**Luz M. Ritacco**

**CS-NJ fellow**

**TKH fellowship 23-24**

**Due date: January-03-2024**

**P1-W-12**

**IF-Cybersecurity Phase 1 Final Project**

**Creating and setting a virtual Home Security -Lab**

**What is a Home-Lab?**

A home-lab for cybersecurity is a small version of an actual IT infrastructure that we can set up and control in our own space. It is a safe and isolated environment where we can investigate, study, and test various cybersecurity subjects and tools, without generating any threat or damage to the real world.

A Virtual cyber home lab it is a simulation platform that we created to replicate real-world IT systems and networks. It allows us to test and develop our cybersecurity skills in a safe, isolated environment. We can use a Virtual cyber home lab to practice various scenarios, such as defending against cyberattacks, conducting penetration testing, or performing digital forensics. This way, we gain hands-on experience with different cybersecurity aspects, such as threat detection, system hardening, and incident response.

**General Overview**

In this Project, we will learn how to create a cybersecurity home-lab from scratch. We will use VirtualBox to run Ubuntu desktop as your host machine and install pfSense as a firewall to protect your network simulations. We will also configure Snort as an intrusion detection system and use Splunk as a security information and event management (SIEM) tool, use Metasploitable2 as target/victim Virtual machine. Finally, we will set up Kali Linux as an attacker machine to perform various penetration testing scenarios.

# Planning and setting a goal of our virtual cyber-Home Lab

# The goal of this Cybersecurity Home Lab is to plan, design, build, and properly configure a virtualized personal cybersecurity training and learning environment This will allow me to practice and learn various cybersecurity skills and concepts, such as network security, penetration testing, malware analysis, digital forensics, and more. I will use a combination of open-source and commercial tools and platforms to create a realistic and dynamic lab environment that meets the final project requirements.

**Security Home-Lab Components**

* + **Virtual Box**

|  |
| --- |
| **VirtualBox:** is a virtualization software that allows users to run multiple operating systems on one machine. Developed by Oracle Corporation, VirtualBox is a **free and open-source** solution. With VirtualBox, users can easily create and manage virtual machines, which act as separate computers in isolated environments.  **VirtualBox:** is highly favored for its numerous features. Users can **simultaneously run multiple operating systems,** seamlessly integrate host and guest operating systems, and enjoy compatibility with a wide range of operating systems including **Windows,**[Linux](https://www.howto-do.it/what-is-linux/)**, and macOS.** |

* + **Ubuntu Desktop**

|  |
| --- |
| **Ubuntu** is a popular Linux-based operating system that offers a variety of desktop environments to choose from. The default desktop environment for Ubuntu is GNOME, which is a user-friendly and intuitive interface that is easy to navigate. GNOME provides a variety of features such as a top bar, activities overview, and workspaces that allow you to work with apps, windows, and appointments. You can also connect to wireless and wired networks, use a VPN, and create a wireless hotspot. |

* + **Kali-Linux**

|  |
| --- |
| **Kali Linux** is a Debian-derived Linux distribution designed for penetration testing. With over 600 preinstalled penetration-testing programs, it has earned a reputation as one of the best-operating systems used for security testing. As a security-testing platform, it is best to install Kali as a VM on VirtualBox.  **Kali-Linux** has a rolling release model, ensuring up-to-date tools on your system. Also, there is an active community of users providing ongoing support. |

* + **pfSense**

|  |
| --- |
| **PfSense** is an **open-source** firewall and routing software based on **FreeBSD**. So, it provides a secure and stable solution for **network security**. One key feature of pfSense is its ability to create and manage **virtual private networks (VPNs)**. This allows users to securely connect to their network from remote locations, encrypting and protectingtheir data.  **PfSense** also offers advanced **firewall** features, including stateful packet filtering. This allows the firewall to make decisions based on the connection context. It also includes traffic shaping capabilities to prioritize network traffic and ensure critical applications receive enough bandwidth. |

* + **Snort**

|  |
| --- |
| **Snort** is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity. |

* + **Splunk**

|  |
| --- |
| **Splunk** is a software platform that searches, analyses, and visualizes machine-generated data collected from your IT infrastructure as well as from your business's websites, applications, sensors, and other devices.  **Splunk** performs capturing, indexing, and correlating the real-time data in a searchable container from which it can produce graphs, reports, alerts, dashboards, and visualizations.  **Splunk** Enterprise Security is Splunk’s SIEM that helps you do all sorts of things, including security monitoring, incident response and management, compliance, and threat hunting. |

* + **Mataslpoitable**

|  |
| --- |
| **Metasploitable** is a virtualized Linux-based operating system that comes pre-loaded with a variety of vulnerabilities often found in operating systems that can be exploited. It is designed specifically for practicing penetration testing, network security, and Metasploit-Framework skills, among other things.  **Metasploitable** is a modular and customizable virtual machine that can be easily set up using a VM manager like VirtualBox. It is a great tool for learning and practicing ethical hacking in a secure environment. |

**Setting up the virtual Home-Lab**

* Setting up Our own virtual security lab using VirtualBox: <https://www.virtualbox.org/>
* Install Ubuntu Desktop on virtual box: [*https://ubuntu.com/download/desktop*](https://ubuntu.com/download/desktop)
* Install and Configuring pfSense Firewall on Ubuntu Desktop: [*https://www.pfsense.org/download/*](https://www.pfsense.org/download/)
* Setting up Snort on pfSense asIntrusion Detection/Prevention System *IDS,*
* Configuring Splunk on Ubuntu Desktop: [*https://www.splunk.com/*](https://www.splunk.com/)
* Install Splunk Universal Forwarder: <https://www.splunk.com/en_us/download/universal-forwarder.html>
* Install Metasploitable 2 in a VirtualBox: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
* Install and preparing Kali Linux for Attack Simulations: <https://www.kali.org/get-kali/#kali-platforms>

**Virtual Cybersecurity Home Lab-Diagram**

**A diagram of a computer network

Description automatically generated**

**Setting and preparing the Virtual Home-Lab**

Fist all, we will need a computer with a ***minimum of 16GB of RAM*** to effectively run multiple virtual machines simultaneously. Also, ensure you have ample storage space for the software installations and data generated during the lab activities. Having a ***reliable internet connection*** is beneficial for accessing online resources and updates.

**VirtualBox installation:** Itis particularly User-friendly with its intuitive interface, while Proxmox offers a suite of advanced features, making it ideal for setting up more complex network simulations. All these tools play a key role in creating a cybersecurity lab for practical learning and exploration ***(Please see the detail documentation for the installation/conf steps).***

A blue and white cube with white text

Description automatically generated

**Ubuntu desktop Installation**: This process it should not be difficult – we must create a new Virtual Machine on the VirtualBox, configure that Virtual Machine as we need it for the home lab, select a boot disk ISO image and boot from that installation image. When installation is complete, you will see a notification window. You must restart your Virtual Machine with Ubuntu on VirtualBox. ***(Please see the detail documentation for the installation/conf steps)***

A screenshot of a computer

Description automatically generated

**pfSense, Installation**: It should be straightforward process to install it on our VirtualBox since it is a free and open-source firewall and router software, plays a vital role in our cybersecurity home lab. It allows us to create network segmentation, dividing our virtual machines into different network zones that simulate a realistic network environment. It also improves our lab's security by monitoring network traffic and blocking any potential threats, protecting our learning space. Moreover, the practical skills we gain in managing network security through pfSense are essential for any cybersecurity practitioner. Therefore, in this lab, pfSense will be a key tool, helping us to effectively manage and secure our virtual network***. (Please see the detail documentation for the installation/conf steps).***

A screenshot of a computer

Description automatically generated

**Snort installation:** It should be easy process to install snort packets for our home lab since itis an open-source IDS that can easily be installed on a pfSense firewall to protect a home or corporate network from intruders. Snort can also be configured to function as an intrusion prevention system (IPS), making it very flexible. (***Please see the detail documentation for the installation/conf steps***).

A screenshot of a computer

Description automatically generated

**Splunk,** Installation and Settings within a VirtualBox is an important step in creating a cybersecurity environment that's both robust and flexible. Splunk helps analyze large amounts of data, such as security logs, making it a vital tool for security monitoring. By configuring Splunk in Virtual box, you are creating a controlled space where it can run without affecting other parts of your computer system. This approach allows for more focused monitoring, efficient use of resources, and easier scalability as your needs grow. It is a balanced solution that meets the demands of both novice users and seasoned professionals, providing a streamlined path to enhanced cybersecurity monitoring. We will be using an Ubuntu Desktop for our Splunk instance. ***(Please see the detail documentation for the installation/conf steps).***

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Installing Universal Forwarder:** In order to log the activities on endpoints, Splunk uses a mechanism called the universal forwarder. It is used to send alerts to indexers. Also, they provide reliable, secure data collection from various sources and deliver the data to Splunk Enterprise or Splunk Cloud for indexing and analysis.

The installation process is very similar to Splunk Enterprise, using the Ubuntu terminal coping theLinux .deb version to paste in the command line and follow the steps to install. ***(Please see the detail documentation for the installation/conf steps).***

A screenshot of a computer program

Description automatically generated

### A screenshot of a computer Description automatically generated

**Metasploitable 2**, Installation and setting up in the virtual machine, we must create a new Virtual Machine on the VirtualBox, configure that Virtual Machine as it need it for the home lab, Metasploitable 2 will be used to test the security on our network and practice ethical hacking in a safe environment. It is easy to set up and customizable. ***(Please see the detail documentation for the installation/conf steps).***

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Kali Linux** installation and setting in the VirtualBox, we must create a new Virtual Machine on the VirtualBox for our Home-Lab we are preparing Kali Linux for attacking simulation since Kali is a specialized Linux distribution, specifically tailored for digital forensics and penetration testing. It is a fundamental tool in our cybersecurity lab due to its capacity for simulating diverse types of cyber-attacks. Loaded with numerous security tools, Kali Linux enables us to emulate real-world attacks on our virtual network. This lab helps us learn cybersecurity in a practical way by setting up Kali Linux for attack scenarios. Kali Linux is a key tool for ethical hacking and penetration testing. By configuring it for this lab, we are creating an essential learning environment. ***(Please see the detail documentation for the installation/conf steps).***

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Here My Virtual Home Lab**

I have successfully completed the setup of the virtual cyber home lab with all the necessary components for this project. I have learned how to use the tools that are essential for creating a home lab. I have also practiced with detection rules, SIEM content, rule tuning, and attack scenarios to develop skills from different perspectives. ***(Please see the picture below).***

A screenshot of a computer

Description automatically generated

Using kali Linux, I successfully performed a penetration test on metasploitable2, a vulnerable virtual machine. I also monitored some data activity from Splunk, a software platform for data analysis. This was a challenging but rewarding task that demonstrated my skills and knowledge in ethical hacking and cybersecurity***. (Please see the pictures below).***

***A screenshot of a computer

Description automatically generated***

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Below are few of the issues I went into during the installation and setting up process.**

**☑ Metasplitable2 installation**: I had some issues installing Metasploitable2 in the VirtualBox such as:

* The virtual machine gets stuck at the startup screen.
* The installation process fails due to an error.
* The virtual machine does not boot after installation.

I spent a lot of time trying to fix the installation issues. I followed the troubleshooting steps, but nothing worked. I had to uninstall and reinstall the software several times, but I still encountered errors. I need assistance so I can be guided through the process and had helped on resolve the problem. Finally, I was able to install a working machine.

**☑** **PFSense Updating:** when I did the installation of pfSense in the virtual machine I used version 2.7.0 which worked fine, I was able to Install Snort Packets but when I was try the home lab, I had to update to version 2.7.2 which created an error on Snort packets I had to Re-install Snort.

**☑** **Ubuntu installation**: I was using Desktop the Installation was a straightforward process. I installed the PFSense & Snort and ended It was running perfect but when I was trying to test the home lab had several compatibility issues, such as unable to login in pfSense, Firefox was too slow, I end up uninstalling & reinstalling Ubuntu and declining automatic updates for Ubuntu.

**☑** **Kali-Linux installation**: I successfully downloaded and set up a new virtual machine in VirtualBox. It was the first software I installed, but I encountered few problems when I did the updated version of the VirtualBox from 6.1 to 7.1 version. I could not get it to work, so I uninstalled and reinstalled the software.

**☑** **Home-Lab Topology:** My initial plan was to set up a home lab topology using ubuntu Desktop and install pfsense-Snort packets on it. However, I encountered a few problems with the first installation and had to switch to kali-Linux instead. This also required me to modify few of the drawings.

**☑One of the final issues** I ran into was having internet connectivity on Ubuntu or Kali machine, making unable to access pfSense and Splunk Enterprise interfaces. The issue was resolve by checking the settings of each VM and ensuring that they had the correct internal network and/or bridged adapter configured. This also required VM restarts after changing the network settings. (it was time consuming and frustration process for this part of the lab settings).

**What I had learned from this lab environment setup are:**

* It is important to follow the instructions carefully and verify each step before proceeding to the next one. (especially when we are going to set up the network of each machine).
* It is useful to have a backup plan in case something goes wrong, or the expected results are not complete. (Make sure to do a clone machine or snapshot to make easy the process if we need to start all over again).
* It is beneficial to document the process and the outcomes for future reference and improvement.
* Instead of struggling alone, reach out to someone who can assist you and teach you something new. You can also take a break and refresh your mind before tackling the problem again. Both strategies can help you overcome obstacles and achieve your goals.
* It is challenging to troubleshoot and resolve issues that may arise during the setup, but it is also rewarding to learn from them.

**Conclusion**

The first component of our virtual home lab is the Host PC. It must meet the minimum hardware/software requirements to support the tasks and configuration we will perform. I use VirtualBox Workstation, which allows us to run multiple virtual machines simultaneously on one system.

Following, I set up a secure network environment using Ubuntu, pfSense, and Snort. First, I installed Ubuntu desktop on a host machine and configured its settings according to lab needs. Then, I installed pfSense firewall on another machine and connected it to the host machine. pfSense firewall is a powerful tool that allows us to create network segments and apply security policies to them. I also installed Snort on the pfSense machine, which is a software that monitors network traffic and detects intrusions, threats, and anomalies. By using these tools, we were able to create a comprehensive solution for network security and management.

Next, I install and configure Splunk on an ubuntu terminal, as well Splunk forwarder packets server as the home lab SIEM tool. That grabs data from different areas of your lab such as firewalls or servers and sends it to Splunk. This lets us check the network’s safety by reviewing the collected data.

Following, I install and configure Metasploitable 2 in the VirtualBox to create a virtual machine intentionally vulnerable for testing security tools and demonstrating common vulnerabilities.

Finally, I prepared Kali Linux, to be the attacker machine since it a potent tool designed for conducting penetration testing and security audits.

This Virtual security home lab is a setup in our home that simulates a professional network environment. It has various components and tools that we can use to learn and practice various aspects of cybersecurity. It is a safe place to test our skills and learn from our mistakes. It is important to use a separate setup for your lab, one that does not hold any critical data like personal files or sensitive information. This setup will serve as your experimental-learning lab.

In conclusion, the goal of a virtual security home lab is to provide a safe place to learn and practice cybersecurity skills, and to prepare us for real-world challenges that you may face in a large-scale/enterprise network.

**References:**

<https://www.youtube.com/watch?v=TW4l7X6G6Ak>

<https://www.virtualbox.org/wiki/Downloads>

<https://docs.rapid7.com/metasploit/metasploitable-2/>

<https://www.vulnhub.com/entry/metasploitable-2,29/>

<https://www.vulnhub.com/>

<https://www.youtube.com/watch?v=TW4l7X6G6Ak>

<https://www.youtube.com/watch?v=5iafC6vj7kM>

<https://docs.google.com/document/d/1A81KwMSI4zlnOXa-l6GDFry13Rj0YKBFnsfsvJKrIK0/edit>

<https://go.gliffy.com/>

<https://sourceforge.net/projects/metasploitable/>

<https://www.kali.org/get-kali/#kali-installer-images>

<https://youtu.be/6y-xqGoY9MY?si=cyIL2T-aJF8tjlWu>

<https://youtu.be/TvQfD5oUN5o?si=9Tnhx-t4yN0ulJjP>

<https://www.youtube.com/watch?v=TW4l7X6G6Ak>

<https://youtu.be/LX-Y-99zJ3M?si=5-1oISa99nNiQYp3>

<https://www.youtube.com/watch?v=yf3jetn4tN8>

<https://www.makeuseof.com/install-set-up-snort-ids-on-linux/>

<https://linuxgenie.net/how-to-install-snort-on-ubuntu-22-04/>

<https://www.bitsioinc.com/install-splunk-linux/>

<https://www.youtube.com/watch?v=LI4v7UDxxto&t=154s>