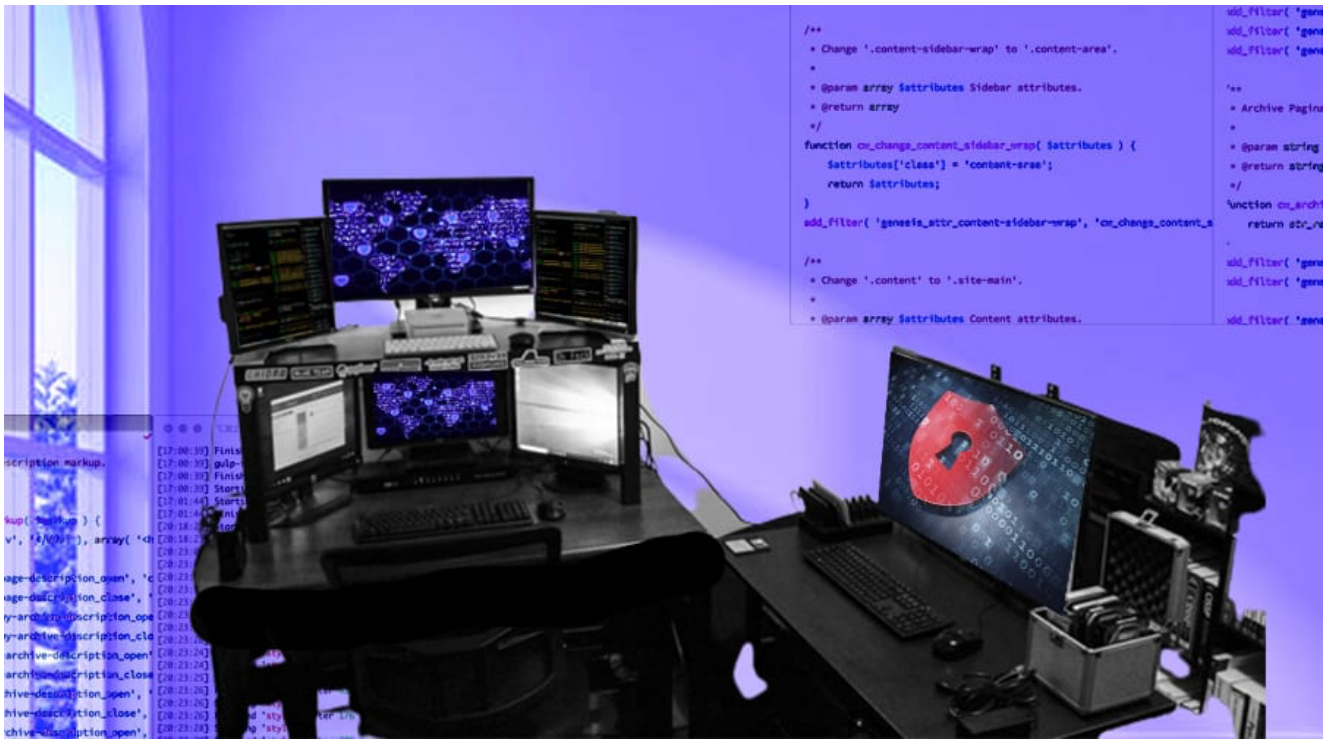
User Guide

Manual on creating a

CYBERSECURITY

HOME LAB



Ebenezer Adekeye | Info-Tech Project | Dr. Shuting Park | Deliverable Guidelines:

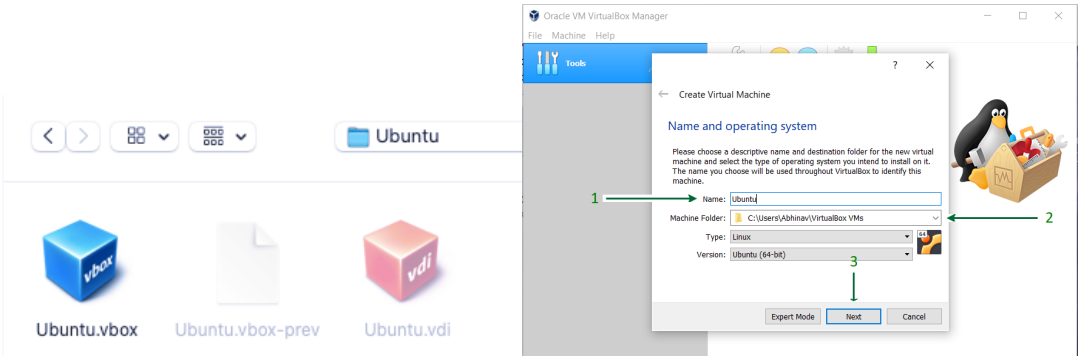
Resource: https://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/

Purpose: This Cybersecurity Home Lab walks through the process of configuring, optimizing, and securing an IT infrastructure. Although this will be at a relatively small scale, you can learn and apply the knowledge gained from this project to a real-world enterprise infrastructure. Throughout my project, I created everything internally and for anyone to create a Home Lab themselves, they will need to take the same similar steps to get started:

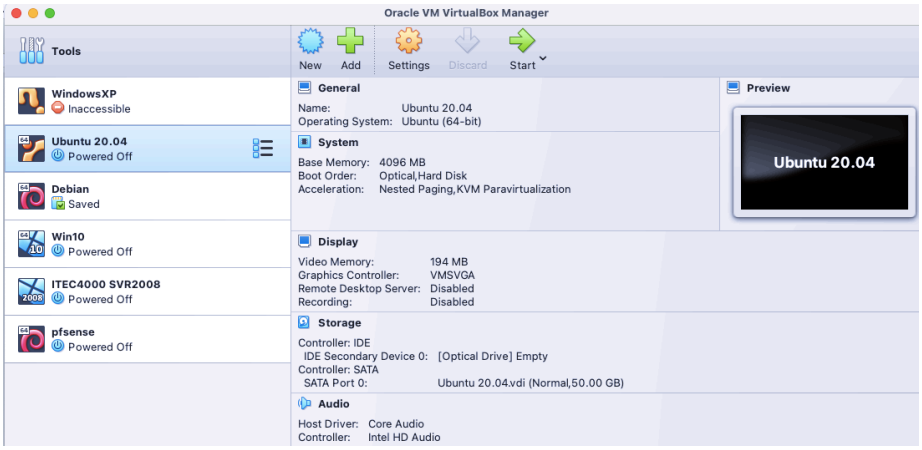
Building Host PC

- Install VirtualBox or VMware Workstation as a hypervisor. Either option is effective, but I used VirtualBox. Once it's installed, you can import your operating system's iso file.

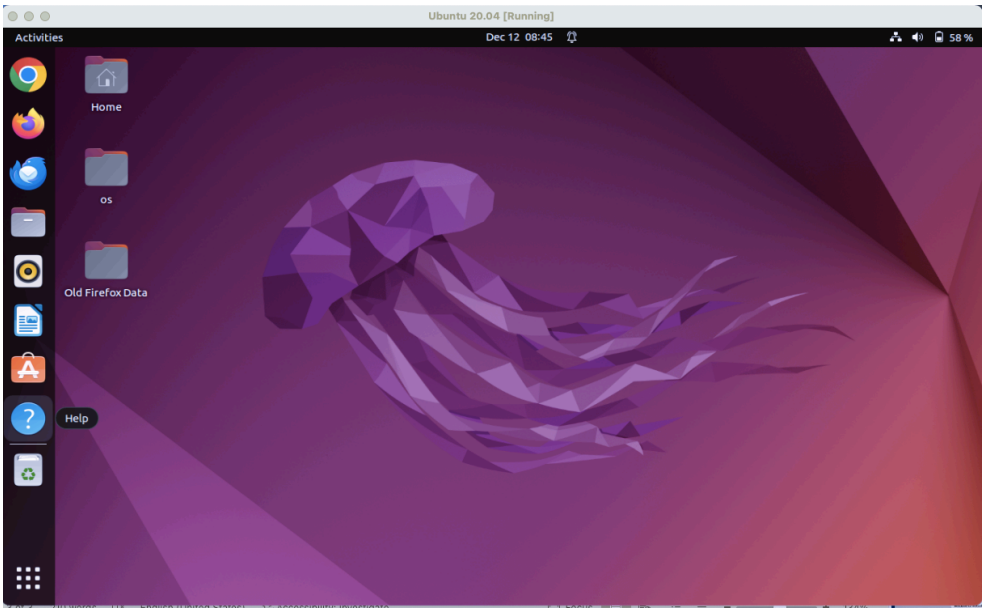
- Ubuntu: the Linux machine that I used that can be added to the network for exploitation, detection, or monitoring purposes.
    - Install an Ubuntu *.iso, .vbox, or .vdi* file from *Ubuntu's* main website and import it into the VBox import settings.



    - Once created, you will see the new OS available in Virtual Machine.

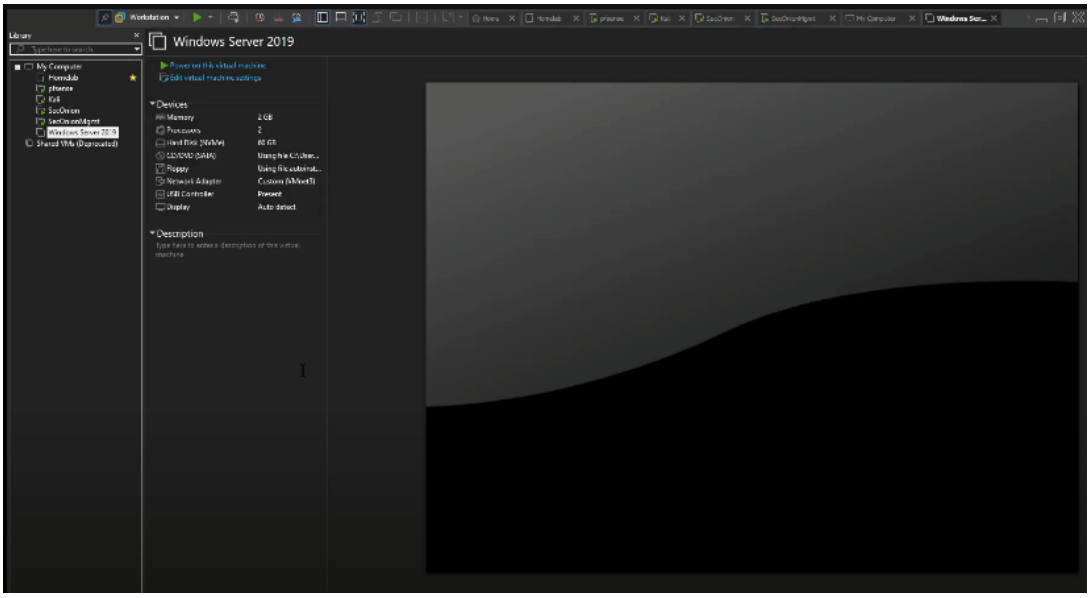


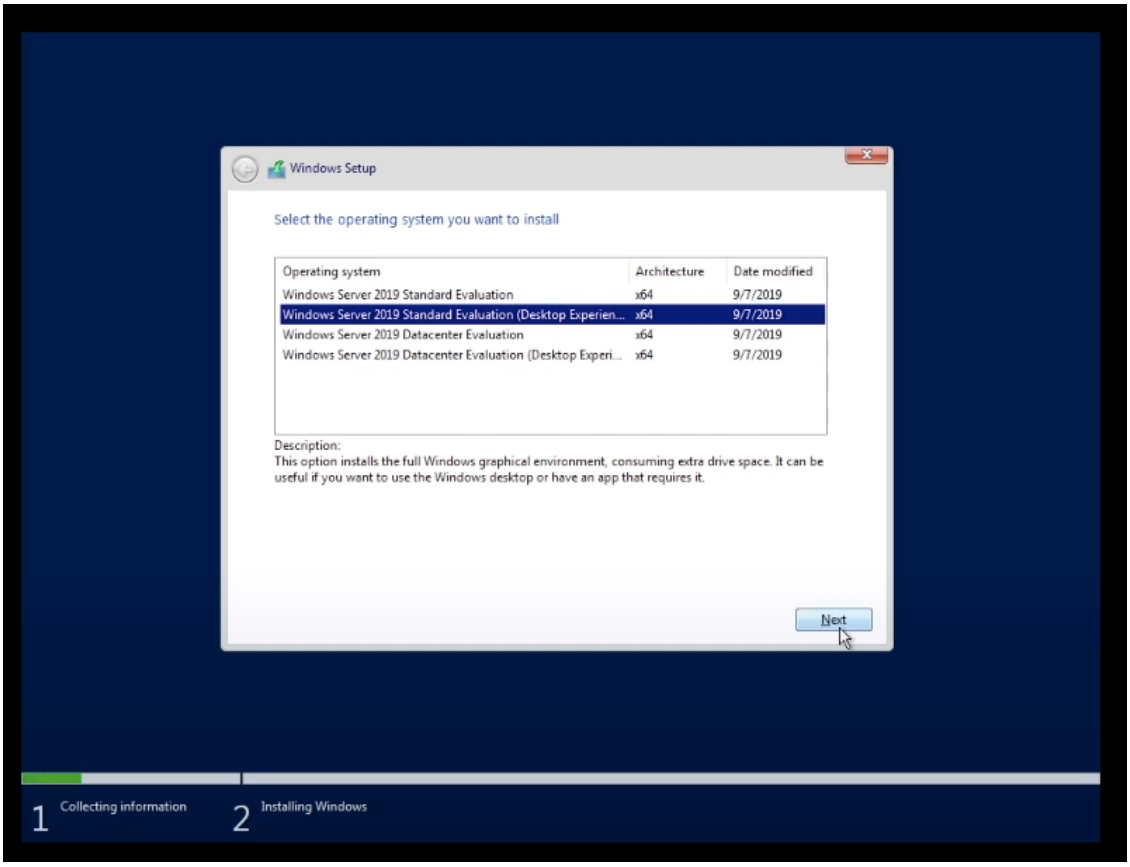
- When you *start* the machine, you can now access the machine and you can start exploring around with the Linux virtual machine.

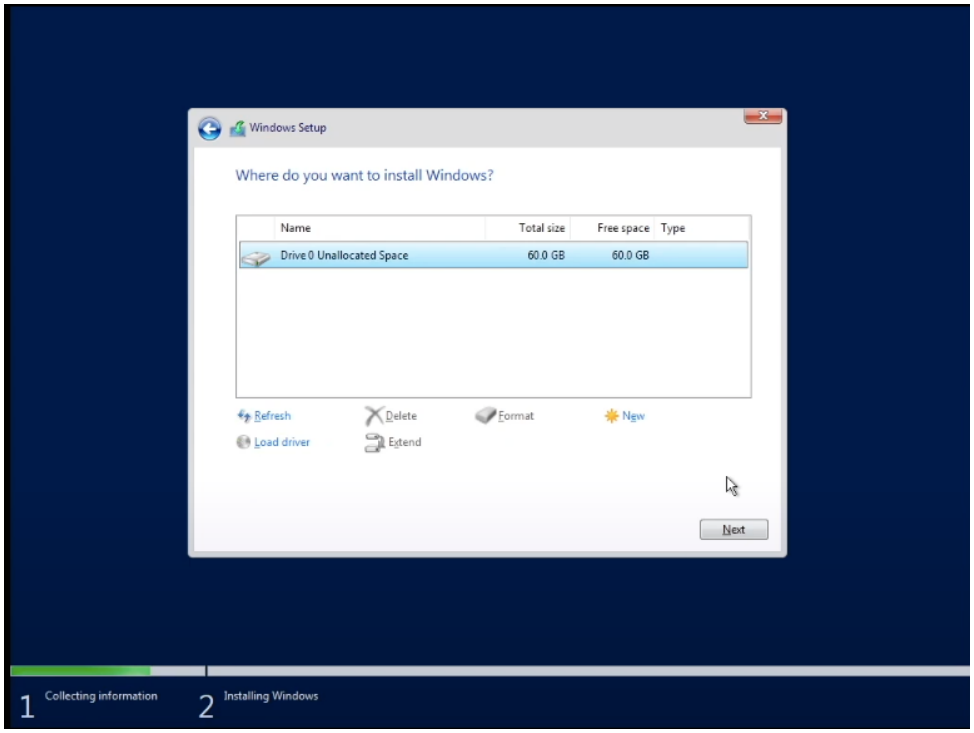


- Configuring a Windows Server as a Domain Controller

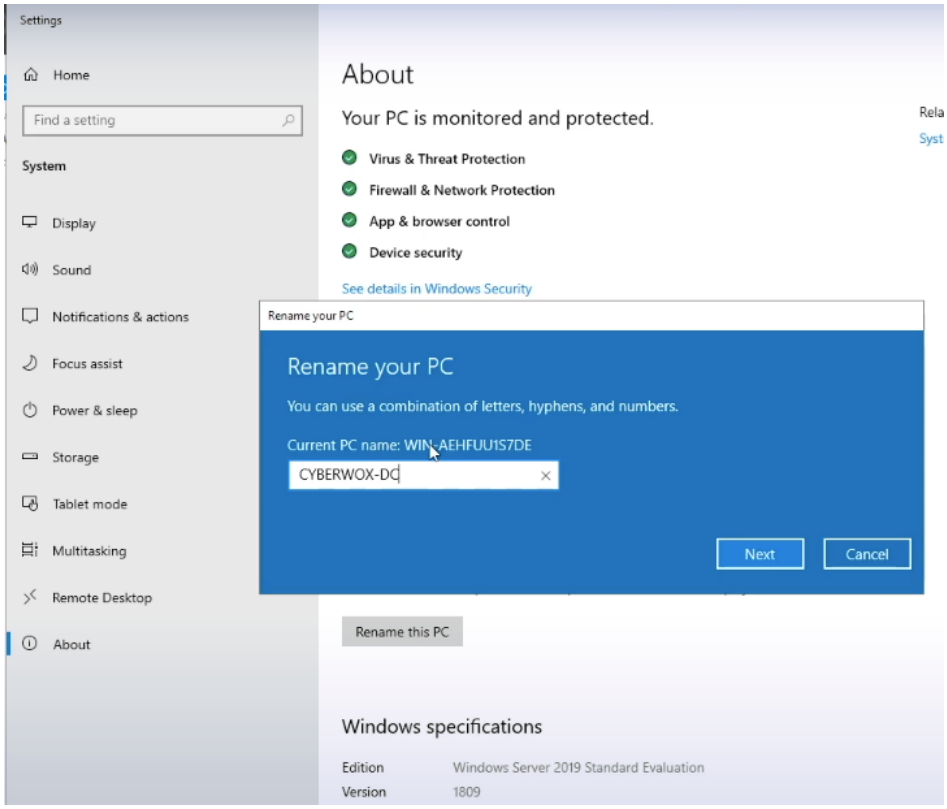
- Install Windows Server 2019 on VMWare Hypervisor



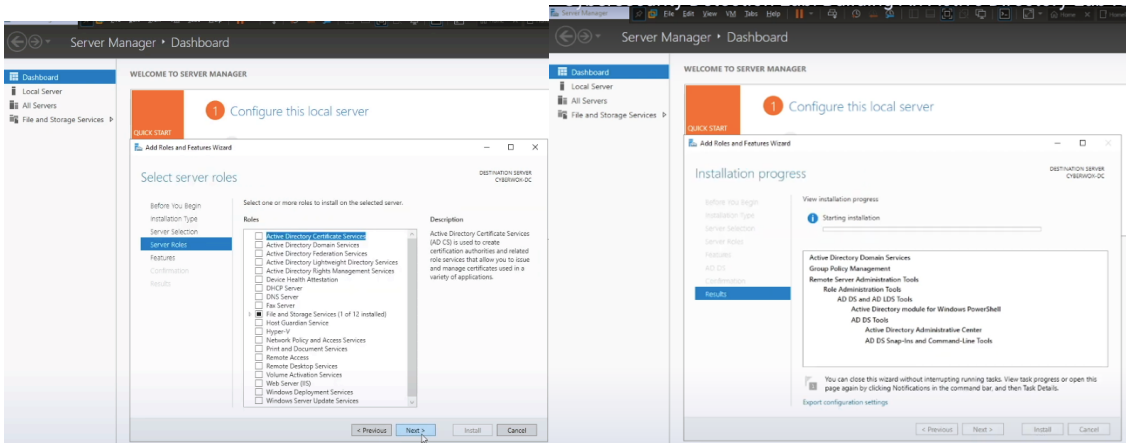


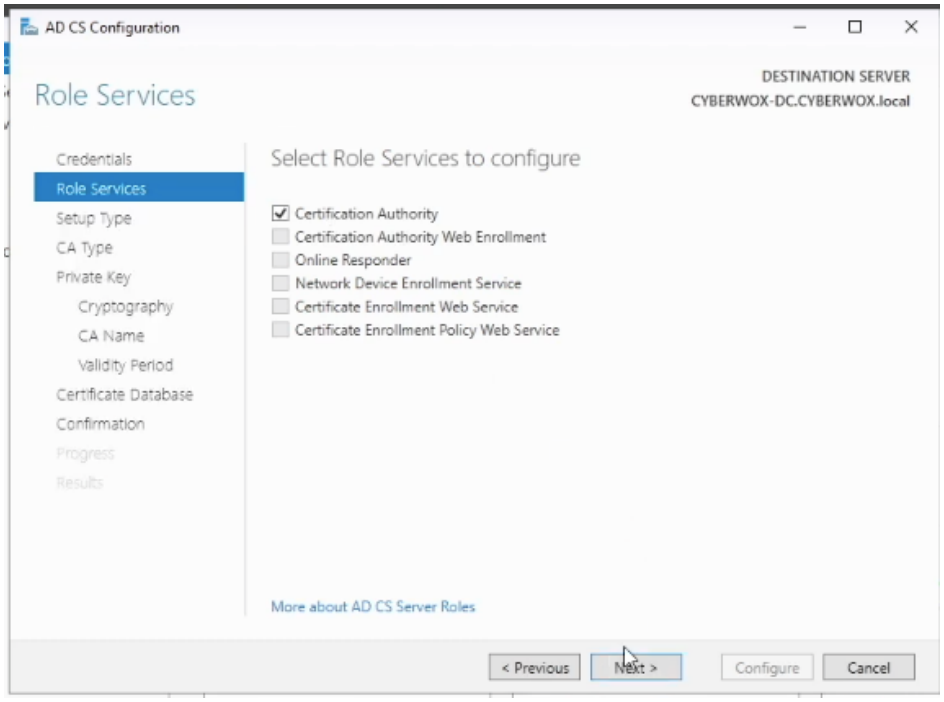


- Set up the machine and rename the PC.

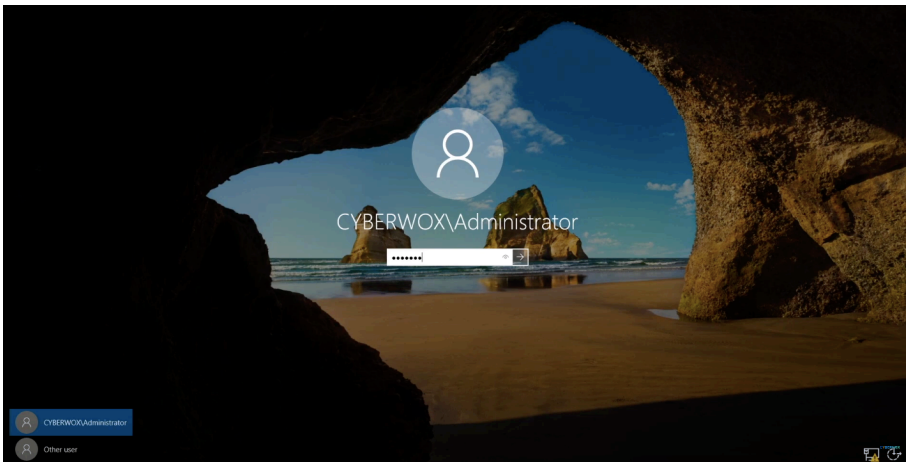


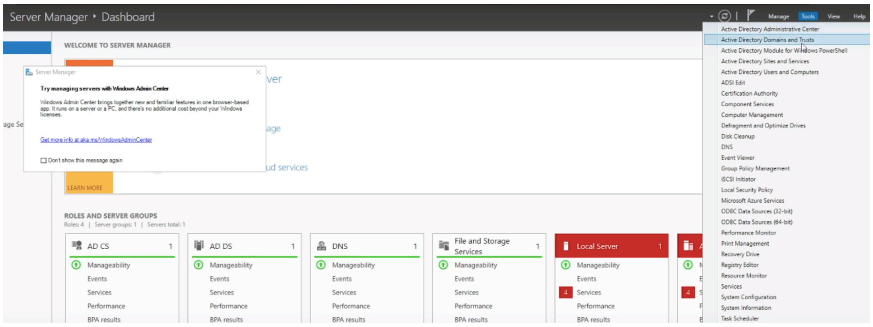
- Navigate to Server Manager and add the *"Active Directory Certificate Services"*
- Then, install the configurations to convert the local server to perform as the Domain Controller.

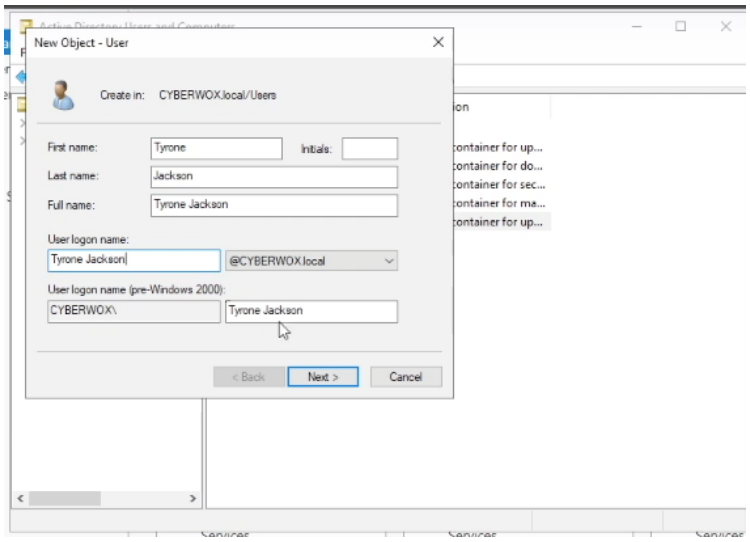




- Once you add the roles, you can restart your machine and you can log in with the *Administrator* account.
- Create a user profile and configure the IP of the default gateway.

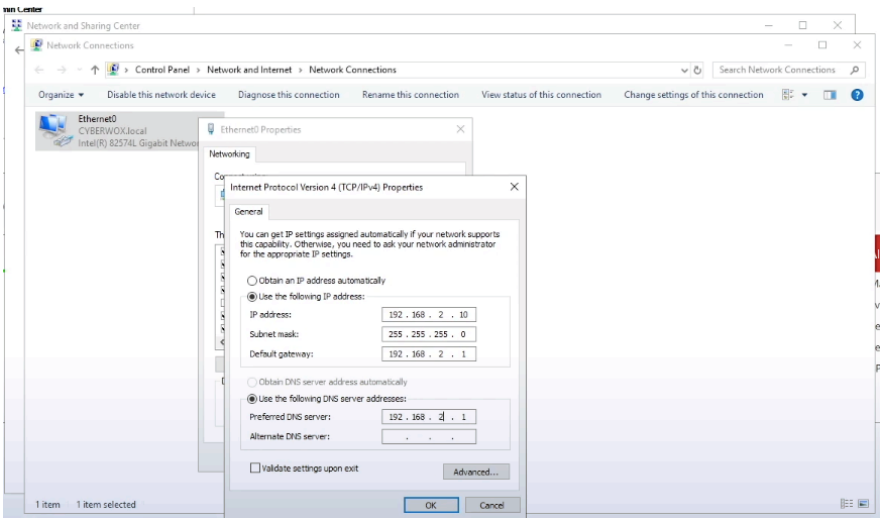




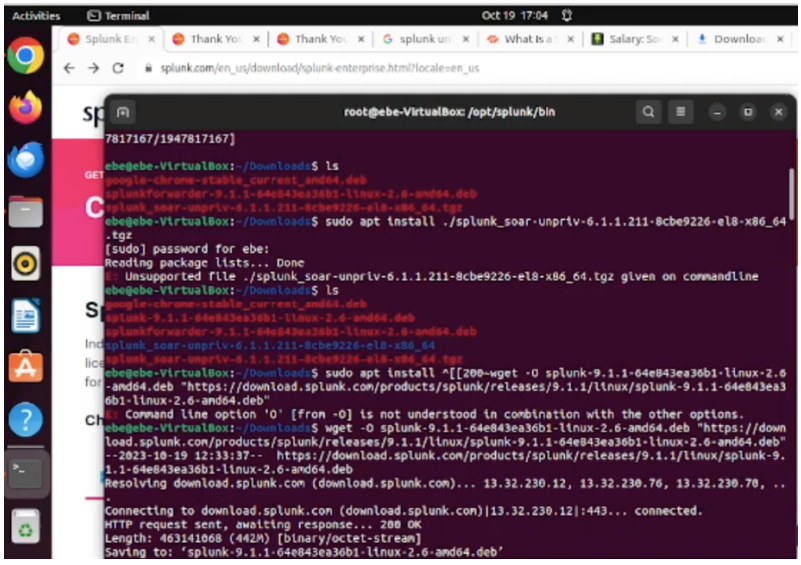


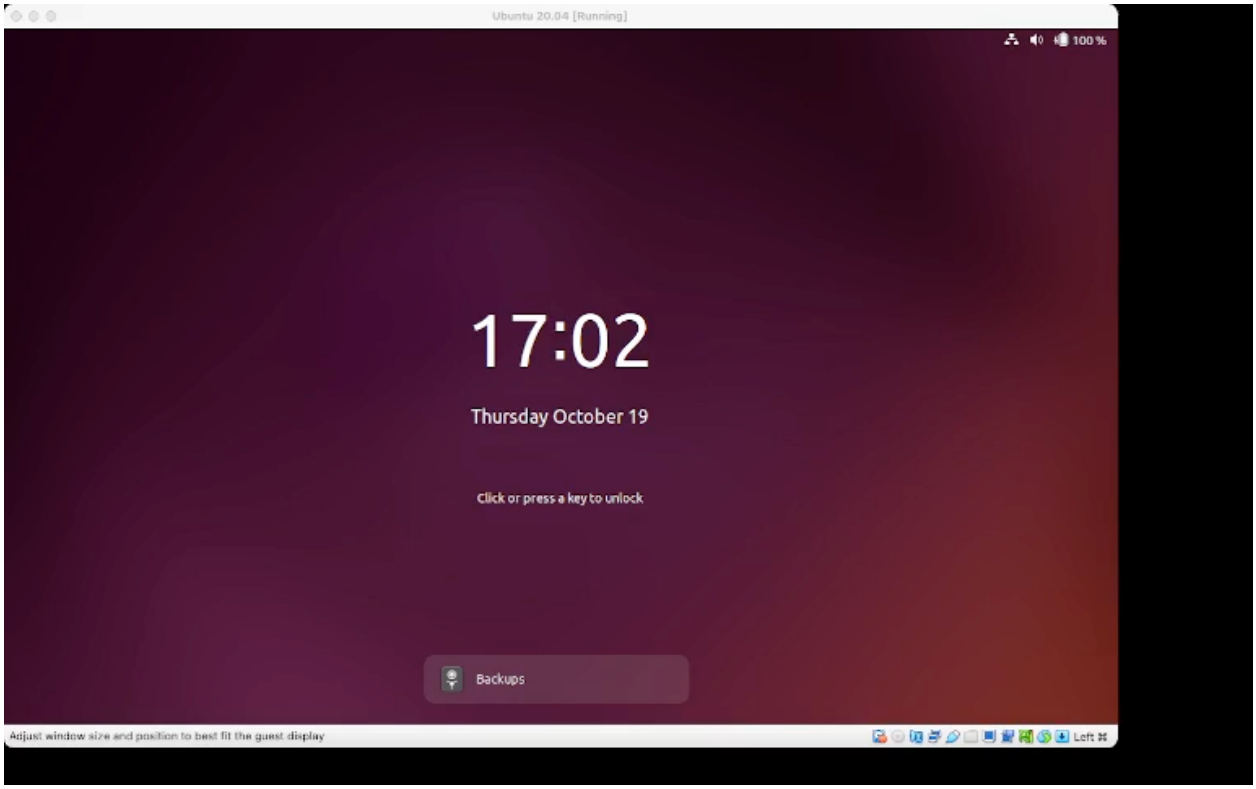
Now Use pfsense as the default gateway for the Domain Controller

- Navigate to Control Panel > Network and Internet > Network Connections

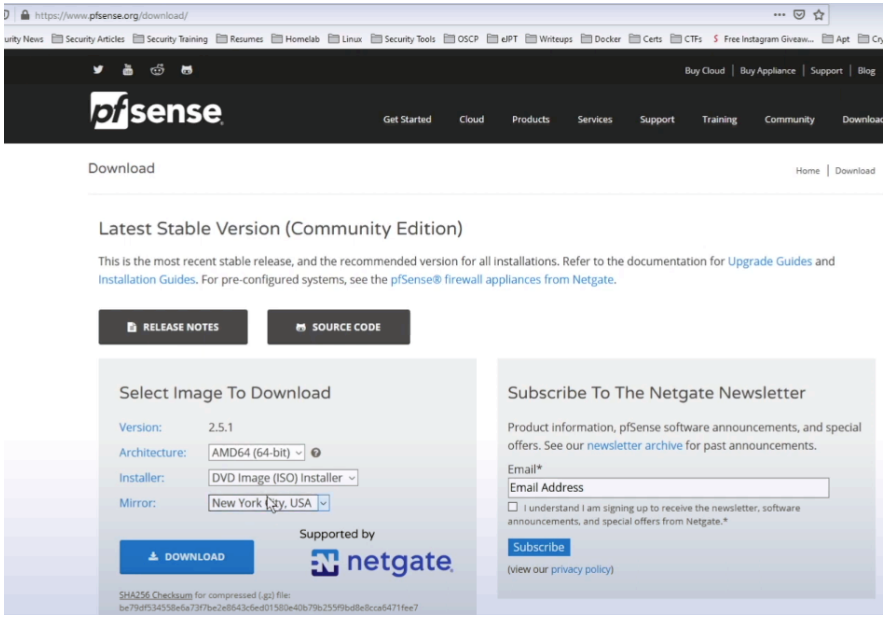


- Configuring Windows desktops
- Configure/Install Splunk Enterprise
  - Splunk will be installed using commands via Ubuntu's terminal.
  - https://medium.com/@dannyopara/installing-splunk-enterprise-on-ubuntu-step-by-step-guide-b545982038c3
  - ***Step-by-Step provided below***





- Configuring pfSense firewall for Network Segmentation & Security
  - Install pfsense from the website. Add the iso file to VMWare, and run the virtual machine created.



- The pfsense machine will power on and start with a screen similar to this. Accept all the default settings to install the machine and allow it to reboot.

- Enter option 1 to begin configuring the interfaces.

- Enter option 2 to configure the LAN interface.
  - The IP address, 192.168.1.1 is going to be used to access the pfsense WebGUI via the Kali Machine

```
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

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
```

Use the configuration 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
```

Use the configuration below for the OPT2 interface

```
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
```

- 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.

- ***Configuring Kali Linux as an attack machine***
  https://youtu.be/i0j-6iFBozg?si=qZcU1bsC1C_U7yk-

    - I couldn't configure this on my home lab machine, but this is a video on how to set up the Kali Linux machine in your home lab.