***User Guide***

***Manual on creating a***

***Cybersecurity***

***home lab***

****

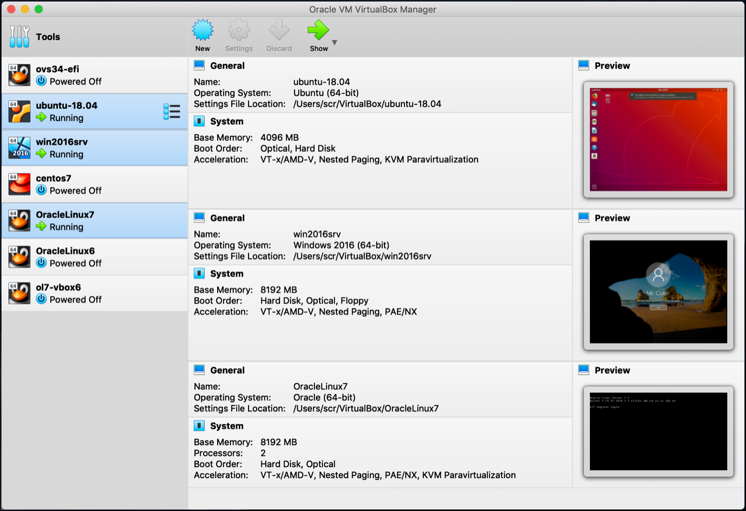
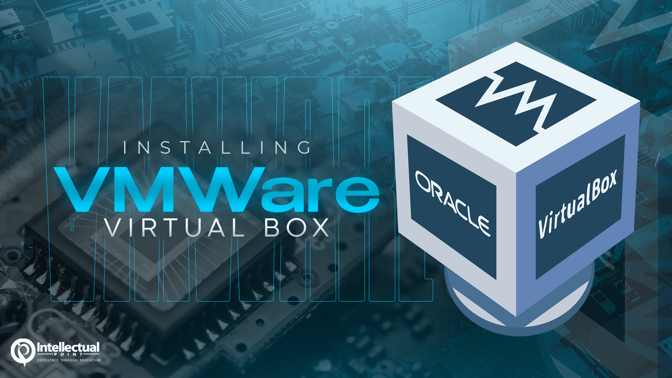
Ebenezer Adekeye | Info-Tech Project | Dr. Shuting Park | Deliverable Guidelines:

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:

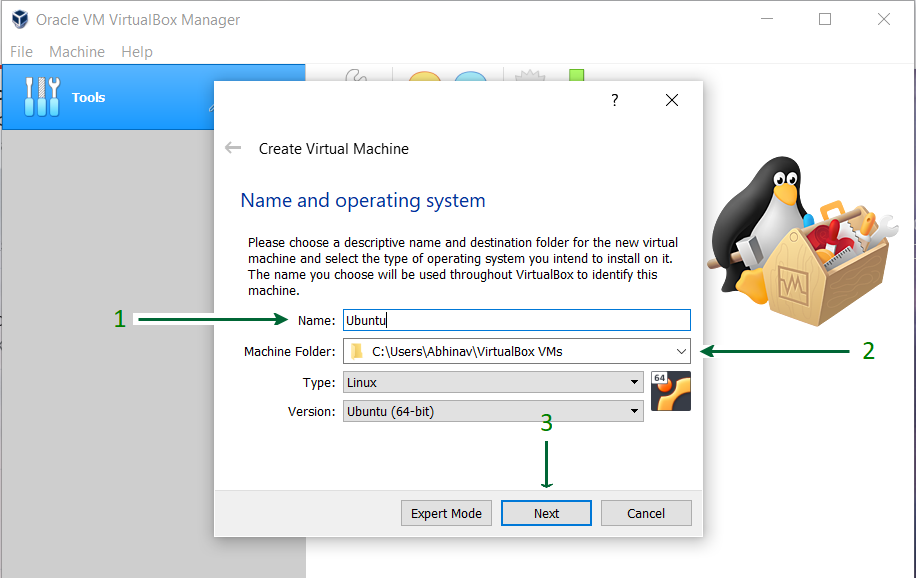
***Building Host PC***

* 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.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

* Configuring a Windows Server as a Domain Controller
  + Install Windows Server 2019 on VMWare HypervisorA screenshot of a computer

    Description automatically generatedA computer screen shot of a computer

    Description automatically generated

A screenshot of a computer

Description automatically generated

* + Set up the machine and rename the PC.

A screenshot of a computer

Description automatically generated

* + 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.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

* 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.

A screenshot of a login screen

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Now Use pfsense as the default gateway for the Domain Controller

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

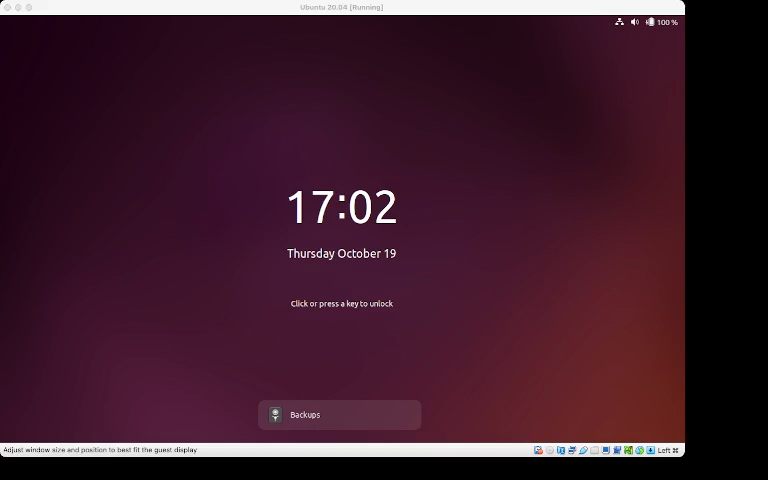
A screenshot of a computer

Description automatically generated

* 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***

A screenshot of a computer screen

Description automatically generated



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

A screenshot of a computer

Description automatically generated

* 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.

A screenshot of a computer

Description automatically generated A computer screen with white text

Description automatically generated

* 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

A screenshot of a computer program

Description automatically generated

Use the configuration below for the OPT1 interface.

A screenshot of a computer

Description automatically generated

Use the configuration below for the OPT2 interface

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer screen

Description automatically generated

This ends the configuration of the pfsense VM.

* ***Configuring Kali Linux as an attack machine***

<https://youtu.be/i0j-6iFBozg?si=qZcU1bsC1C_U7yk->

* I wasn’t able to configure this on my home lab machine, but this is a video on how to setup the Kali Linux machine in your home lab.