Day Cyberwox · Apr 26, 2021 · 12 min read

Building a Cybersecurity Homelab for Detection & Monitoring

Updated: Jan 9, 2022

For troubleshooting/help with this lab, please join our discord server and I'll be glad to help!

Discord

In Cybersecurity, it could be a daunting task to apply and implement security concepts if there is an unavailability of practical and safe infrastructure to carry out these activities.

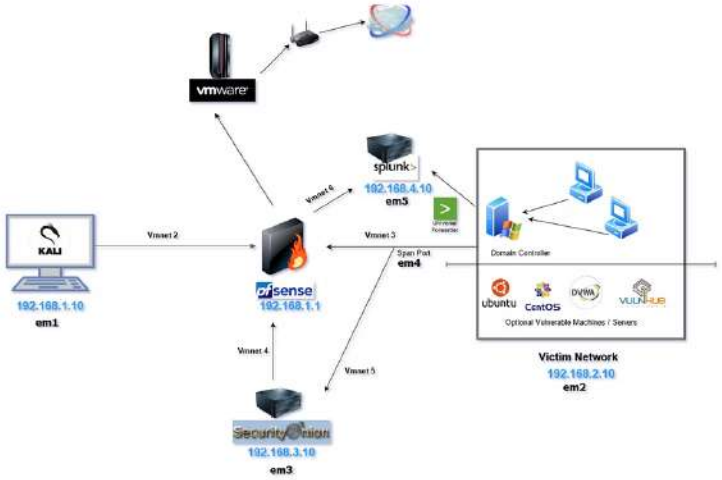
I approached this project with that in mind. This homelab walks through the process of configuring, optimizing, and securing an I.T infrastructure. Although this will be at a relatively small scale, you will be able to apply the knowledge gained in a real-world large-scale/enterprise infrastructure.

What is a Homelab?

A Homelab, as the name implies, is an environment in your home that is used to practice and improve your skills in a specific field. This home lab has components and tools similar to large-scale infrastructures. It's a safe environment to work with these components and learn how they work.

CONTENT

HOMELAB NETWORK DESIGN & TOPOLOGY



Building The Host PC

For this lab, I'll be using a PC I built a while back specifically for this purpose. The hardware requirements are listed below:

CPU: AMD Ryzen 5 3600X 3.8 GHz 6-Core Processor
RAM: G.Skill Ripjaws V Series 32 GB (2 x 16 GB) DDR4 Memory
STORAGE: Crucial P1 1TB M.2-2280 NVME SSD
GRAPHICS CARD: MSI GeForce GT 710 2 GB Video Card
MOTHERBOARD: Asus TUF GAMING X570 ATX Motherboard
HOST OPERATING SYSTEM: Windows 10 Pro
FULL PC BUILD: PC Part Picker List

Here's a video tutorial for building the PC:

You can also buy a dedicated server or even use an old laptop as long as it is capable of running all the required VMs. Typically 8GB of RAM is okay but I recommend 16GB if you can.

Downloading & Installing VMware Workstation Pro

For the purpose of this lab, I'll be using VMware Workstation 16 Pro as my hypervisor. This license costs about $120 with a student discount but I assure you it is a very worthwhile investment.

Download VMware Workstation Player

Here's a video on how to install VMware Workstation:

VirtualBox is also a free and feature-rich alternative Hypervisor from Oracle. If you cannot afford the VMware license, VirtualBox is equally good.

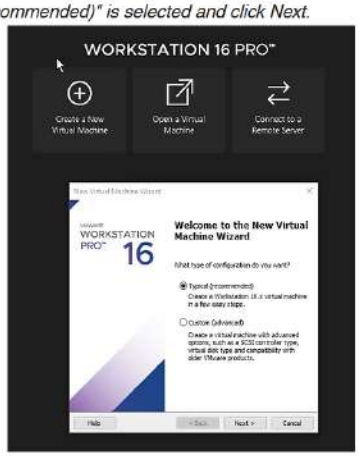
Download Virtualbox

Configuring pfsense

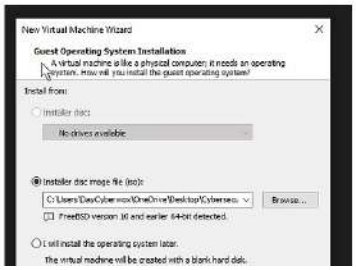
pfsense will be configured as a firewall to segment our private homelab network and will be only accessible from our Kali Linux machine.

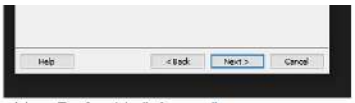
Download the pfsense ISO file from here: Download pfSense Community Edition

Click "Create a New Virtual Machine" on VMware Workstation Homescreen.
Make sure "Typical (recommended)" is selected and click Next.

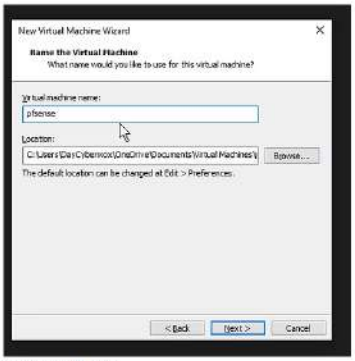


Click "Browse" and navigate to the folder where your pfsense file is located.
Click Next.





Rename your Virtual Machine. Preferably "pfsense"
Click Next.

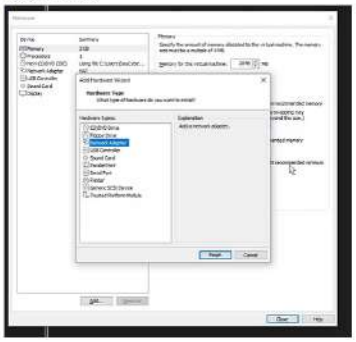


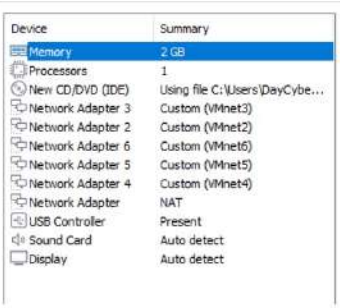
20GB disk size is sufficient for this VM.
Ensure that the "Split virtual disk into multiple files" option is selected.
Click Next.

Click "Customize Hardware".

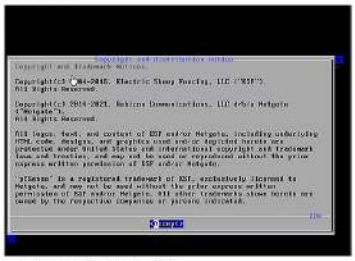
Increase the memory to 2GB.

Add 5 network adapters and correspond them with a VMnet interface as shown below. Then click Finish.





The pfsense machine will power on and start with this screen. Accept all the defaults. pfsense will configure and reboot.



You should end up with a screen similar to this.

Enter option 1

Should VLANS be set up now [y:n]?: *n*

Enter ***em0, em1, em2, em3, em4 & em5*** *respectively for each consecutive question*

Do you want to proceed [y:n]?: *y*

```
Enter an option: 1


Valid interfaces are:

em0     00:0c:29:e2:ec:5e   (up)
em1     00:0c:29:e2:ec:68   (up) Intel(R) PRO/1000 Network Connection
em2     00:0c:29:e2:ec:72 (down) Intel(R) PRO/1000 Network Connection
em3     00:0c:29:e2:ec:7c (down) Intel(R) PRO/1000 Network Connection
em4     00:0c:29:e2:ec:86 (down) Intel(R) PRO/1000 Network Connection
em5     00:0c:29:e2:ec:90 (down) Intel(R) PRO/1000 Network Connection

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
```

```
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]? y
```

Enter option 2
We'll start with the LAN interface (2)
The ip address ***192.168.1.1*** *is going to be used to access the pfsense WebGUI via the Kali Machine*

Use the configuration below for the Lan interface.

```
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
```

Use the co

```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

nfiguration below for the OPT1 interface.

```
Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Enter the number of the interface you wish to configure: 4

Enter the new OPT2 IPv4 address.  Press <ENTER> for none:
> 192.168.3.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT2 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT2 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Use the configuration below for the OPT2 interface

Leave the OPT3 interface without an IP as it is going to have the span port with traffic that Security Onion will be monitoring.

Use the configuration for the OPT4 interface

```
Enter the number of the interface you wish to configure: 6

Enter the new OPT4 IPv4 address.  Press <ENTER> for none:
> 192.168.4.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new OPT4 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

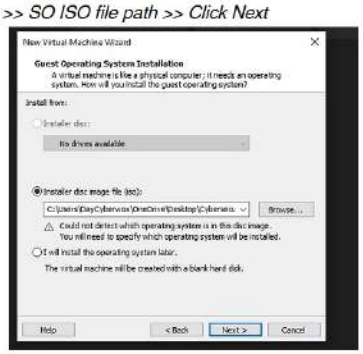
This ends the configuration of the pfsense VM. The rest of the configuration will be done via the kali machine through the WebConfigurator.

Configuring Security Onion

This will be the all-in-one IDS, Security Monitoring, and Log Management solution.

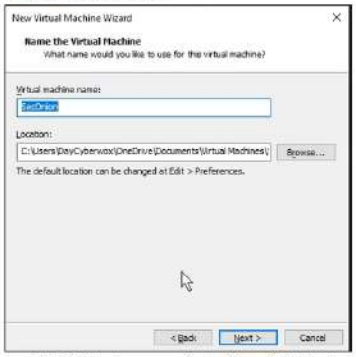
Download the Security Onion ISO file from here

Select Typical installation >> Click Next
Installer disc image file >> SO ISO file path >> Click Next

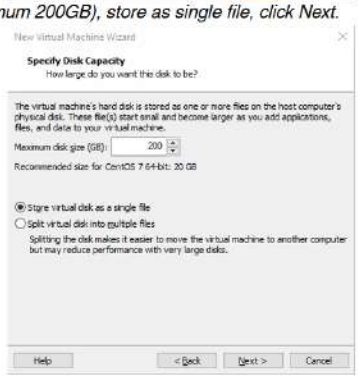


Choose Linux, CentOS 7 64-Bit and click Next.

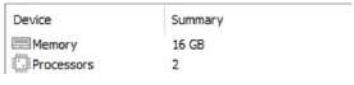
Specify virtual machine name and click Next.

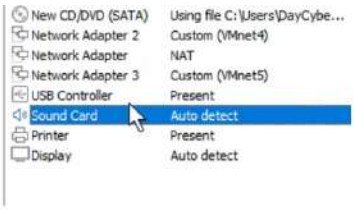


Specify disk size (minimum 200GB), store as single file, click Next.



Click "Customize Hardware" and do the following:
~ Change memory to 4-32GB
~ Add two Network Adapters and assign them Vmnet 4 & Vmnet 5 respectively





Click "Finish"

Power the virtual machine and click Enter when prompted:

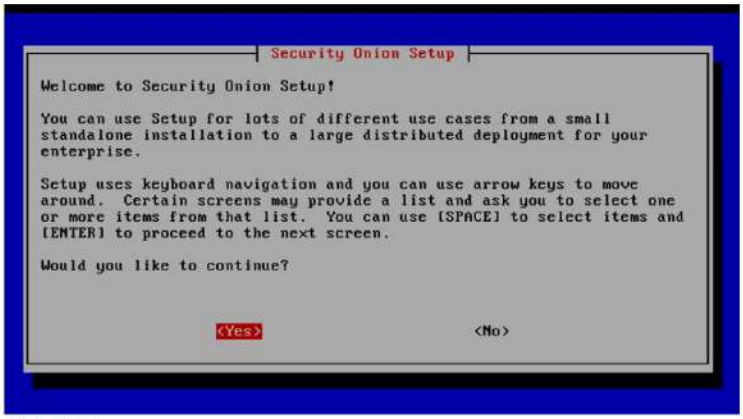
After the initial stages of loading, type "yes" when prompted

~ Set a username & password:

After Security Onion Reboots, proceed with the following:

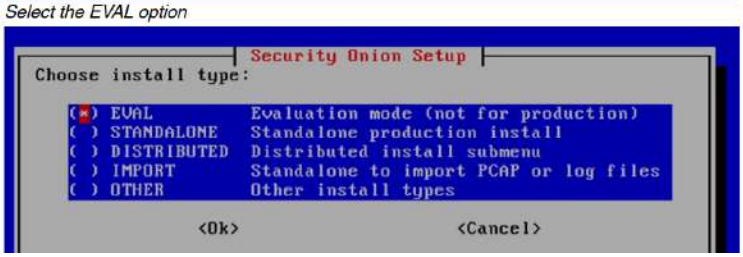
Enter the username & password

Select "Yes"

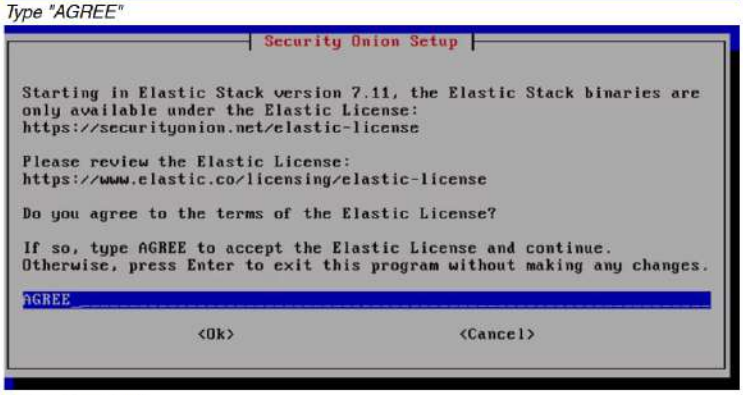


Click Enter

Select the EVAL option



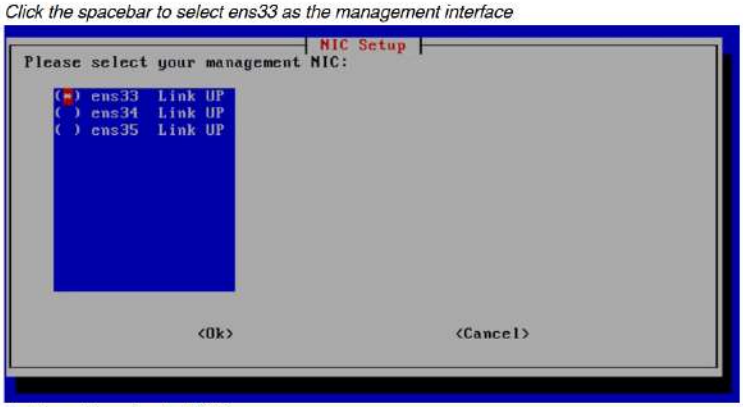
Type "AGREE"



Select "Standard"

Set a hostname, and a short description

Click the spacebar to select ens33 as the management interface



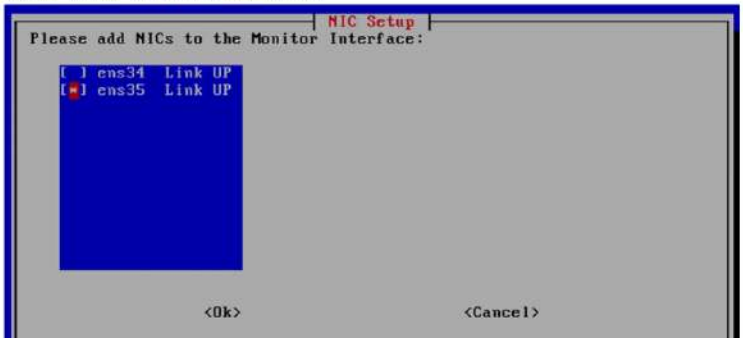
Set the addressing to DHCP:

Select "YES" at the next prompt

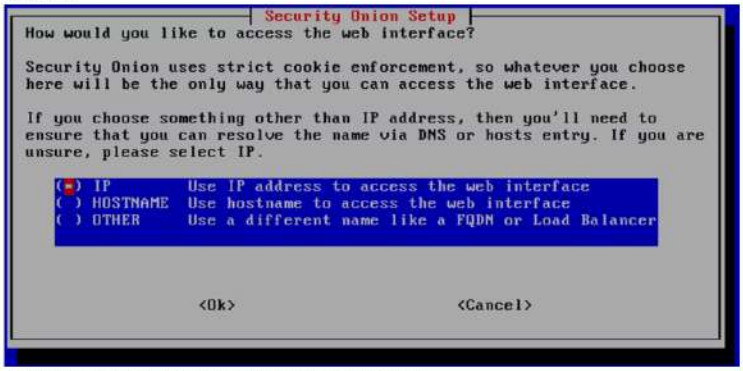
Select "OK" at the next prompt

Select "Direct" for the next prompt

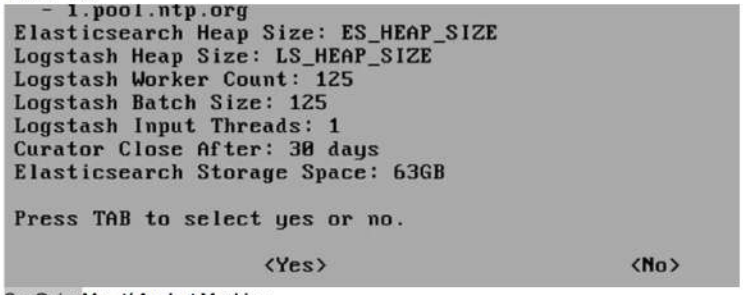
Select "ens35" as the Monitor Interface



Select "Automatic" for the OS patch schedule"
Accept the default home network ip
Accept all the defaults
Enter an email address and password for the admin account
Select "IP"



Select "Yes" for the NTP server & accept the defaults
Take note of your final settings before proceeding! If possible take a screenshot.
Most important detail is the IP address for web access.
Select "Yes"



SecOnion**Mgmt/ Analyst Machine**

After installing Security Onion, having access to the web interface will be done from an external Ubuntu Desktop simulating a SOC/Security Analyst accessing a SIEM or any other tool from their device.

In order to this, you'll first have to configure an Ubuntu Desktop. This is a very easy process and I'll not be covering it in this write-up but it is covered in the video. Be sure to use all the default settings for the Ubuntu Desktop configuration.

Download Ubuntu Desktop

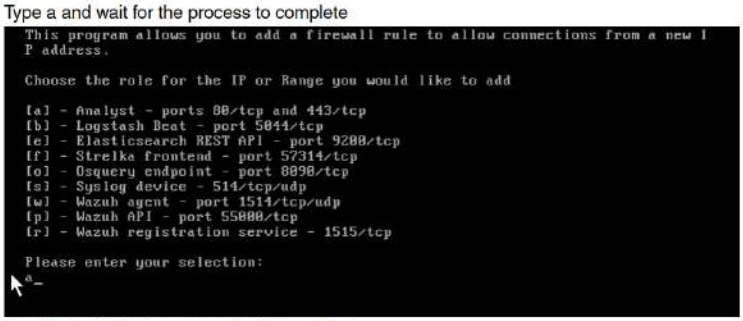
Install Ubuntu Desktop

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

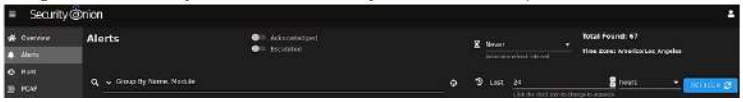
Head back to your Security Onion instance and run the following command

```
sudo so-allow
```

Enter your password
Type a and wait for the process to complete



Type in the IP Address from the Ubuntu Desktop
This will create a firewall rule on Security Onion that will allow you web access from your Ubuntu Desktop
Navigate to the Security Onion IP Address on your Ubuntu Desktop:



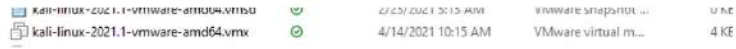
This ends the configuration of the Security Onion VM.

Configuring Kali Linux

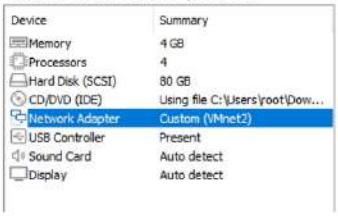
Kali Linux will be used as an attack machine to propagate different forms of offensive actions against the Domain Controller and the other machines attached to it.

Download the Kali Linux ISO from here

Since you're downloading the VM file, all you'll need to do is to click on the .vmx file from the Kali Folder you downloaded and it will automatically load up the default Kali image in VMware.



*Before powering on the Kali, change the Network Adapter to **Vmnet2** and its Memory to **4GB,** then power it on and use default credentials as specified.*



After powering on, use this command to change the default password to a more secure one of your choice:

```
passwd
```

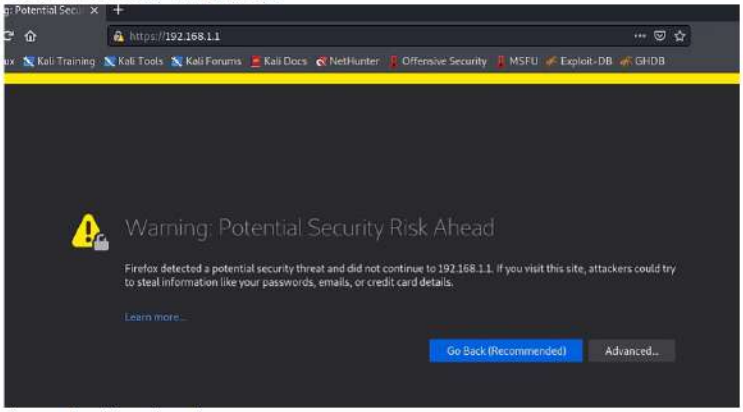
The Kali machine is ready for use.

---

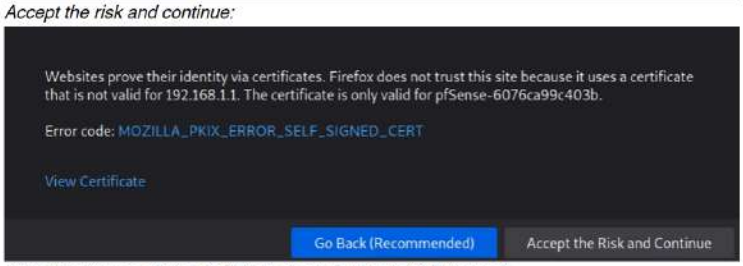
pfsense Interfaces and Rules

Now that the Kali machine is set up, the pfsens WebConfigurator can be accessed in order to make some changes to the pfsense interface and firewall rules.

*Navigate to the web browser and search for **192.168.1.1***
Select "Advanced..." at this screen:

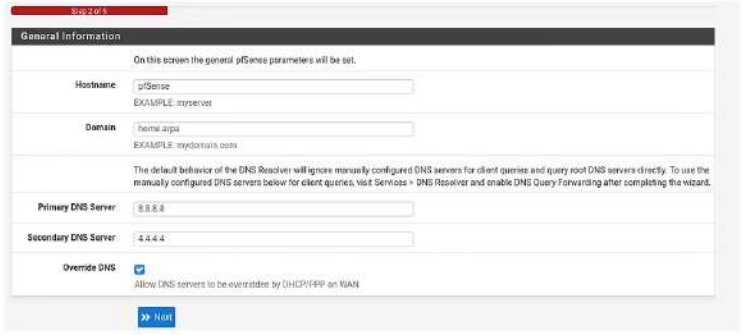


Accept the risk and continue:



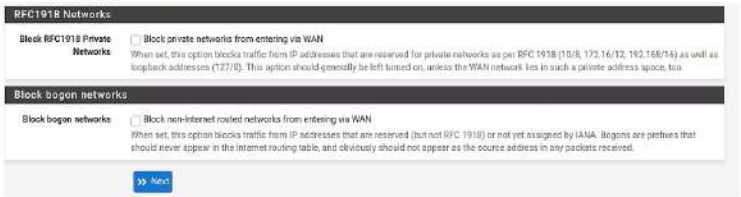
*Sign in to pfsense using default credentials **"admin" & "pfsense"***

*You'll be greeted with a **"Wizard/pfSense Setup/"** page.*
*Click Next till you get to Step **2 of 9**.*
*Add **8.8.8.8** as your Primary DNS Server*
*Add **4.4.4.4** as your Secondary DNS Server*
Click Next.



*At Step **3 of 9**, Choose your Timezone*

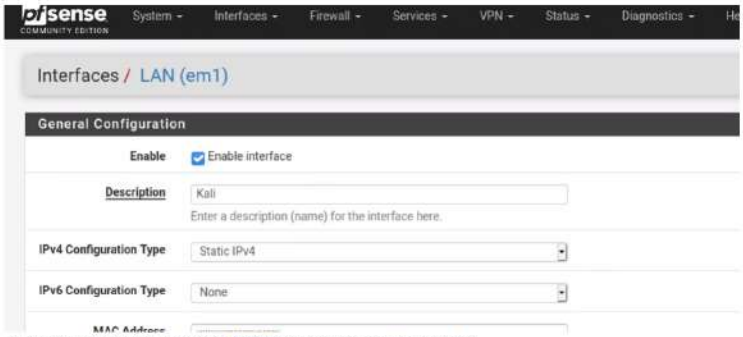
Click Next.
*At Step **4 of 9**, untick the last two options*
*At Step **5 of 9**, Click Next*



*At Step **6 of 9,** Set a new Admin Password*
Click Next.
*At Step **7 of 9**, Click **Reload***
Finish

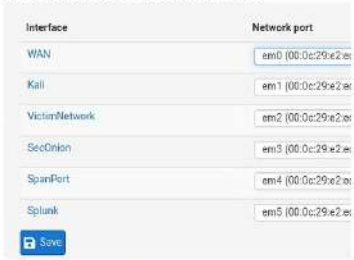
At this point, pfsense Wizard is complete and changes can now be made to the Interfaces.

*Click on **Interfaces**.*
*Select **LAN***
*For "Description", Change **LAN** to **Kali** as this is the Kali interface*
*Scroll all the way down and Click **Save***



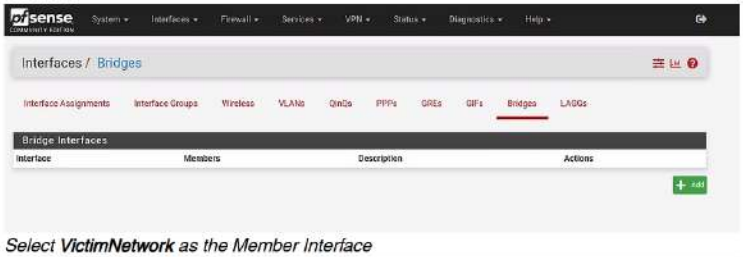
If you get this error, use this Article to troubleshoot and fix it

Then do this for the rest of the Interfaces as shown below



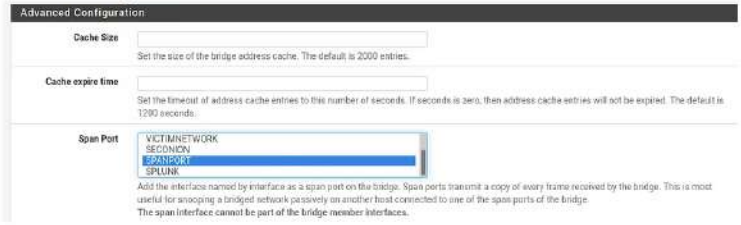
*For **OPT3** Be sure to Enable Interface as shown below*

*Back at **Interfaces Assignment** select **Bridges***
*Click **Add***

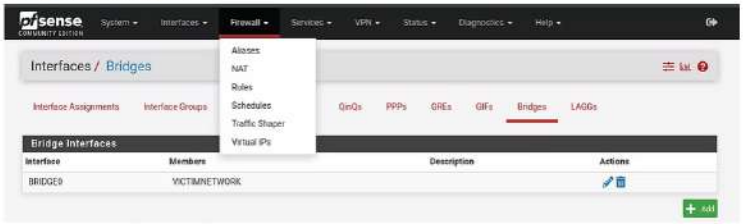


*Select **VictimNetwork** as the Member Interface*

*Then select **Display Advanced***
*Under **Advanced Configuration** for **Span Port**, select **"SPANPORT"***
*Scroll all the way down and Click **Save***



Click Firewall >> Rules



*Select the **Add** button with the arrow pointed downward*
*~ Under "edit Firewall Rule" for Protocol select **ANY***
*~ Scroll all the way down and **SAVE***

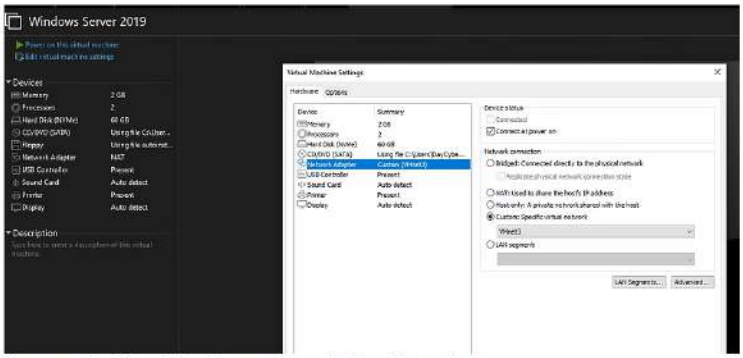
This is the majority of the firewall configuration needed for pfsense.

Configuring Windows Server as a Domain Controller

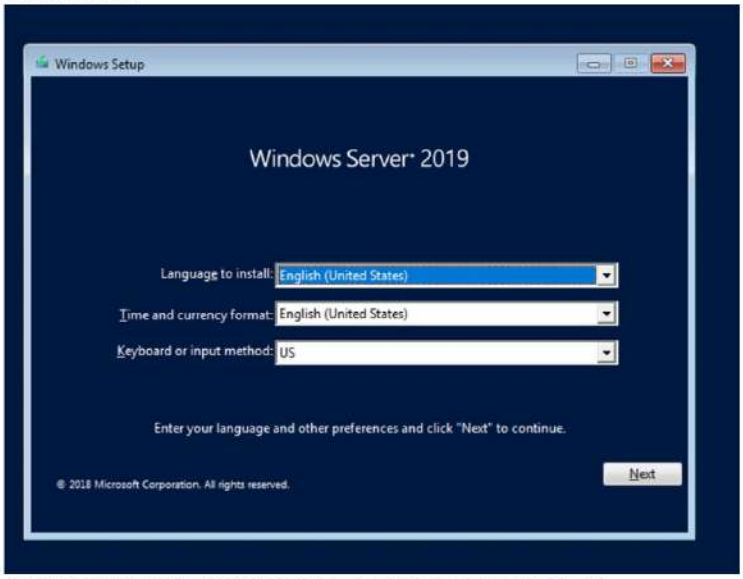
The goal of this portion of the lab is to set up an Active Directory domain with a Windows 2019 Server as the Domain Controller and 2 Windows 10 machines. This portion of the lab is very easy to set up and I'll be using The Cyber Mentor's youtube guide for an Active Directory Hacking Lab.

Download the Windows 2019 Server Evaluation Copy
Download the Windows 10 Evaluation Copy

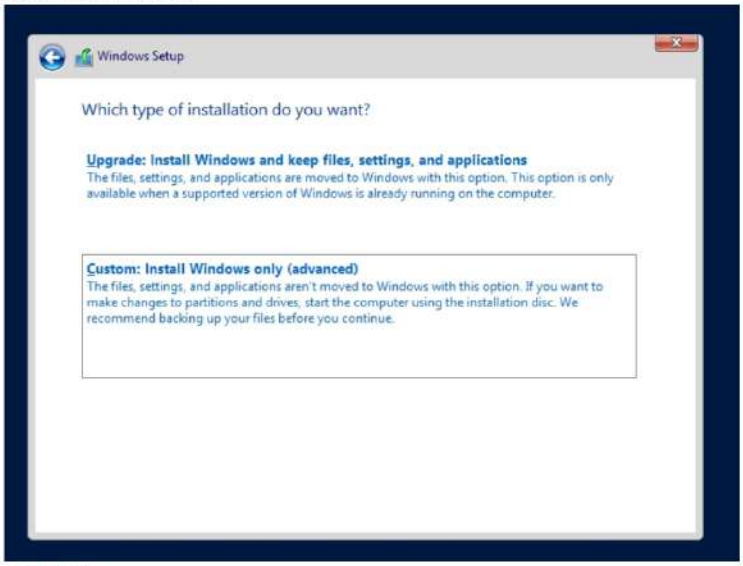
~ Important Details for Windows Server Installation
(Please read the below before installing the Windows Server on VMware)
** Install in VMware as usual with defaults*
** Do not worry about a product key, simply click **Next***
** At the end of the installation, be sure to change the Network Adapter to **Vmnet3***
**** Make sure to UNCHECK** "Power on this virtual machine after creation".*
** After the VM has been installed, click "Edit virtual machine settings" and remove the Floppy drive.*



Power on the Virtual Machine and immediately click any key.
*Click **Next***
*Click **Install Now***

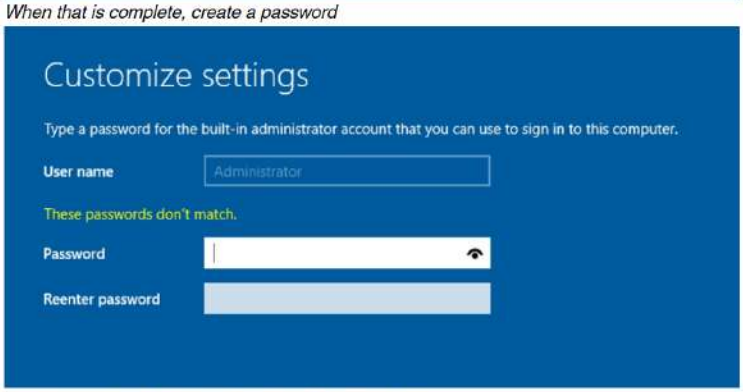


*Select the **Windows Server 2019 standard Evaluation (Desktop Experience)***
Accept the License Terms
*Click **Next***
*Select the **Custom Install***

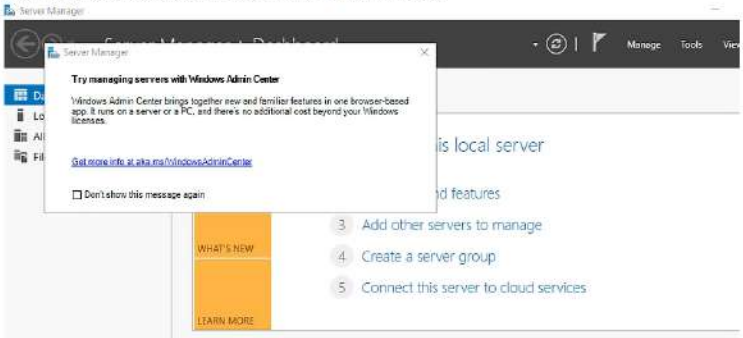


*Click **New***
*Click **Apply***
*Click **OK***
*Click **Next***
You should have this screen now

When that is complete, create a password

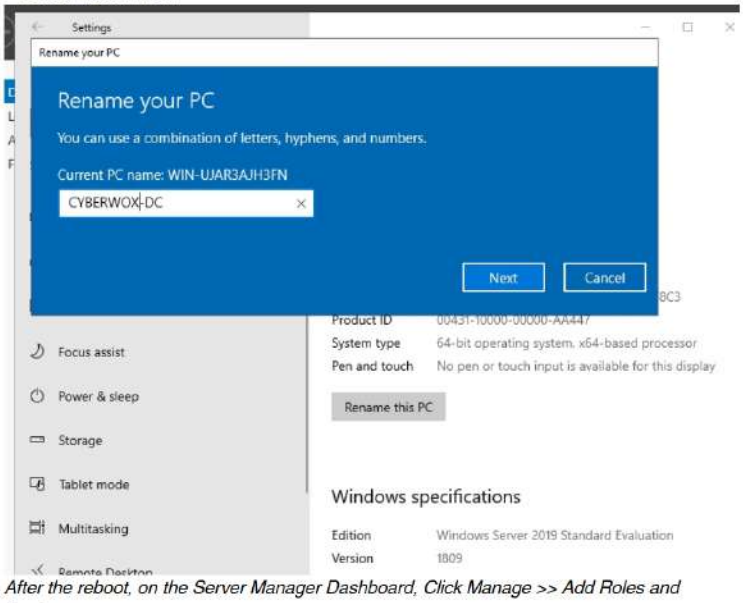


After the installation, you should end up with this screen

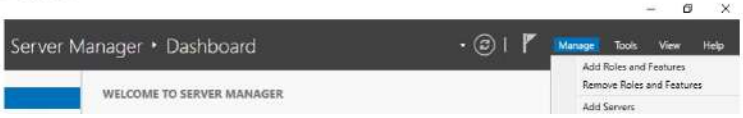


Rename the Domain Controller

~ Navigate to Settings in the search bar
~ Search for settings in the search bar
~ Search for "pc name" in the settings search
~ Select Rename PC and rename the PC your choice name
~ Select Restart Now



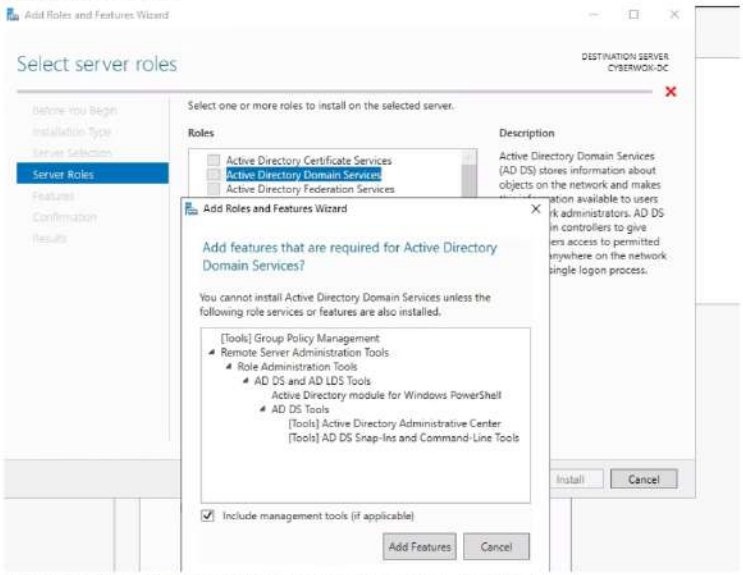
After the reboot, on the Server Manager Dashboard, Click Manage >> Add Roles and Features



*Keep clicking **Next** till you get to the **Server Roles** menu*

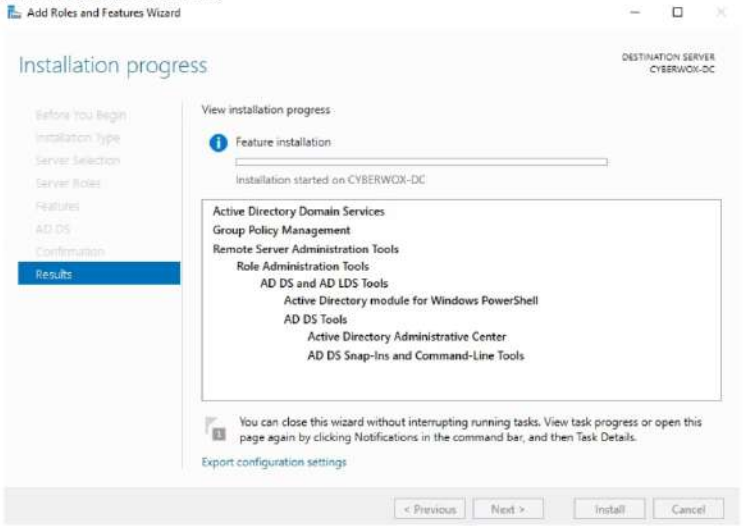
*Select **Active Directory Domain Services***

*Select "**Add Features**"*



*Click on **Next** till you get to the Confirmation menu, then click **Install***

*After the Install, Click **Close***



Click on the flag with the yellow caution triangle

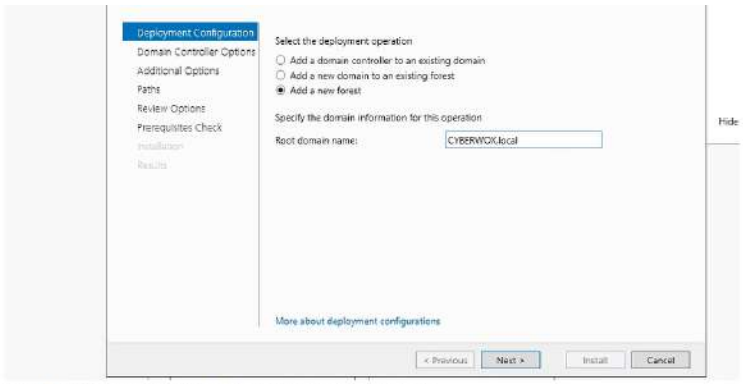
** Select "**Promote this server to a domain controller**"*

** Select **Add a new forest***

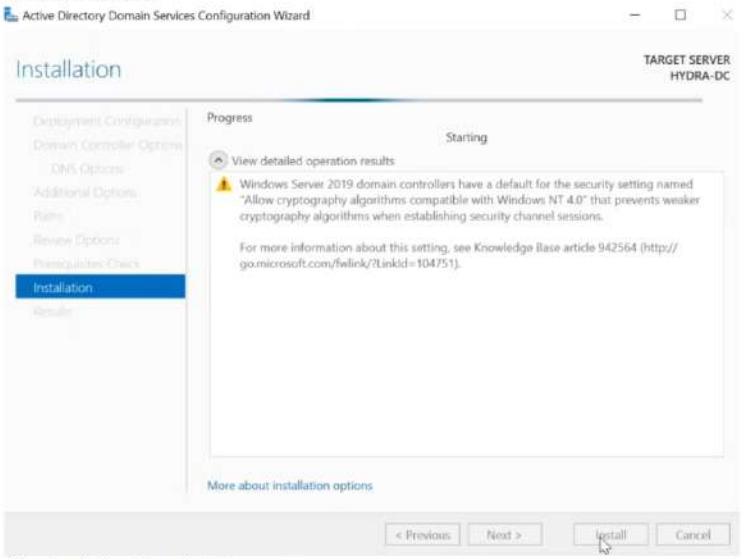
** Specify a domain name*

** Click **Next***

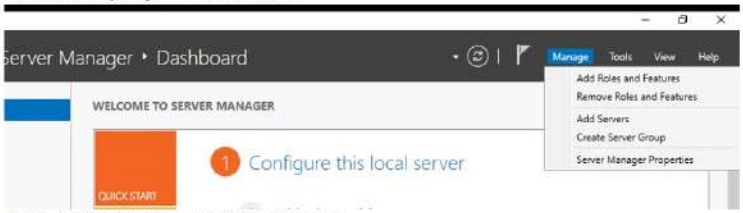
**** Set a Password***



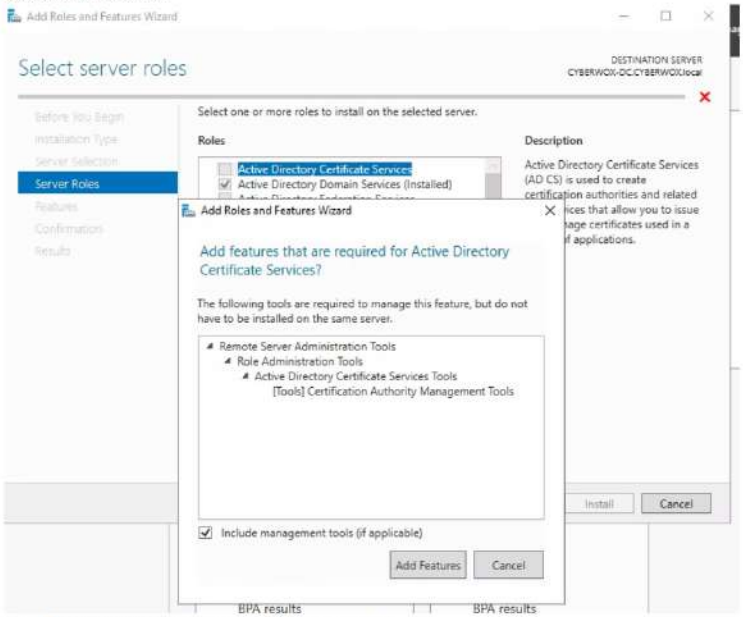
*Click **Next** till you get to the **Prerequisites Check** Menu*
*Click **Install***
Wait for the Reboot



After the Reboot, Log back in
Select Manage >> Add Roles & Features again on the Server Manager
*Click **Next** till you get to **Server Roles***

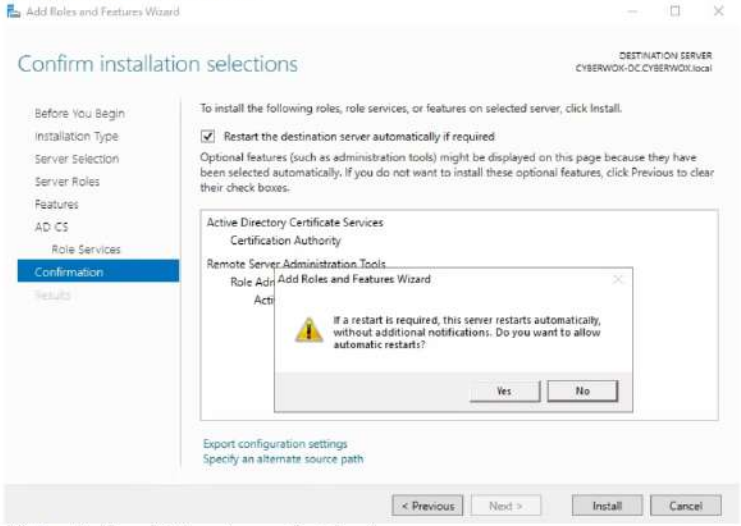


*Select **Active Directory Certificate Services***
*Select **Add Features***

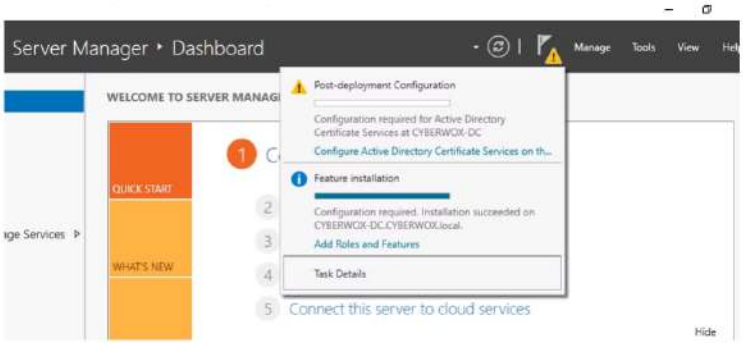


*Click **Next** till you get to the **"Confirmation"** menu*
*Check **"Restart the destination server automatically if required"***

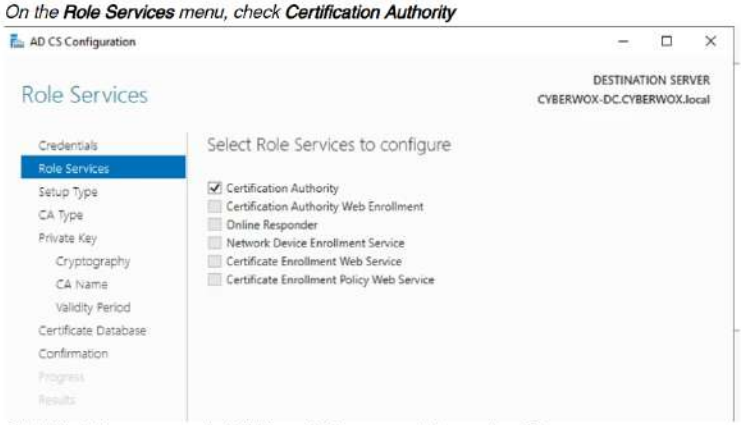
*Select **Yes***
*Select **Install***
*After the Installation, Click **Close***



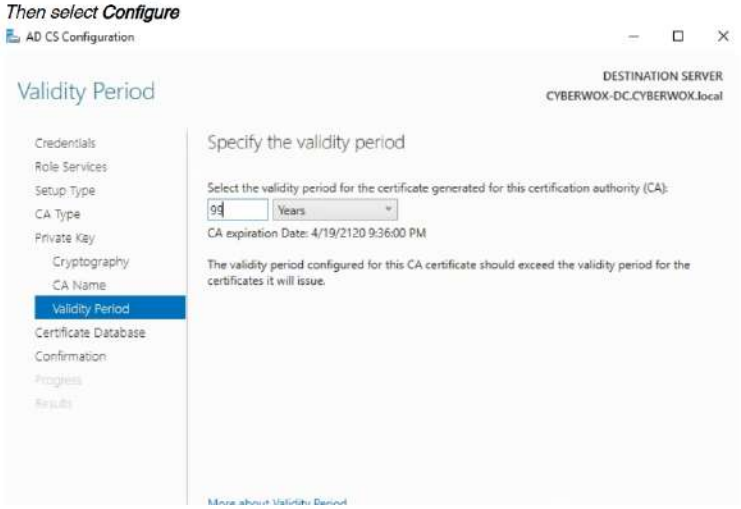
Click on the flag with the yellow caution triangle
*Select "**Configure Active Directory Certificate Services on the destination server**"*



*Click **Next** on **Credentials***
*On the **Role Services** menu, check **Certification Authority***

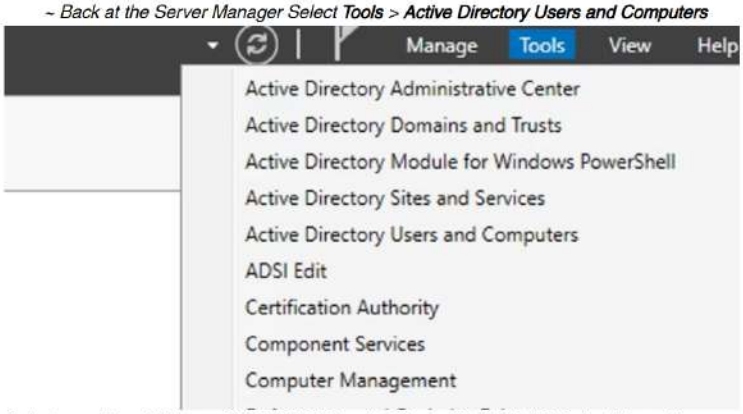


*Click **Next** till you get to the **Validity period** menu and change it to **99** years*
*Click **Next** till you get to the **Confirmation** menu*
*Then select **Configure***



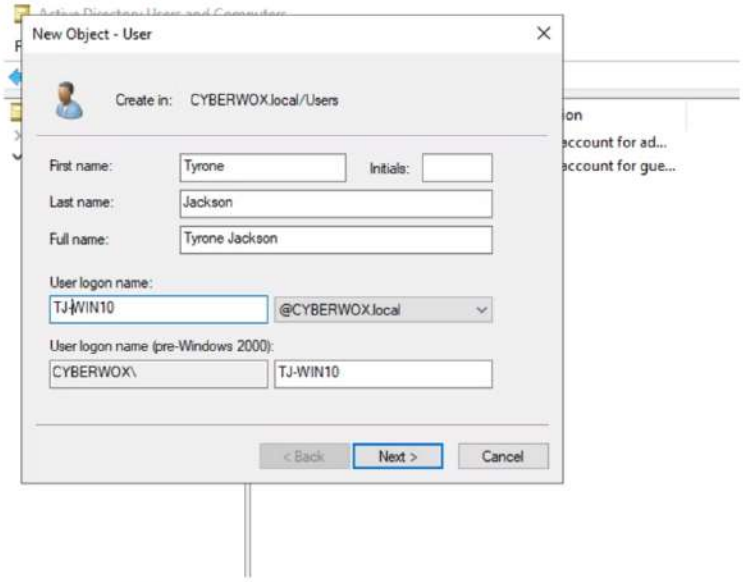
Manually restart the server in order for all the settings to take effect.
Now add some Users:

*~ Back at the Server Manager Select **Tools** > **Active Directory Users and Computers***

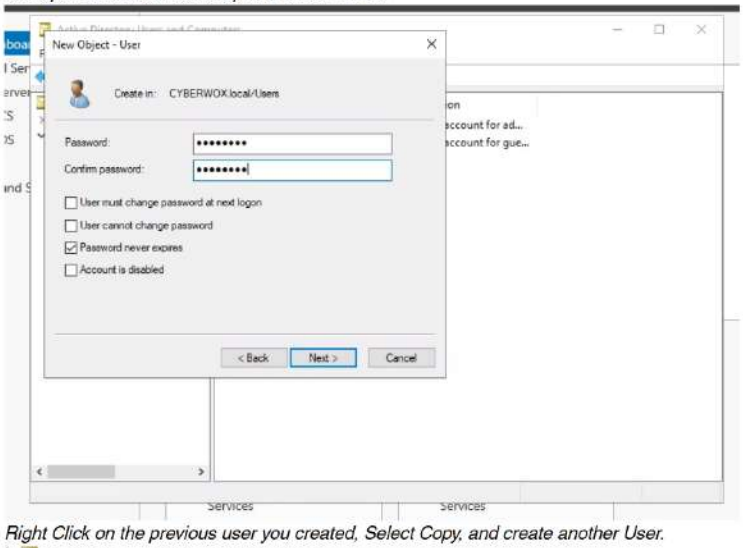


*Select your **Domain Name (CYBERWOX.local)** > **Users**, Right Click & Select **New** > **User***

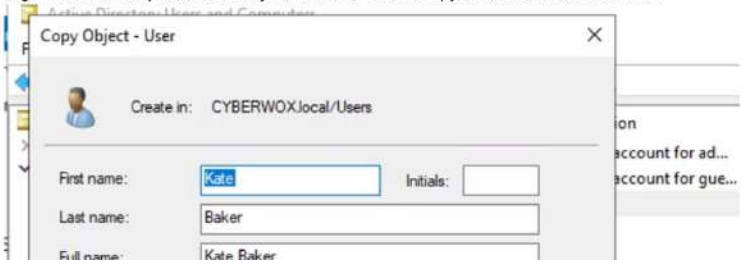
~ Enter a First, Last & User logon name for the user (Disregard the "WIN10" and just set a preferred logon name).

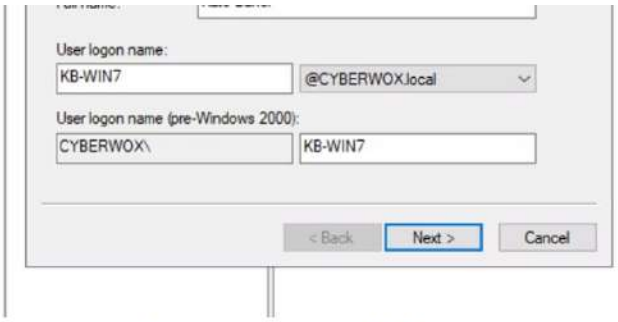


*Set a password that never expires. Select **Finish**.*



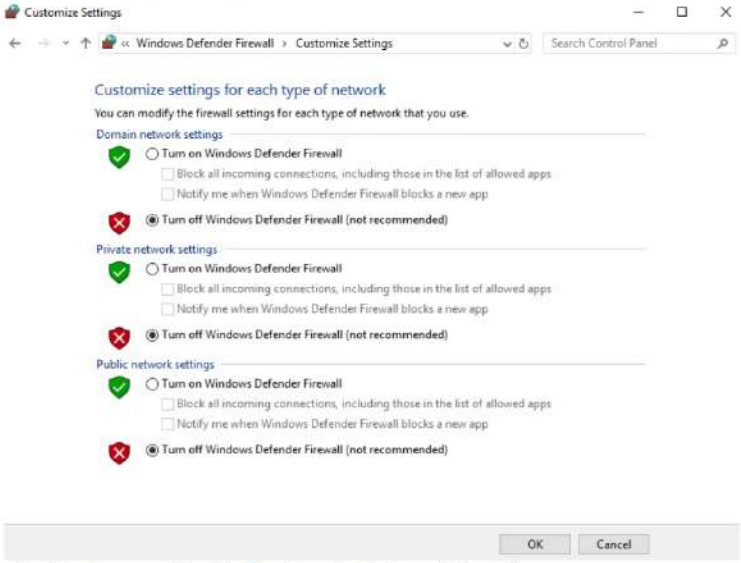
Right Click on the previous user you created, Select Copy, and create another User.



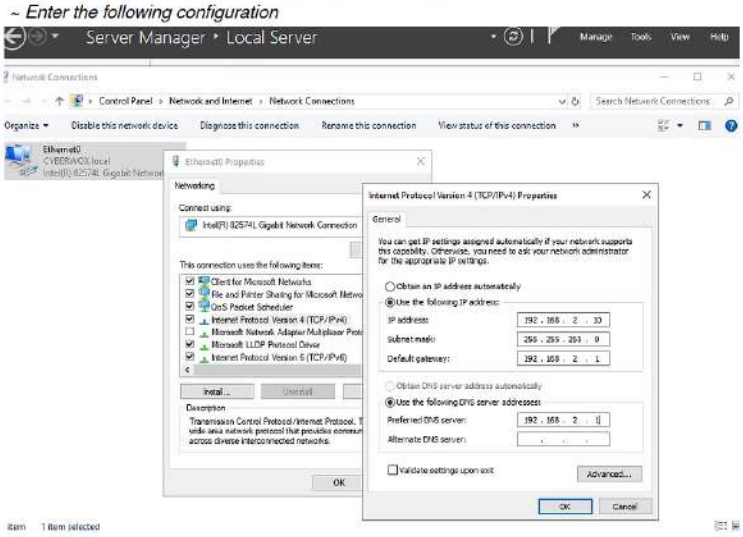


*Disregard the **"WIN7"** and set a preferred logon name.*
After this, add a password that never expires.

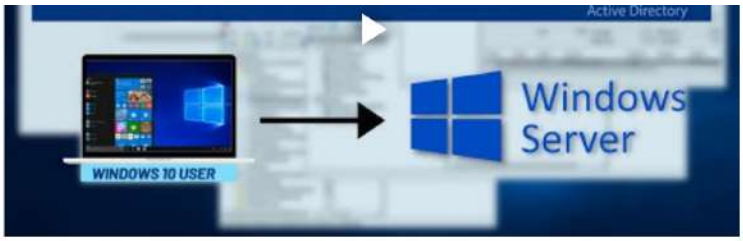
*Search for **"Windows Defender Firewall" > Turn Windows Defender Firewall on or off.***
Turn off the firewall for all Networks



Now Use pfsense as the default gateway for the Domain Controller
*~ Navigate to **Control Panel > Network and Internet > Network Connections***
~ Enter the following configuration



This is the end of the Domain Controller configuration. If you're looking to do a more comprehensive configuration, you should check out [The Cyber Mentor's Video] and follow it in accordance with this lab.



Configuring Windows 10 Desktop & Adding a User to the AD Domain

The goal of this portion of the lab is to add 2 Windows 10 desktops to the Domain and complete the active directory lab. This portion of the lab is very easy to set up and I'll be using The Cyber Mentor's youtube guide for an Active Directory Hacking Lab.

*Note that having 2 desktops is not a hard requirement for this lab as **ONE** desktop is sufficient.*

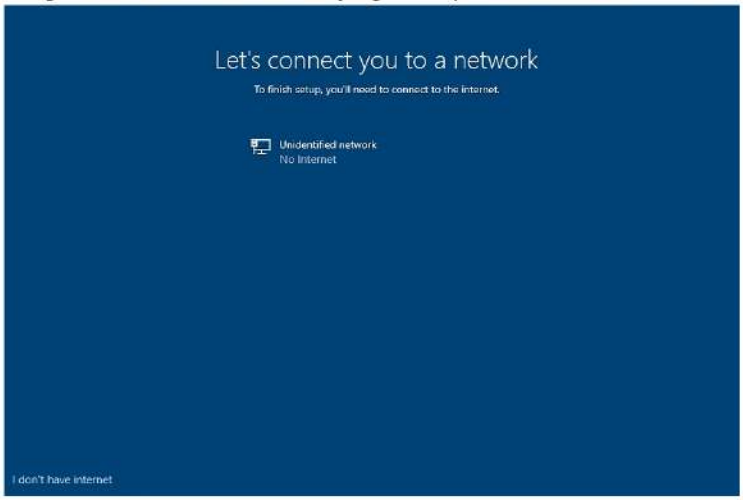
Download Windows 10 Evaluation Copy

~ Important Details for Windows Server Installation
(Please read the below before installing the Windows Desktops)
** Install in VMware as usual with defaults*
** Do not worry about a product key, simply click **Next***
**** 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 the VM has been installed, click "Edit virtual machine settings" and remove the Floppy drive.*

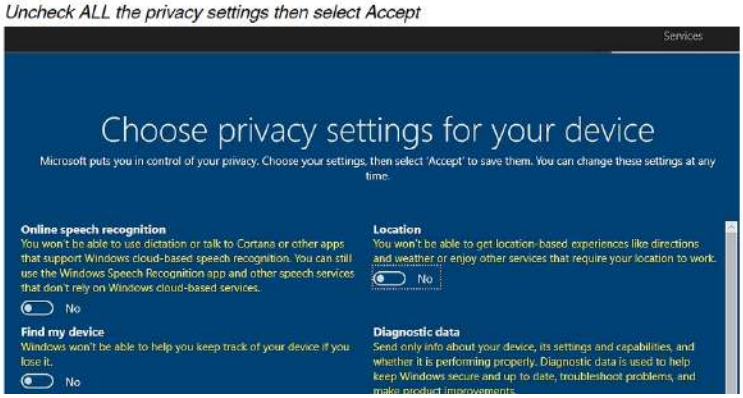
Repeat this process, but this time for the second user.

Use the same configuration steps as the Domain controller:
#Install
#Accept license terms
#Use Custom Install
#Select New > Apply > OK > Next

Configure windows 10 as usual and when you get to this point select "I don't have internet"

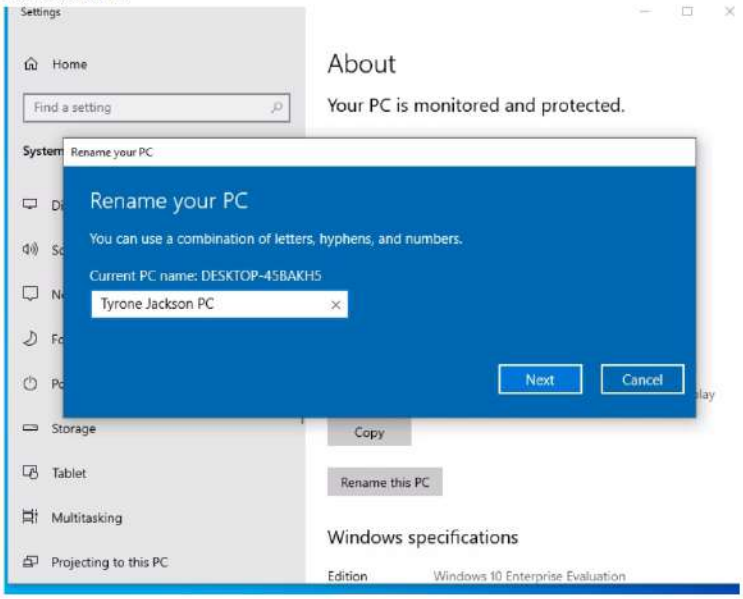


Continue with limited setup
Set the first user and the password (Remember from the DC configuration)
Set the security answers
Uncheck ALL the privacy settings then select Accept



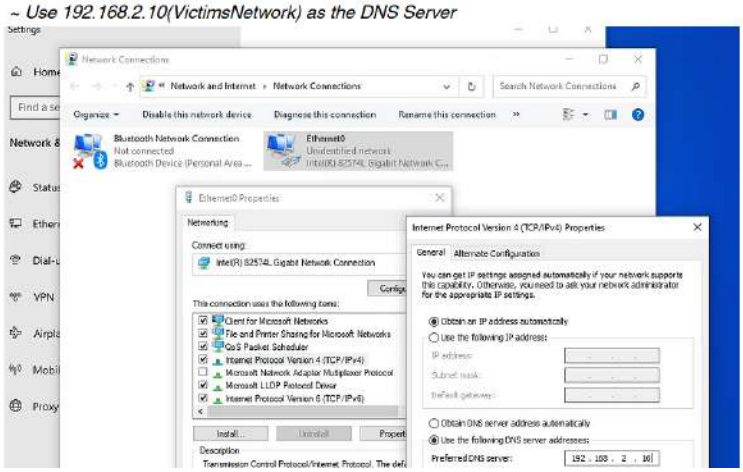
Choose "Not Now" for Cortana
While you wait set up the second desktop with the second user account credentials but the same configurations.

Search "pc name" and change the PC Name according to the designated users
Restart the PC

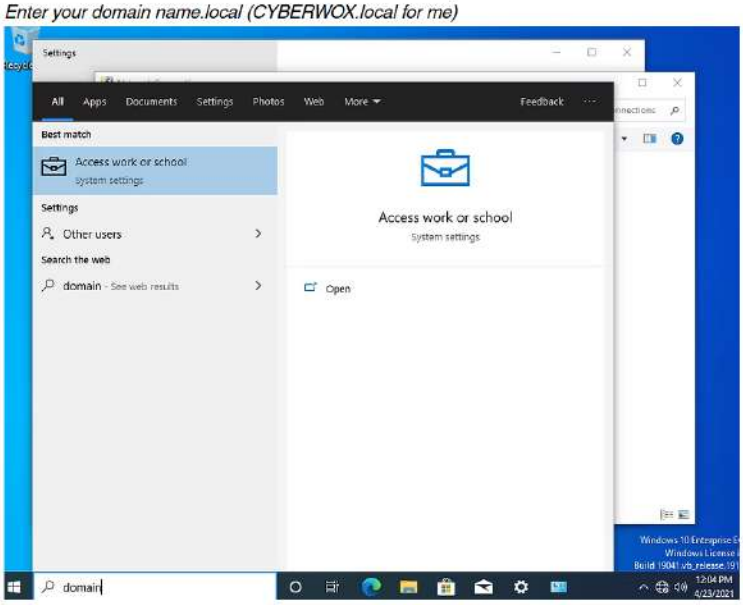


JOINING THE PCs TO THE DOMAIN

~ Navigate to Network Adapter settings
~ Right-click on Ethernet0 and select properties
~ Select IPV4
~ Add an IP Address(192.168.2.21) & Use 192.168.2.1 as the default gateway
~ Use 192.168.2.10(VictimsNetwork) as the DNS Server



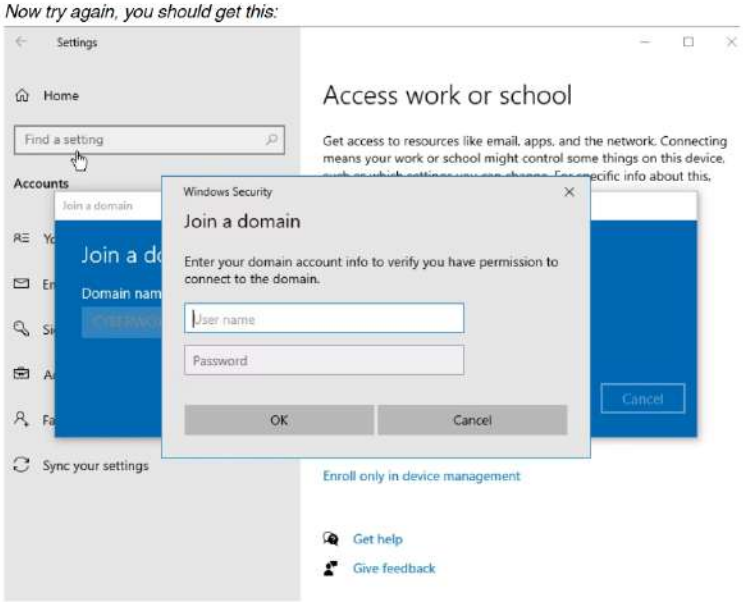
Search "domain" and select Access work or school
Select Connect > Join this device to local Active Directory Domain
Enter your domain name.local (CYBERWOX.local for me)



YOU WILL GET AN ERROR. THIS IS EXPECTED, DON'T PANIC LOL.
Head over to pfsense:

At Services > DHCP Server > VICTIMSNETWORK> DNS Server ---- This should be the IP of your domain controller(192.168.2.10)
At Services > DHCP Server> VICTIMSNETWORK > Other Options > Domain Name ----- This should be the domain name (CYBERWOX.local)

Now try again, you should get this:



Enter the Username: Administrator and the password of your DC
Select Skip
Restart

Repeat this process for the second machine.

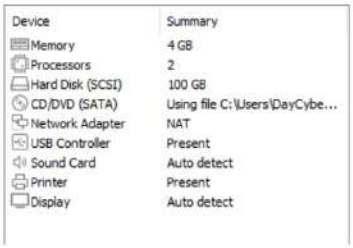
Installing Splunk on a Ubuntu Server

Splunk is one of the most widely used SIEMs in the Cybersecurity industry. Splunk essentially aggregates logs and datasets from various data sources and correlates all that information for easy searching, parsing & indexing.

If you're looking to learn more about Splunk, check out our resources on Splunk:
Splunk Fundamentals 1
Splunk Core Certified User Certification

The first part of this process will be installing a **Ubuntu Server** for our Splunk instance

Download Ubuntu Server
After downloading the Ubuntu server, create a new virtual machine with the following settings then start the virtual machine:



Before powering on the machine, enter the *Virtual Machine Settings* and remove the CD/DVD drive with the file named *autoinst.iso*, as well as the Floppy drive with the file *autoinst.flp*

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

Installing an OpenSSH server is based on your preference but I recommend installing it. You can also add any services you want but it's not necessary for this lab.

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

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

```
To see these additional updates run: apt list --upgradable


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

daycyberwox@splunk:~$
```

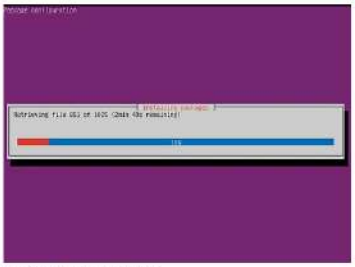
For the Splunk server, you have one of two options
- Accessing it with the AnalystVM using SSH
- Installing a GUI (Ubuntu Desktop) on the Ubuntu Server

I'll be installing a GUI on the Ubuntu Server for this lab using the following steps:
- Install tasksel

```
sudo apt install tasksel
```

- Install the ubuntu desktop GUI but note that there are a variety of options to choose from

```
sudo  tasksel install ubuntu-desktop
```



- Reboot the VM with the "reboot" command

```
reboot
```

After rebooting, you should have your GUI.

Installing Splunk

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

Open the terminal and navigate to the downloads directory

```
daycyberwox@splunk:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
daycyberwox@splunk:~$ cd Downloads
daycyberwox@splunk:~/Downloads$ ls
splunk-8.2.0-e053ef3c985f-Linux-x86_64.tgz
daycyberwox@splunk:~/Downloads$
```

Untar the file

```
daycyberwox@splunk:~/Downloads$ ls
splunk-8.2.0-e053ef3c985f-Linux-x86_64.tgz
daycyberwox@splunk:~/Downloads$ tar xvzf splunk-8.2.0-e053ef3c985f-Linux-x86_64.
tgz
```

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

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

Installing Universal Forwarder on Windows Server

In order to log the activities on endpoints, Splunk uses a mechanism called the universal forwarder. The universal forward can be installed on windows, *nix & mac agents to forward logs to your Splunk instance.

Add the **Vmnet6 network** adapters to the Splunk adapter

Set up "Receiving" on your Splunk server
Navigate to Settings >> Forwarding and Receiving >> New Receiving Port

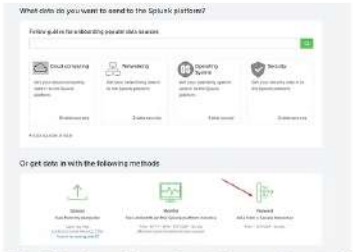
Enter port **9997** and save

Navigate to Settings >> Indexes >> New index
Name the index "wineventlog" and save

On your Windows Server, Download the Universal Forwarder
Now install the forwarder:
Accept the License Agreement & click Next

Create a preferred username and password
Enter the IP Address of your Splunk server and the default ports as prompted (8089 & 9997)
Install

Navigate back to your Splunk Instance >> Settings >> Add Data
Select "Forward"



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

Select Local Events Logs and choose your desired event logs >> Next

Select "wineventlog" as the index >> Review >> Submit

This brings us to the end of this homelab. This was fun and exciting to work on and I hope you found value in this process.

At this point, this lab is yours to dominate. You have all the knowledge and tools you need to do a lot of labbing, research, and anything you want to do. Work on detection rules, SIEM content, rule tuning, and even attack scenarios in order to build skills from various angles.

I'll be adding to this lab from time to time to keep it as detailed and updated as possible.

For troubleshooting/help with this lab, please join our discord server and I'll be glad to help!

Lab Projects

Comments