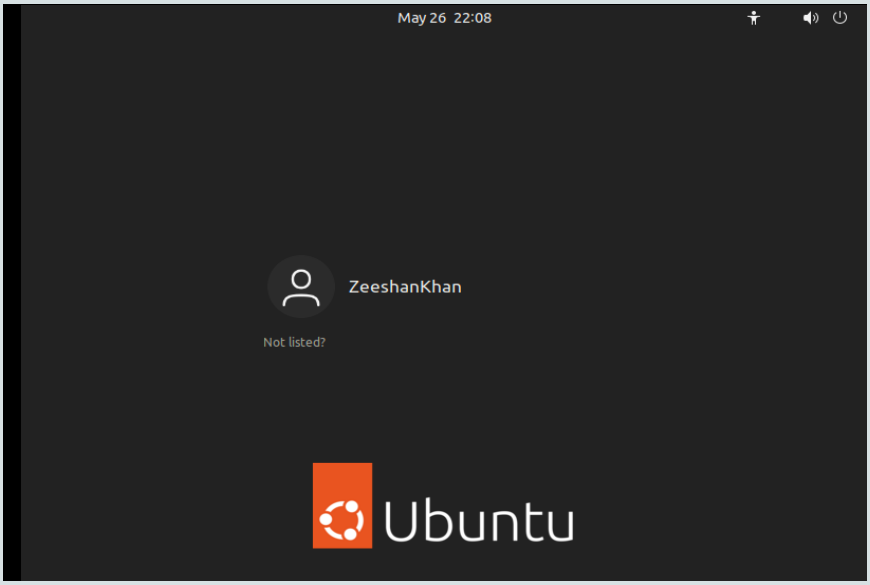

Figure 86

- After rebooting, you should see that GUI is installed in Ubuntu server for easy and user friendly interaction.

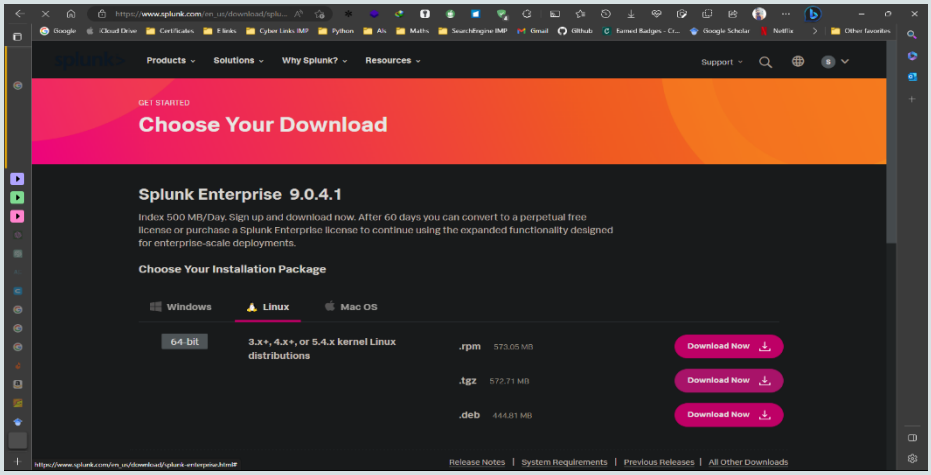

Figure 87

- On your Ubuntu Server, Navigate to Splunk.com and Click on 'Free Splunk'. Then create an account. Under 'Splunk Core Products' >> Splunk Enterprise >> Download Free 60-Day Trial. Select the Linux package and download the .tgz file

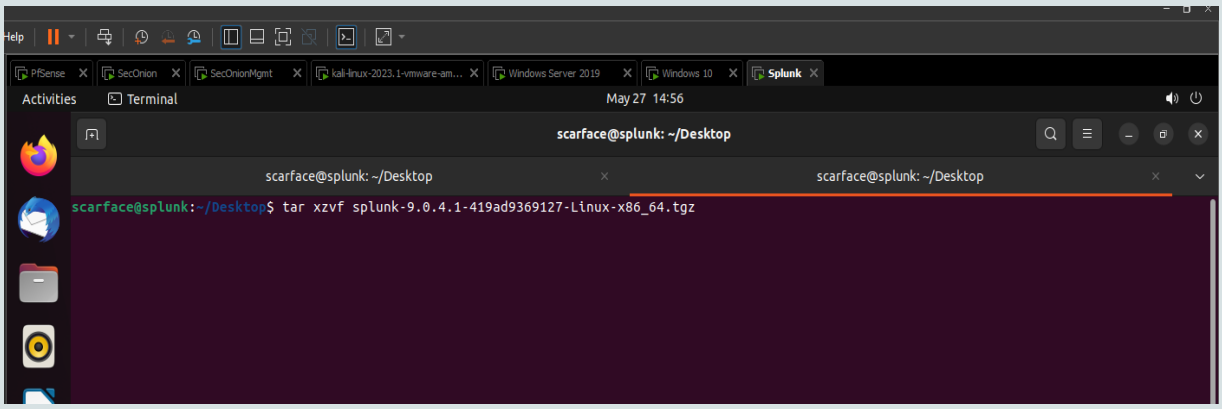

Figure 88

- Open the terminal and navigate to the downloads directory and un-zip the file by running tar xvzf splunk-9.0.4.1-419ad9369127-x86_64.tgz.

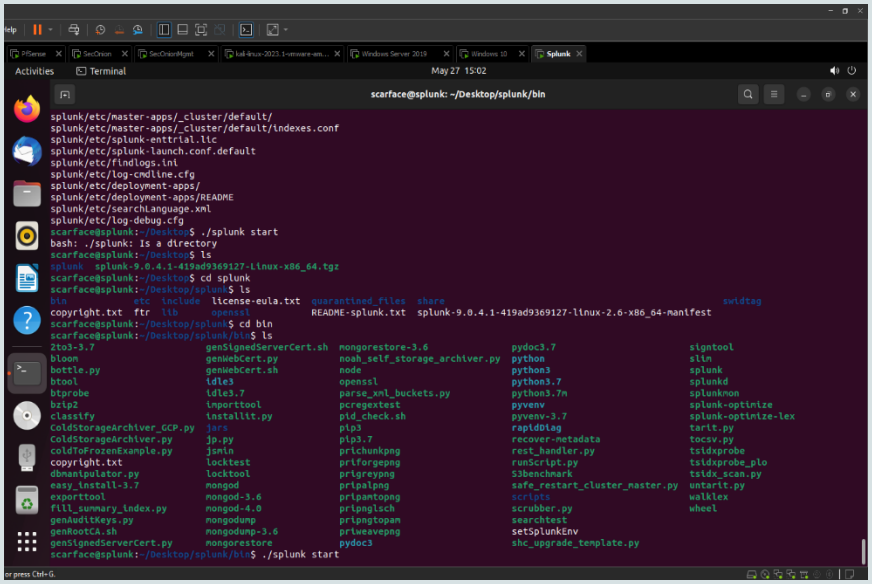

Figure 89

- Navigate to the ~/splunk/bin directory and use the command "./splunk start" to start the splunk instance and Enter an admin username and password of your choice.

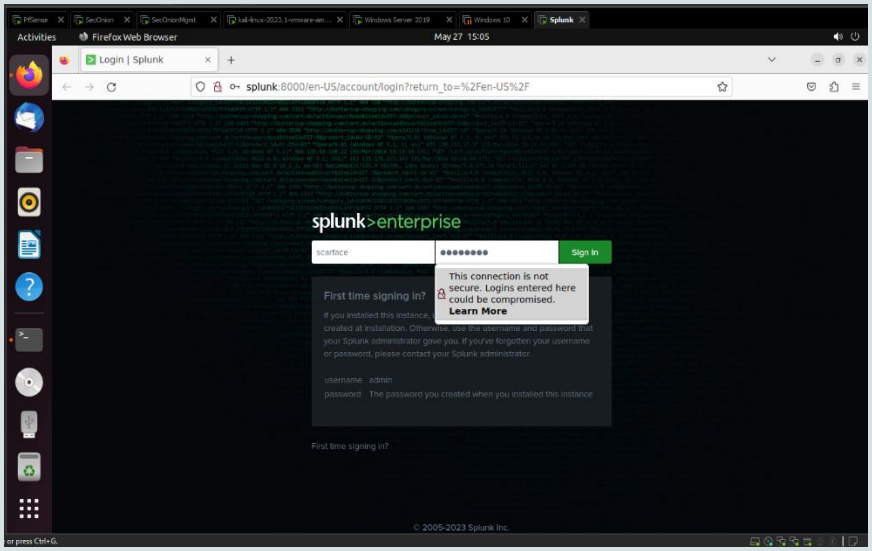

Figure 90

- Navigate to http://splunk:8000 your browser and Log in with the username and the password you configured in the previous step.

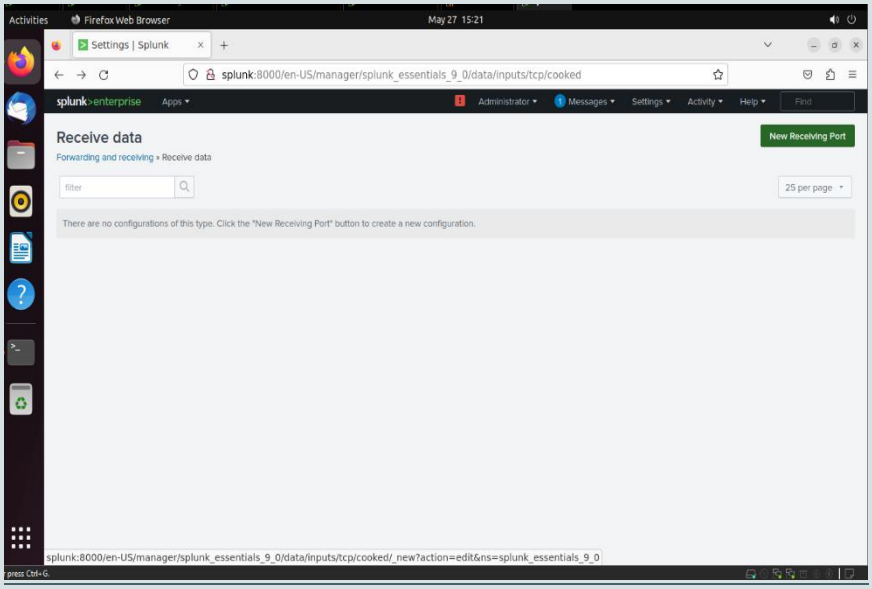

Figure 91

- Set up “Receiving” on your Splunk server and Navigate to Settings >> Forwarding and Receiving >> New Receiving Port

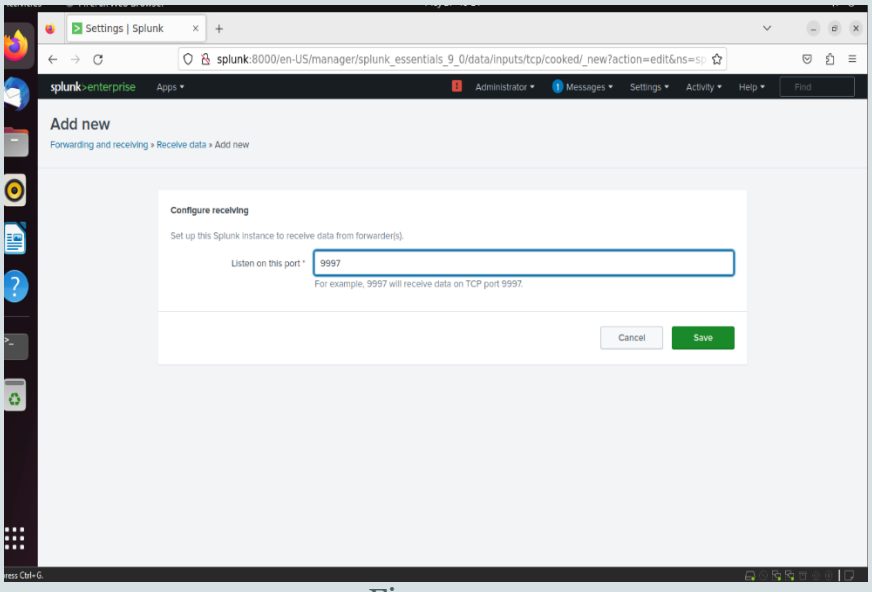

Figure 92

- Enter port 9997 and save.

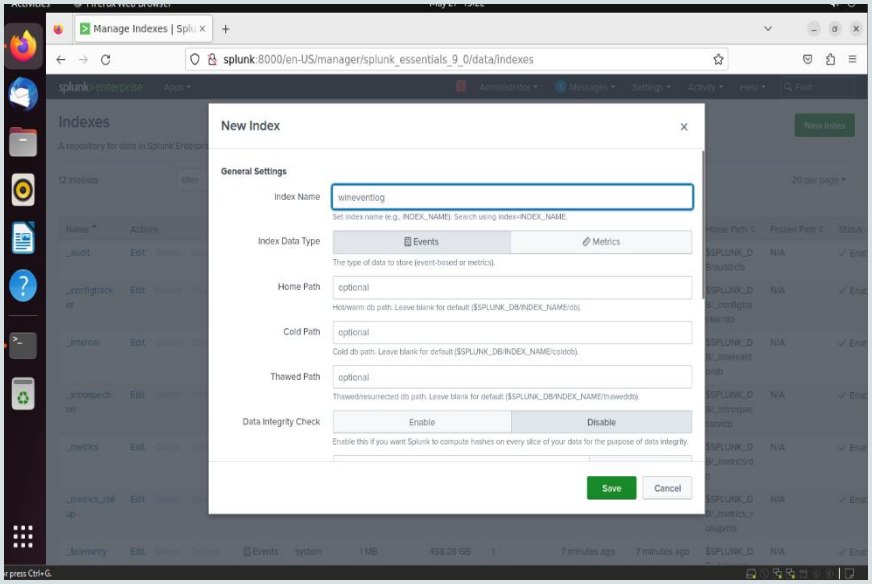

Figure 93

- Navigate to Settings >> Indexes >> New index and name the index ‘wineventlog’ and click Save.

Splunk Universal Forwarder

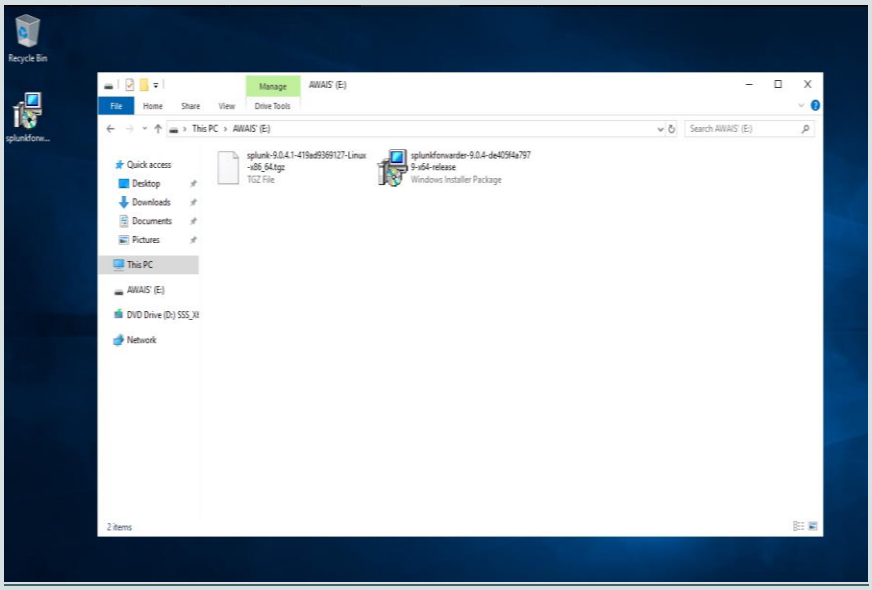

Figure 94

- On your Domain Controller (Windows Server 2019, Download the Universal Forwarder by going to splunk.com.

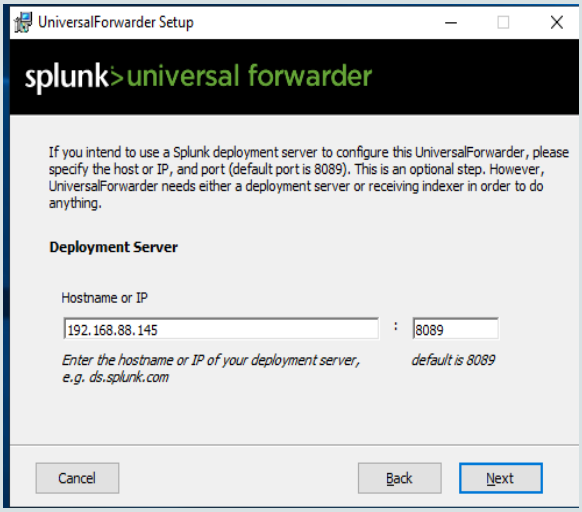

Figure 95

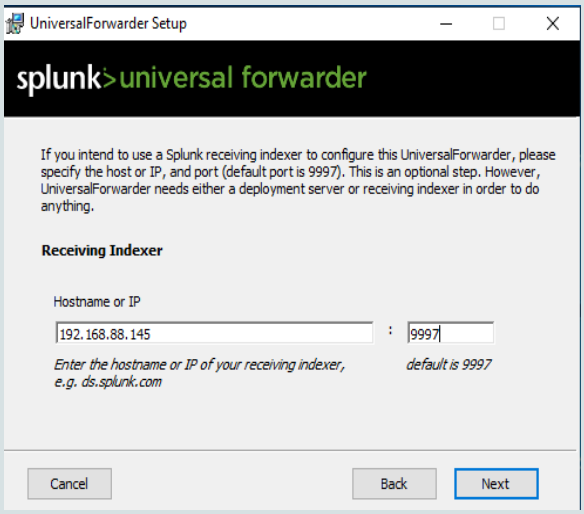

Figure 96

- Now for the installation of the Forwarder, Accept the License Agreement & click Next and create a preferred username and password and Enter the IP Address of your Splunk server and theefault ports as prompted (8089 & 9997) and click Install

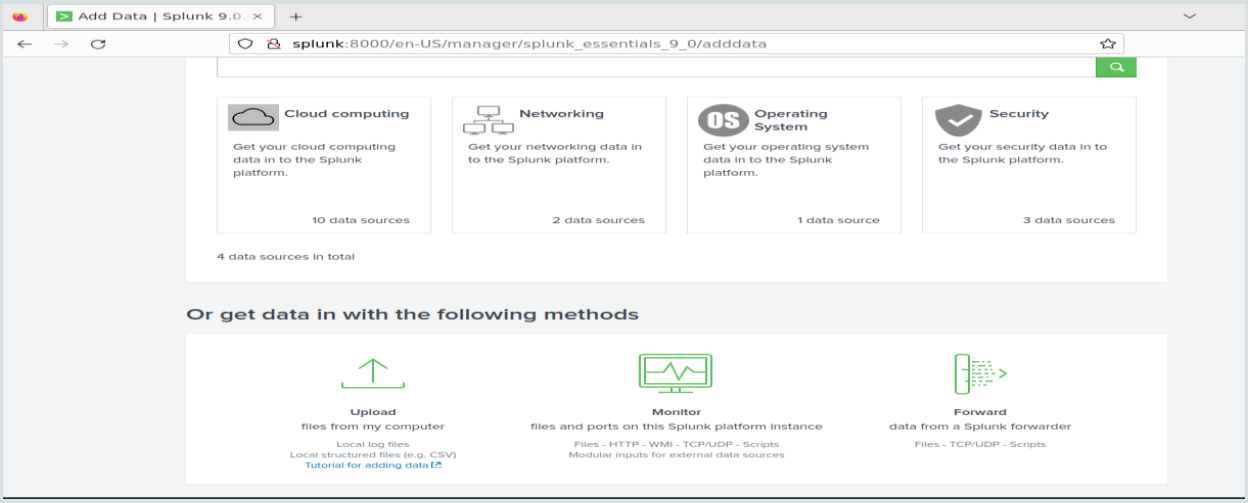

Figure 97

- Navigate back to your Splunk Instance >> Settings >> Add Data and select 'Forward'

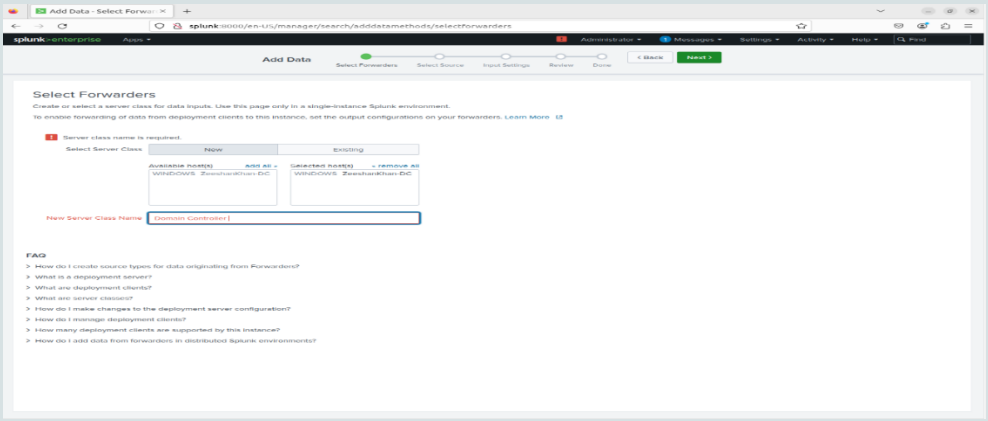

Figure 98

- Select the Domain Controller (Windows Server) >> Enter a Server Class Name e.g “Domain Controller” >> Next

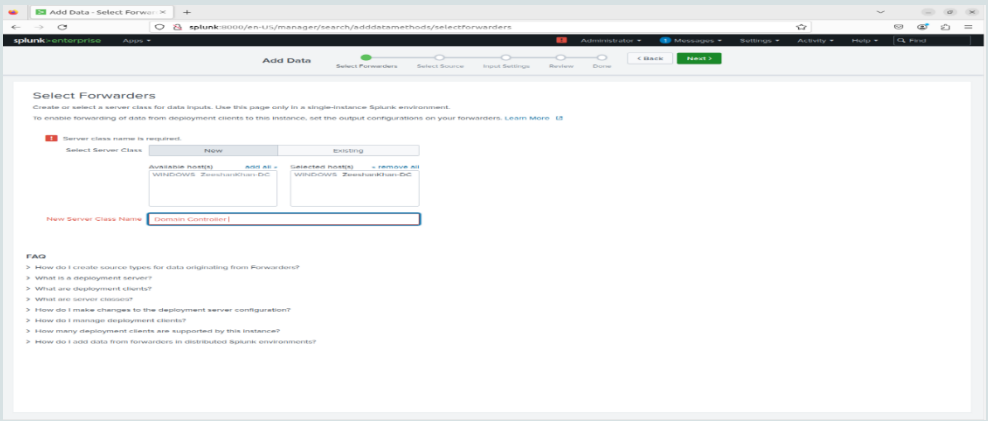

Figure 99

- Select the Domain Controller (Windows Server) >> Enter a Server Class Name e.g ‘Domain Controller’ >> Next

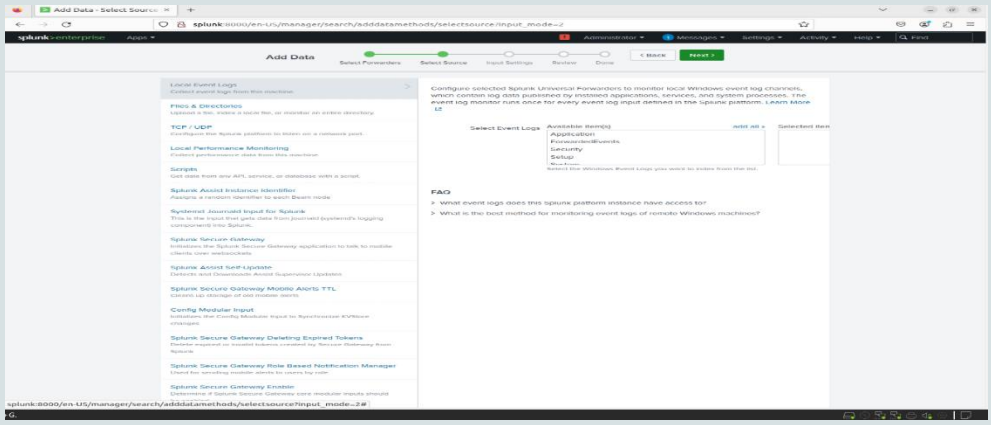

Figure 100

- Select the Local event >>Select all options and click on ‘next’. After that select wineventlog’ as the index then Review and Submit. This brings us to the end of this lab. This was fun and exciting to work on and I hope you found value in this process.

Lab Analysis

Task	Executed (Yes/ No)	Notes
Splunk deployment	Yes	Deployed using VMware, pfSense, Security Onion, Kali Linux, Windows Server/10, Splunk & Universal Forwarder, Ubuntu Server,

Details of task

It has been observed that requisite information (windows logs) can be accessed by the above mentioned tool deployment. Observations have been duly shared in this document.

Impact

Splunk for Windows log monitoring improves visibility, enabling real-time detection of security threats and operational issues. Centralized log management with it streamlines analysis, correlation, and reporting, aiding in compliance and troubleshooting. It's scalability and flexibility helps in empowering organizations to efficiently monitor and optimize their Windows infrastructure.

Remediation/ Recommendations

Apart from windows log monitoring, Splunk may also be used for search and analysis, correlation searches, dashboards, visualizations, machine learning, anomaly detection, compliance, reporting, and data archival.

Revalidation

Not required.