Setting Up a Cybersecurity Home Lab.

Why a Home Lab?

If you're looking to gain `hands-on cybersecurity experience` and bolster your resume, setting up a `cybersecurity home lab` is a great idea. Many entry-level job seekers face rejections due to lack of experience. To overcome this, internships and personal projects are crucial. This project guides you through setting up a simple home lab using your laptop or PC.

What is a Home Lab?

> A cybersecurity home lab is a specialized setup that allows individuals to learn and practice cybersecurity skills in a controlled environment.

It typically includes:

- Hardware (computers, routers and firewalls)
- Software components
- Security tools

The home lab enables the simulation of real-world scenarios:

- Network attacks and defenses
- Vulnerability assessments
- Penetration testing
- Incident response

Downloading VirtualBox

1. Go to the **VirtualBox website**.
2. Click on **Downloads**.
3. Choose the appropriate version for your operating system (Windows or Mac).
4. Install VirtualBox after downloading.
5. Download the **Extension Pack** for all supported platforms.
6. Agree to the terms to install the extension pack.

   Note: But since the operating system of my host machine is Linux mint, there's no need for the above steps. Enter the command below to install virtual box:

   ```
   sudo apt install virtualbox
   ```

Getting the Ubuntu ISO

1. Go to the **Ubuntu website**.

2. Download the latest **LTS (Long Term Support)** version.

Getting the Kali Linux ISO

1. Go to the **Kali Linux website**.
2. Click on **Get Kali**.
3. Download the **Installer Images** for the 64-bit version.

Setting Up Ubuntu in VirtualBox

1. Open **VirtualBox**.
2. Click on **Machine** and then **New**.
3. Name the virtual machine "Ubuntu".
4. Select the downloaded Ubuntu ISO image.
5. Click **Next**.
6. Change the username and password if desired.
7. Allocate at least **2 GB of memory** (if available).
8. Keep the processors at **1 CPU**.
9. Click **Next**.
10. Allocate around **20-25 GB** of disk space.
11. Click **Finish**.
12. Power up the Ubuntu virtual machine.

Ubuntu Setup Process

1. If it doesn't automatically open, double-click Ubuntu to start the VM.
2. Click **Install Ubuntu**.
3. Choose your language (e.g., English).
4. Select your keyboard layout (e.g. UK or US).
5. Click **Next** through the options.
6. Choose to install required media formats.
7. Select "Erase disk and install Ubuntu".
8. Create an account with a username, password, and timezone.
9. Click **Install**.
10. If any errors occur, click **Cancel** and close the window.

Setting Up Kali Linux in VirtualBox

1. In VirtualBox, click **New**.
2. Name the virtual machine "Kali".

3. Choose the Kali ISO image.
4. Click **Next**.
5. Allocate at least **2 GB of memory**.
6. Keep the processor at **1 CPU**.
7. Leave the disk space settings as default.
8. Click **Finish**.
9. Power up the Kali virtual machine.

Kali Linux Setup Process

1. Select **Graphical Install** and press Enter.
2. Choose your language (e.g., English) and continue.
3. Select your country location and keyboard layout.
4. For the hostname, leave it as "kali" and continue.
5. For the domain name, you can make one up or skip it.
6. Create a username (e.g., klaysoc) and password.
7. For partitioning disks, choose "Guided - use entire disk".
8. Click **Continue** through the options, keeping the recommended settings.
9. Select "Finish partitioning and write changes to disk".
10. Choose "Yes" to write changes to the disk.
11. For the boot loader, choose "Yes" and continue.
12. Select your device and continue.
13. Click **Continue** to reboot.
14. Log in with the username and password you set.

Setting Up Networking

1. Go to **Settings** in VirtualBox.
2. Click on **Network**.
3. Choose **NAT Network**.

If you can't select NAT Network:

1. Go to **Files** -> **Tools** -> **Network Manager**.
2. Click **Create** under **NAT Networks**.
3. Go back to the Network settings for both VMs.
4. Choose the created NAT Network.

Now, both your Ubuntu and Kali virtual machines are set up with network connectivity.

Updating OS Firmware

To update your operating systems to the latest firmware for both Ubuntu and Kali, follow these steps:

Ubuntu

1. Open the command line.
2. Enter the following command:

   “sudo apt update && sudo apt upgrade”

   This command updates the system and installs any essential tools that Ubuntu needs.

Kali

1. Open the command line.
2. Enter the following command:

   “sudo apt update”

   This updates the system.
3. To install any additional tools, enter:

   “sudo apt upgrade”

Simulating a Network Attack and Defense

To simulate a network attack and defense using Ubuntu and Kali:

Simulating an Attack from Kali

1. Type the following command, replacing `[IP address of Ubuntu]` with the actual IP address:

   “nmap -A [IP address of Ubuntu]”

   - To find the IP address of Ubuntu, go to Ubuntu and type `ip a`, then press Enter. Look for `inet` followed by the IP address (e.g., `10.0.2.5`).
2. If successful, it should display "Host is up" and show the Nmap scan report for the IP address.

Defending Against the Attack Using Ubuntu

1. Install the **Uncomplicated Firewall (UFW)**:

   “sudo apt install ufw”

2. Enable UFW:

`“sudo ufw enable”`

3. Allow SSH connections:

   `“sudo ufw allow ssh”`

4. Allow connections from the IP address of Kali (replace `[IP address of Kali]`):

   `“sudo ufw allow from [IP address of Kali]”`

   - Find the IP address of Kali using `ip a` on the Kali system.

5. Check the UFW status:

   `“sudo ufw status”`

   - The status should show as "active."

Analyzing Network Traffic with Wireshark

To analyze network traffic, you can use Wireshark on Ubuntu to capture the traffic.

1. Install Wireshark:

   `“sudo apt install wireshark”`

   - When prompted, select "Yes" for installing Wireshark without granting superuser privileges.

2. Run Wireshark:

   `“sudo wireshark”`

3. Click capture for your network to start capturing traffic coming into your network.

Simulating the Attack Again

1. From Kali, type the same Nmap command as before, replacing `[IP address of Ubuntu]` with the actual IP address:

   `“nmap -A [IP address of Ubuntu]”`

2. Observe the TCP packets being sent in Wireshark on Ubuntu to see the attack in progress.