**For my GitHub click** [**here!**](https://github.com/thehappiihacker)

**Sp**A black background with a black square

Description automatically generated with medium confidence**ring 2024**

**Edward Brennan**

**Building a Cybersecurity Homelab for Detection & Monitoring** In the realm of cybersecurity, applying and implementing security concepts can present challenges when practical and secure infrastructure is lacking. Bearing this in mind, I undertook this project.

This homelab guides you through the steps of configuring, optimizing, and securing an IT infrastructure. While the scale may be modest, the skills acquired can be readily applied to larger, real-world enterprise setups.

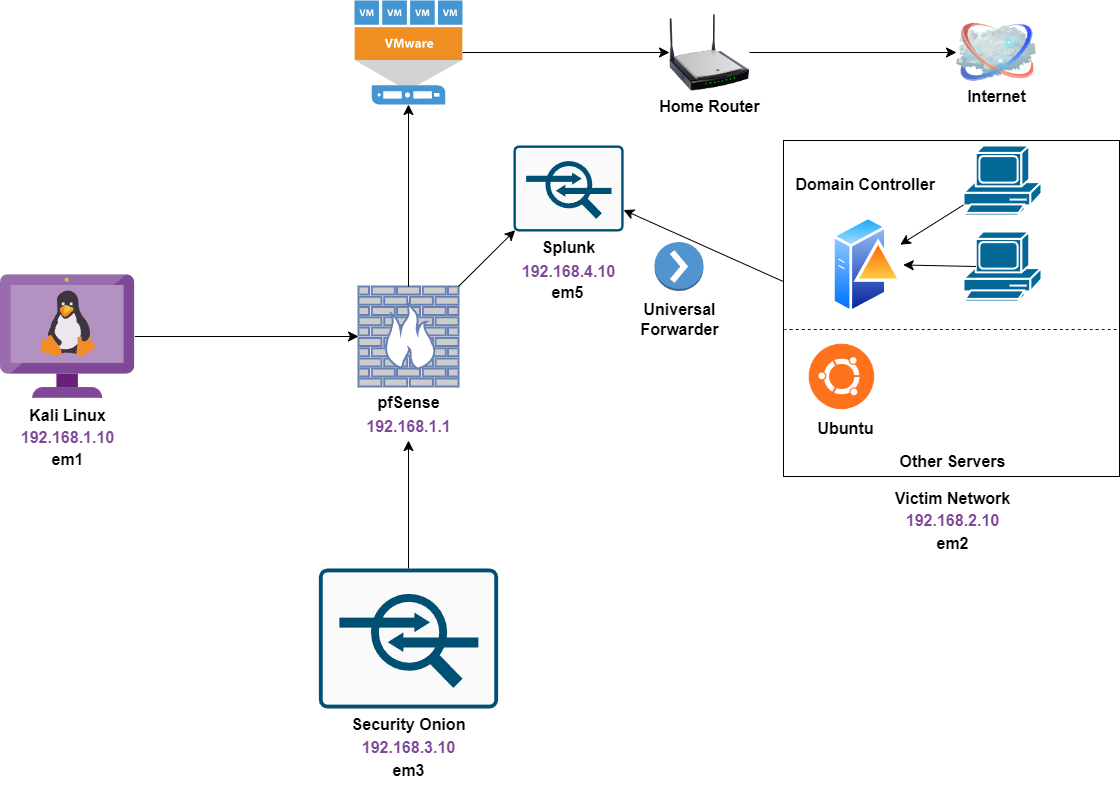
**What is a Homelab?**

A Homelab, as its name suggests, serves as a dedicated space within your home where you can hone and enhance your expertise in a particular field. This domestic laboratory is equipped with components and tools akin to those found in expansive infrastructures. It offers a secure setting for hands-on experimentation with these elements and gaining a deeper understanding of their functionalities.

***CONTENT***

* *Building Host PC*
* *Installing VMware Workstation as hypervisor*
* *Configuring pfSense firewall for Network Segmentation & Security*
* *Configuring Security Onion as an all-in-one IDS, Security Monitoring, and Log Management solution*
* *Configuring Kali Linux as an attack machine*
* *Configuring a Windows Server as a Domain Controller*
* *Configuring Windows desktops*
* *Configuring Splunk*
* *Ubuntu/CentOS/Metasploitable/DVWA/Vulnhub machines: All these are potential Linux machines that can be added to the network for exploitation, detection, or monitoring purposes.*

**HOMELAB NETWORK DESIGN & TOPOLOGY**

****

**Building The Host PC**

**CPU: Intel® Core ™ i5-9400f CPU @ 2.90 GHz**

**RAM: Team T-FORCE Vulcan Z 3200MHz 3200 MHz (max speed) 16GB (2 X 8 GB)**

**Storage: Intel 665p (1.0 TB)**

**Graphics Card: AMD Radeon RX 5700 XT**

**Motherboard: Gigabyte B365 Motherboard**

**Host OS: Win10**

**Downloading and Installing VMware Workstation Pro**

For this part of the lab, I followed the instructions [here](https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html). If you are a student, use a student email to get a lower-priced version with all the great features. This is going to turn into a yearly subscription.

A different option is VirtualBox if you cannot shell out the money for VMware Pro. I will be a little different of configuration for the lab, however. Main difference being VMWare autodetects the OS type and assists that way while VirtualBox does not. [Here](https://www.virtualbox.org/wiki/Downloads) is the link**.   
  
Installing and Configuring pfSense** Pfsense will be set up as a firewall to partition our private homelab network, restricting access solely to our Kali Linux machine.

Download the pfSense iso file from [here.](https://www.pfsense.org/download/) Make sure to select your correct architecture. For most people it should be AMD 64-bit version and the DVD Image (ISO) Installer.

**A screenshot of a computer

Description automatically generated**

In VMware, click “Create a New Virtual Machine”.   
 Next, select Typical (recommened). Then click Next.  
A screenshot of a computer

Description automatically generated

Click “Browse” and locate the file with the needed ISO in it. **Suggestion: keep all ISO files in the same place for ease of recreating this lab.**   
Click Next

A screenshot of a computer

Description automatically generated

Name you VM something simple, like pfSense. Then click Next  
A screenshot of a computer

Description automatically generated  
 Keep defaults, and click Next.

A screenshot of a computer

Description automatically generated

Click “Customize Hardware…”.  
A screenshot of a computer

Description automatically generated  
 Increase the memory to 2gb (2048 MB).

A screenshot of a computer

Description automatically generated

Add five (5) network adaptors and match them with a VMnet interface. Match below. And then click Close>Finish.

A screenshot of a computer

Description automatically generated  
The pfSense machine will power on and start with this screen. Accept all the defaults. pfSense will configure and reboot.  
You know it is configured correctly when you get to this.A screenshot of a computer

Description automatically generated

Enter Option 1  
**Should VLANS be set up now (y:n)?: n**For the following questions, enter em0, em1, em2, em3, em4 & em5 IN ORDER. This is important for the whole lab. Look below.  
A screenshot of a computer program

Description automatically generated  
  
This is what should pop up next.

A screenshot of a computer

Description automatically generated  
**Do you want to proceed [y:n]? y**Select option 2  
Starting with LAN interface(press 2)   
The Ipv4 address will be **192.168.1.1** which is going to be pfSense WebGUI via Kali Machine   
The screenshot provides all the settings: **A screenshot of a computer

Description automatically generated**

Use the configuration below for the OPT1 interface (Press 3)**.**

A screenshot of a computer screen

Description automatically generated  
Use the configuration below for the OPT2 interface (Press 4)**.  
A screenshot of a computer

Description automatically generated**

Leave OPT3 interface without configuring. This will be a span port for SecOnion monitoring.   
Use the configuration below for the OPT4 interface (Press 6)**.**A screenshot of a computer

Description automatically generated

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

**Installing And Configuring Security Onion in VMWare**

Security Onion is an all-in-one security monitoring solution. It has IDS, log management, and other features that will make our learning so much better.

Download the SecurityOnion ISO [here.](https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md)  
  
In VMWare, click File>New Virtual Machine> Typical (recommened)>Next  
**A screenshot of a computer

Description automatically generated**

Navigate to where you save the ISO file and select it. It will not auto detect the OS this time, so select Linux>CentOS 7 64-bit  
**A screenshot of a computer program

Description automatically generated**

Click Next, then name the machine ‘SecOnion’. Then Click Next.  
**A screenshot of a computer

Description automatically generated**

Make sure the Max Disk Size is 200GB, and select Store Virtual Disk As A Single File. Click Next **A screenshot of a computer

Description automatically generated**

* Select Customize Hardware and change memory to minimum 12 GB
* Change Processors from 1 to 4
* Add two Network Adapters and assign Vmnext4 and Vmnext5 respectively.  
  A screenshot of a computer

  Description automatically generated

Click Close>Finish.  
Boot Machine.  
A screen shot of a computer

Description automatically generated  
If you press nothing, SecOnion will start to run. When it is done initializing, type ‘yes’ when prompted.

A screenshot of a computer

Description automatically generated

Create a username and password. Since this is a VM, make it something easy and even make your passwords the same for simplicity across as many machines as you can. Feel free to make them as complex as you would like.

Let SecOnion un all scripts.

Press enter to reboot.  
When prompted enter in username and password.   
  
Select ‘Yes’

A screenshot of a computer screen

Description automatically generated

Click Enter  
A screen shot of a computer

Description automatically generated

EVAL should auto-select, if not select EVAL. The hit Enter.

A screen shot of a computer

Description automatically generated

Type out ‘AGREE’  
A computer screen shot of a computer

Description automatically generated

When prompted for minimum requirements, hit Enter through, and then after go into settings to change to those defaults.  
  
Select ens33  
A screenshot of a computer

Description automatically generated

Set Addressing to DHCP. Then hit Enter

A computer screen with a hand pointing to a blue and white screen

Description automatically generated  
Next prompt select Yes and hit enter.  
Select OK

Select Standard

Select Direct

Select ens35 as the monitor interface. Then hit Enter  
A screenshot of a computer

Description automatically generated  
Select Automatic for patching scheme  
Accept default home ip  
Accept all default until the email address section. Enter in email for admin account.   
Select IP  
A screenshot of a computer error

Description automatically generated

Select Yes for NTP servers. Keep default server.   
A screenshot of a computer

Description automatically generated  
  
When asked to run so-allow, select NO then continue.   
A screenshot of a computer

Description automatically generated

Take a screen shot of the next settings menu! It is important in order to remotely access SecOnion via web. The important part is the Management IP.   
A screenshot of a computer

Description automatically generated

It will now begin installing, which takes a long time. Once it is done, enter in creds.  
A screenshot of a computer

Description automatically generated

Enter the following command: sudo so-allow  
A screenshot of a computer program

Description automatically generated

Select A

Then Enter the IP address noted from the Ubuntu Desktop

**Setting up Ubuntu Desktop to Manage SecOnion** When you are a SOC Analyst or in that type of role, you would access your IDS using it’s IP address. This would be through some web portal.

In order to do this, we will be adding a Ubuntu Desktop in order to use a web portal to access our machine.   
  
[Download Ubuntu Desktop](https://ubuntu.com/download/desktop)  
  
[Install Ubuntu Desktop](https://getlabsdone.com/10-easy-steps-to-install-ubuntu-19-04-on-vmware-workstation-15/)  
  
Go to File>Create a New Virtual Machine. Same as before

Select Typical(recommened)>Next  
Select Browse and navigate to the ISO

Fill in the information as such, and create a username and password. Then hit next.  
A screenshot of a computer

Description automatically generated

Now, name the machine.   
A screenshot of a computer

Description automatically generated

Leave defaults.

A screenshot of a computer

Description automatically generated

No customization in hardware needed on this one! Just connection to the internet, which is by default. Hit Finish.

First boot while take awhile to load up. Select defaults for the install.   
Installation completion will require a reboot, and reboot away!

Once you log in, got to terminal. Run the following command: sudo apt install net-tools  
A screenshot of a computer

Description automatically generated

Enter password for Ubuntu, install will complete.   
  
With these tools installed, run ifconfig. Note the inet address. Ours will be different.   
A screenshot of a computer

Description automatically generated  
  
Head back to your Security Onion instance and run the following command: sudo so-allow

Type in password and wait.   
  
Select a from these options  
A screenshot of a computer

Description automatically generated

Type in the IP address from the Ubuntu desktop, this will tell the firewall to allow that IP to look at SecOnion.   
  
Use FireFox in Ubuntu to navigate to the SecOnion IP

A screenshot of a computer

Description automatically generated

The log in will be the email and password you set up during the installation of Sec Onion. Feel free to use the hamburger menu in the top right to explore the tool.   
  
**Installing Kali Linux**

K Kali Linux will be an easy install. Download the install package [here.](https://www.kali.org/get-kali/#kali-installer-images)  
  
Chose the Recommended version.  
A screenshot of a computer

Description automatically generated

Let it install then go to VMWare.   
  
File>New VM  
  
Select Typical(recommended) and navigate to the ISO  
  
Choose these settings. Click Next

. A screenshot of a computer

Description automatically generated

Name it Kali Linux. Click Next.  
A screenshot of a computer

Description automatically generated

Leave defaults. Click Next.  
A screenshot of a computer

Description automatically generated

Customize settings and add a Network Adapter  
Map the Network Adapter 2 to VMnet 2. Click Close>Finish.  
A screenshot of a computer

Description automatically generated

Power on the machine.  
Proceed with Graphical Install.  
Let the machine run, then configure with your desired language.  
Continue through defaults till you get to host name.  
Leave name as Kali  
A screenshot of a computer error

Description automatically generated

Leave domain name blank.

A screenshot of a computer

Description automatically generated

Full name is Kali  
A screenshot of a computer error

Description automatically generated

User name is Kali

A screenshot of a computer screen

Description automatically generated

Password is what you would like.

Select time zone and let it run.

Select Guided

A screenshot of a computer error

Description automatically generated

Select Default Disk  
A screenshot of a computer error

Description automatically generated

Select Default  
A screenshot of a computer error

Description automatically generated

Continue> Change to yes> Continue and let it install.  
A screenshot of a computer

Description automatically generated

Select Default as “Xfce (Kali’s default…). Hit conitinue.A screenshot of a computer

Description automatically generated

Install Boot Loader

A screenshot of a computer error

Description automatically generated

Select Drive /dev/sda Then Continue

A screenshot of a computer

Description automatically generated

Click continue. Installation will be complete, reboot to boot into Kali Linux.

My password and user:

Kali

Admin

Our kali machine will be used to configur pfSense interface and rules.

pfSense Rules and Configuration

We will use our Kali machine monitor pfSense.

Open up the browser in Kali, and in the search bar type in our IP for pfSense.

A screenshot of a computer

Description automatically generated

The default username is admin and password is pfsense. CASE SENSITIVE.

Click Sign in You can choose to save it or not. I will save it since it is a VM and I can terminate the VM whenever.

A blue screen with white text and green button

Description automatically generated

Click advanced, then accept the risk.

You will now be in pfSense GUI

A screenshot of a computer

Description automatically generated

For the General Setup, click Next, Next and set primary DNS server to 8.8.8.8 and secondary to 4.4.4.4A screenshot of a computer

Description automatically generated

Chose your timezone.

Next step (4 of 9) uncheck the last two settings. Since this a monitoring lab, it will be best to see the most activity as possibleA screenshot of a computer

Description automatically generated

Step 5 of 9, click next for defaults.

A screenshot of a computer

Description automatically generated

Step 7 of 9, you can change your password here, and save the new one.   
Step 8 of 9, hit reload pfSense.  
Step 9 of 9, click finish

Make sure you read the AUP, it is just to ensure this is for LAB USE not for Enterprise Use.

Navigate to Interface>AssignmentA screenshot of a computer

Description automatically generated

We are going to configure the different assignments. They are set to the pfSense ones we set before.

For LAN:

A screenshot of a computer

Description automatically generated

Click Save at the bottom. Then Apply Changes

Now go to Services>Router Advertisements>Disable Router Mode  
A screenshot of a computer

Description automatically generated

Go back to Interfaces>Kali>Ipv6 Config Type>None>Save  
A screenshot of a computer

Description automatically generated

Go to Interfaces>OPT1 and do the following then hit save:  
A screenshot of a computer

Description automatically generated

Go to Interfaces>OPT2 and do the following then hit save:  
A screenshot of a computer

Description automatically generated

Go to Interfaces>OPT3 and do the following then hit save:

A screenshot of a computer

Description automatically generated

Go to Interfaces>OPT3 and do the following then hit save:

A screenshot of a computer

Description automatically generated

Now Navigate to Interfaces>Assignments>Bridges

A screenshot of a computer

Description automatically generated

Click Add and add the following then scroll down and saveA screenshot of a computer

Description automatically generated

Navigate to Firewall>Rules

Click New>Protocol>ANY>Save>Apply Changes

A screenshot of a computer

Description automatically generated

That is all for configuration, but lets take a snapshot of our system. Right click on pfSense machine>Take Snapshot>Name it Post Wizard Config>Take Snapshot

A screenshot of a computer

Description automatically generated

Do this with the other machines as well.

**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.  
  
[Download the Windows 2019 Server Evaluation Copy](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019)

[Download the Windows 10 Evaluation Copy](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)

**Important Points:**   
Make sure you remove the Floppy Drive, this only appears after you configure the machine, so do not automatically start the machine. I will share screenshots to make this clear. If you do not remove this drive, the Server 2019 will ask for a product key during installation.

Go to File> New VM>Navigate to your Server 2019 ISO

A screenshot of a computer

Description automatically generated

Click Next and ignorre the product key.

A screenshot of a computer

Description automatically generated

Click Next and Name it what you please.  
A screenshot of a computer

Description automatically generated

Keep defaults:

A screenshot of a computer

Description automatically generated

Customize the following hardware:

A screenshot of a computer

Description automatically generated

Click Close and uncheck “Power on this VM….”

A screenshot of a computer program

Description automatically generated

Click Finish.

Before powering on, go to Windows Server VM>Edit VM. You will now see the floppy disk adaptor.

A screenshot of a computer

Description automatically generated

Remove the Floppy adaptor. Then power on the machine. When booting, be prepared to press any key! This will boot into the ISO. If you miss this, you will need to start at the beginning of this section.

Click Next:  
A screenshot of a computer

Description automatically generated

Click Install Now:

A screenshot of a computer

Description automatically generated

Select the Windows Server 2019 Standard Eval (Desktop Experience) Then Next:  
A screenshot of a computer

Description automatically generated

Accept License Terms Then Next:

A screenshot of a computer

Description automatically generated

Select Custom Install:

A screenshot of a computer

Description automatically generated

Click New>Apply>Okay and partitions will format:

A screenshot of a computer

Description automatically generated

Click Next and it should start installing:

A screenshot of a computer

Description automatically generated

Restart when done

Create a custom password: something easy for you(Loveleslie2!)

A screenshot of a computer login

Description automatically generated

Send a CTRL-ALT-Del to your computer using VMWare:

A screenshot of a computer

Description automatically generated

Log in

Go to Settings:

A screenshot of a computer

Description automatically generated

Search “PC Name”:

A screenshot of a computer

Description automatically generated

Select Rename PC and chose the name you like:

A blue screen with white text

Description automatically generated

Select to restart now.

Go to Manage>Add Roles and Features

A screenshot of a computer

Description automatically generated

Defaults and click Next>Next>Next to end up at Server Roles:

A screenshot of a computer

Description automatically generated

Click Active Directory Domain Services>Add Feature:

A screenshot of a computer

Description automatically generated

Click Next>Next>Next>Install:

A screenshot of a computer

Description automatically generated

Click Close

Click the flag with yellow caution>Promote this server to a domain controller:

A screenshot of a computer

Description automatically generated

Select Add New Forest>Specify Domain Name>Next>Set Password:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Click Next>Next>Next>Next>Install>Wait for Reboot:

A screenshot of a computer

Description automatically generated

Select Manage >> Add Roles & Features again on the Server Manager

Click Next>Next>Next> select Active Directory Certificate Services> Add Feature

A screenshot of a computer

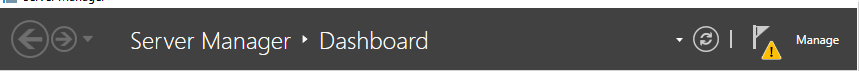
Description automatically generated

Click Next>Next>Next>Next>Check Restart the destination server automatically if required> Install:

A screenshot of a computer

Description automatically generated

Click the flag with the caution symbol:



Select “Configure Active Directory….”

A screenshot of a computer

Description automatically generated

Click Next>Check Certification Authority:

A screenshot of a computer

Description automatically generated

Click Next>Next>Next>Next>Next>Change years to 99:  
A screenshot of a computer

Description automatically generated

Click Next>Next>Configure:

A screenshot of a computer

Description automatically generated

Restart the server manually:  
A computer screen shot of a computer

Description automatically generated

Top right hand corner, select Tools>Active Directory User and Computers:  
A screen shot of a computer

Description automatically generated

Select your Domain name>(Right Click) User> New> User:  
A screenshot of a computer

Description automatically generated

Fill in a fake person account:  
A screenshot of a computer

Description automatically generated

Create a password and set to never expire>Finish: (admin21!)  
A screenshot of a computer

Description automatically generated

Go to User Folder>Select newly created user>Copy and create a second user:

A screenshot of a computer

Description automatically generated

Click the Windows Logo>Search for “Windows Defender Firewall”> Turn off:  
A screenshot of a computer

Description automatically generated

This is not normally recommended!!! Only doing this to create an increase in alerts for our firewall.

Navigate to Control Panel > Network and Internet > Network and Sharing > Change Adapter Settings:

A computer network connection screen

Description automatically generated

Enable the following settings:

A screenshot of a computer

Description automatically generated

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

[Download Windows 10 Evaluation Copy](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)

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.

Go to you Windows Sever machine and log in. Go to cmd prompt and run ipconfig command:

A screenshot of a computer

Description automatically generated

We will be using the Ipv4 address for the next part.

Go to your Kali Linux machine and log into pfSense.

Once logged in go to Services>DHCP Server>VictimNetwork:

A screenshot of a computer

Description automatically generated

Scroll down to DNS Server and fill in the Ipv4 address from your Windows Server:

A screenshot of a computer

Description automatically generated

Add the name of the server under other:

A screenshot of a computer

Description automatically generated

SAVE CHANGES!

Now Create your new VM

A screenshot of a computer

Description automatically generated

Change name to name of the first account you created in WinServer:

A screenshot of a computer

Description automatically generated

Next:

A screenshot of a computer

Description automatically generated

Next>Next>Customize Hardware>Change Network Adapter to VMNet3:

A screenshot of a computer

Description automatically generated

Uncheck Power on Automatically>Click Finish:

Edit Virtual machine>Remove Floppy:

A screenshot of a computer

Description automatically generated

Click fast to boot into ISO properly

Click Next>Install Now:

A screenshot of a computer

Description automatically generated

Accept Terms> Custom Install>Next:

A screenshot of a computer

Description automatically generated

The machine will reboot itself.

Configure window 10 like normal:

A screenshot of a computer

Description automatically generated

Click “I don’t have internet”:

A screenshot of a computer

Description automatically generated

Click Continue with limited setup:

A screenshot of a computer

Description automatically generated

Setup the first username and password from previous step(Arnold):

A screenshot of a computer

Description automatically generated

Go through secuirty questions

Uncheck all privacy settings:

A screenshot of a computer screen

Description automatically generated

Not now to Cortana:

A group of people holding papers and a notepad

Description automatically generated

While you wait set up the second desktop with the second user account credentials but the same configurations. Repeat above steps for second machine.

Rename the first PC Then restart PC:

A screenshot of a computer error

Description automatically generated

While you wait for the second VM to install, do the following:

Navigate to the adaptor settings:

A screenshot of a computer

Description automatically generated

Right Click Ethernet0 and click proerties:

A screenshot of a computer connection

Description automatically generated

Select Ipv4:

A screenshot of a computer

Description automatically generated

Use the following settings:

A screenshot of a computer

Description automatically generated

RESTART BEFORE THE REST!

Search “domain” and select Access work or school:

A screenshot of a computer

Description automatically generated

Click Connect>Join this device to a local Active Directory Domain:

A screenshot of a computer screen

Description automatically generated

Type in your domain name, and it will allow you to add to the domain.

**Configuring Spunk**

Splunk is a SIEM that is widely used in the industry of security. Learning how to use a SIEM would be great to help you break into Cyber. For our Splunk install, we will need to install Ubuntu Server:

[Download Ubuntu Server](https://ubuntu.com/download/server)

Go about setting up a VM like we have previously. This time navigate to Ubuntu Server ISO.

Here is the customization:

A screenshot of a computer

Description automatically generated

Install the server using the first option aka the default method.

After that, let it run, and select default language and keyboard layout Then select Ubuntu Server:

A black and orange screen with white text

Description automatically generated

Click enter>Enter>Enter> Continue while disk check is running>Use below settings:  
A screenshot of a computer

Description automatically generated

Hit Done

Click Done again:

A screenshot of a computer

Description automatically generated

Continue:

A screenshot of a computer

Description automatically generated

Set up similar to this :

A black and white striped background

Description automatically generated

Skip Ubuntu Pro

Install OpenSSH Server:

A black and orange screen with white text

Description automatically generated

Select all services you want then click done. This will start install:

A screen shot of a computer

Description automatically generated

Click Reboot Now once done:

A screenshot of a computer

Description automatically generated

IT will say it failed to mount CD/ROM. That is noraml, hit enter and proceed to log in screen:  
A screenshot of a computer program

Description automatically generated

If login does not appear automatically, hit enter once.

We need to install tasksel to make the GUI like Ubuntu desktop. This makes it overall a better user experience. Use the following command:

sudo apt install tasksel

Say yes:

A screenshot of a computer

Description automatically generated

Run the command that follows:

Sudo tasksel

Select the top option, should be Desktop Experience option. Wait for install:

A screenshot of a computer

Description automatically generated

Run the “reboot” command A screenshot of a computer

Description automatically generated

Once ot reboots, a GUI should come up:

A screenshot of a computer

Description automatically generated

Log in, On your Ubuntu Server, Navigate to [Splunk.com](https://www.splunk.com/)

Click Free Splunk:

A screenshot of a computer

Description automatically generated

Create an account

Log into created account

Click “Free Trials and Downloads Page”:

A screenshot of a cloud trial

Description automatically generated

Scroll to Splunk Enterprise>Get Free Trial:

A screenshot of a phone

Description automatically generated

Click Linux>.tgz>download now:

A screenshot of a computer

Description automatically generated

Scroll all the way down to agree to Terms and Conditions>Access Program:

A pink button with black text

Description automatically generated

It will now start to download. Now open Terminal and navigate to downloads:

A screenshot of a computer

Description automatically generated

Run the following command:

Tar xvzf (current splunk name of downloaded file)

Use the following commands:

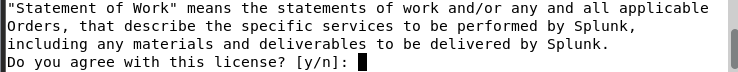
A screenshot of a computer

Description automatically generated

Now **cd bin** to get to the bin. Then use the command: **./splunk start:**

Hold enter to scroll past the terms of service:

Hit Y to agree:

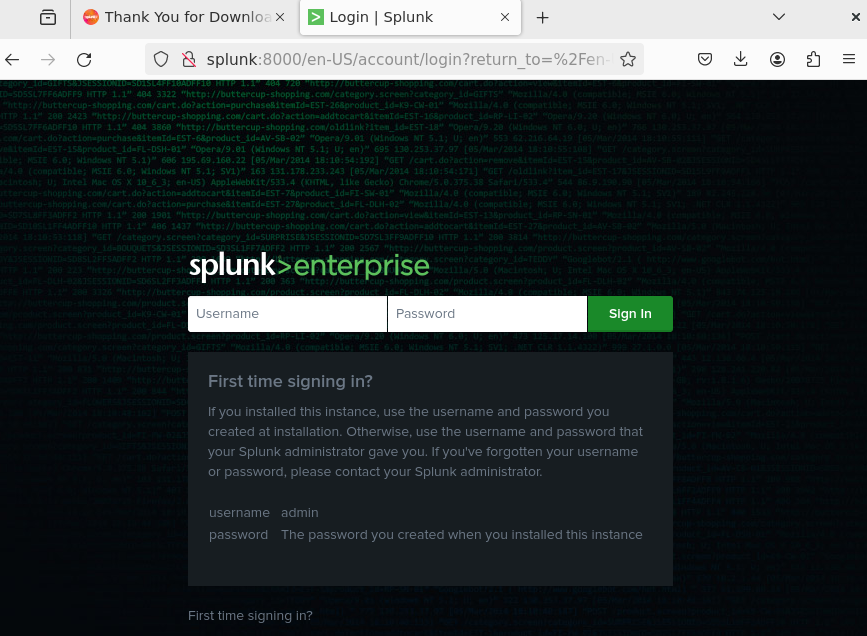
****

Create a username and password:

**A screenshot of a computer program

Description automatically generated**

Splunk will now be available in <http://splunk:8000>



Sign in and save password if you wish.

**Installing Universal Forwarder on Windows Server**

This will be a quick section of the lab. To look at activity on endpoints and log it we will need to install Universal Event Forwarding. This can be installed rather easily. \

First, power down the machine and add a Network Adapter and assign it to Vmnet6:

A screenshot of a computer program

Description automatically generated

Fire up the machine, and in Splunk navigate to Settings>Forwarding and Receiving>New Receiving Port:

A blue line on a white background

Description automatically generated

Enter Port number 9997 and click save.

Navigate to Settings>Indexes>New index

Name the index **WinEventLog** and click save.

On the **WINDOWS SERVER** download the Universal Forwarder: [Download the Universal Forwarder](https://www.splunk.com/en_us/download/universal-forwarder.html)

Start he install process, accept license agreement, and click next.

Click customize options and create a username and password.

Enter the IP Addresss of the Splunk Server and the default ports. These will be 8089 and 9997.

Install and go back to the Splunk VM.

Go to Settings>App Data> Select Forward:

A screen shot of a computer

Description automatically generated

Select the DC>Enter a Server Class (Domain Controller)> Hit Next

Select Local Event Logs and choose the one you want> Hit Next

Select **WinEventLog** as the index>Review>Submit

That is a wrap on this home lab project. You can now look at events and look up how to handle and interpret these events. This is mainly for test purposes, so these machines are almost wide open. You can play around and disallow any ports you’d like. Enjoy! And Shoutout to [CyberWox](https://www.youtube.com/@DayCyberwox) for designing this lab. It was a huge help, I was able to replicate it and get some of my own hands on experience with these things now.