Internship Assessment - Week 2

HACKER LAB SETUP

# Reported by: Dharani R

# Date : 01-03-2024

**E-mail id : dharaniramesh1926@gmail.com**

## Introduction:

We are going to setup hacker lab so you need one attacker machine like Linux and 1 victim machine.

## What is VirtualBox?

VirtualBox is open-source software for virtualizing the x86 computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS. The operating system running in the VM is called the "guest" OS. VirtualBox supports Windows, Linux, or macOS as its host OS. When configuring a virtual machine, the user can specify how many CPU (central processing unit) cores, RAM (random-access memory), and disk space should be devoted to the VM. When the VM is running, it can be "paused." System execution is frozen at that moment in time, and the user can resume using it later.

## How to install?

Step 1: Download VirtualBox

1. Open your web browser and go to the official VirtualBox website: https://www.virtualbox.org/.
2. Click on the "Downloads" link in the navigation menu.
3. On the Downloads page, find the version of VirtualBox that matches your operating system. There are versions available for Windows, macOS, Linux, and Solaris. Click on the appropriate link to start the download.

Step 2: Install VirtualBox

1. Once the download is complete, locate the installer file (usually a .exe file) and double-click on it to start the installation.
2. The VirtualBox Setup Wizard will open. Click "Next" to begin the installation.
3. Choose the components you want to install. Leave the default settings unless you have specific requirements.
4. Select whether you want to create shortcuts and click "Next."
5. Choose the location where you want to install VirtualBox or use the default and click "Next."
6. On the next screen, click "Yes" to install the Oracle Universal Serial Bus (USB) driver.
7. Click "Install" to start the installation process.
8. Once the installation is complete, click "Finish" to exit the wizard.

Step 3: Launch VirtualBox

1. After the installation, find the VirtualBox application in your applications menu or launch it from the desktop shortcut.
2. When VirtualBox opens, you're ready to create and manage virtual machines!

## What is Kali Linux?

## Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity. Kali Linux contains industry specific modifications as well as several hundred tools targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing. Kali Linux is a multi-platform solution, accessible and freely available to information security professionals and hobbyists.

## How to install?

Step 1: Download Kali Linux ISO

1. Go to the official Kali Linux downloads page: https://www.kali.org/downloads/
2. Choose the appropriate version for your system architecture (32-bit or 64-bit) and download the Kali Linux ISO image.

Step 2: Create a New Virtual Machine

1. Open VirtualBox.
2. Click on the "New" button in the toolbar.
3. Enter a name for your virtual machine (e.g., "Kali Linux"), select "Linux" as the type, and choose "Debian" as the version. Click "Next."
4. Allocate memory (RAM) for the virtual machine. Recommended minimum is 2048 MB (2 GB). Click "Next."
5. Choose to create a virtual hard disk now and click "Create."
6. Select the hard disk file type. The default "VDI" should be suitable. Click "Next."
7. Choose between dynamically allocated and fixed size for the virtual hard disk. Dynamically allocated is usually sufficient. Click "Next."
8. Specify the size of the virtual hard disk. At least 20 GB is recommended for Kali Linux. Click "Create."

Step 3: Attach Kali Linux ISO to the Virtual Machine

1. With the new virtual machine selected in the VirtualBox Manager, click on "Settings."
2. Go to the "System" tab and move the "Hard Disk" option to the top of the boot order.
3. Go to the "Storage" tab.
4. Under the "Controller: IDE" section, click on the empty disk icon next to "Controller: IDE."
5. In the Attributes section, click on the disk icon next to "Optical Drive" and choose "Choose a disk file."
6. Navigate to the location where you downloaded the Kali Linux ISO and select it. Click "OK."

Step 4: Install Kali Linux

1. Start the virtual machine by clicking "Start" in the VirtualBox Manager.
2. The Kali Linux installer will boot. Select "Install" from the boot menu and press Enter.
3. Follow the on-screen instructions to complete the Kali Linux installation. You'll be prompted to select language, location, keyboard layout, etc.
4. When prompted to configure the network, provide the necessary information.
5. During the installation process, you'll be prompted to set up users and passwords. Follow the prompts and complete the installation.
6. Once the installation is complete, the system will prompt you to remove the installation media. Press Enter, and the virtual machine will restart.
7. After the restart, you'll be presented with the Kali Linux login screen. Log in with the credentials you created during the installation.

## What is Metasploitable 2?

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

## How to install?

Step 1: Download Metasploitable 2

1. Visit the following GitHub repository to download Metasploitable 2: https://github.com/rapid7/metasploitable2
2. Click on the green "Code" button and choose "Download ZIP" to download the repository as a ZIP file.
3. Extract the contents of the ZIP file to a location on your computer.

Step 2: Import Metasploitable 2 into VirtualBox

1. Open VirtualBox.
2. Click on "File" in the menu and select "Import Appliance."
3. In the "Import Virtual Appliance" window, click on the folder icon to browse for the Metasploitable 2 OVA file. The OVA file is usually located in the folder you extracted from the ZIP file.
4. Select the Metasploitable 2 OVA file and click "Open."
5. Review the appliance settings, and if everything looks fine, click "Import."
6. The import process will take some time. Once it's done, you should see Metasploitable 2 listed in your VirtualBox Manager.

Step 3: Configure Metasploitable 2

1. With Metasploitable 2 selected in the VirtualBox Manager, click on "Settings."
2. Go to the "Network" tab.
3. Make sure that "Adapter 1" is enabled, and select "NAT" as the Attached to option. This allows Metasploitable 2 to access the internet.
4. Optionally, you can add another network adapter by clicking the "+" icon. Select "Host-only Adapter" to allow communication between your host machine and Metasploitable 2.
5. Click "OK" to save the settings.

Step 4: Start Metasploitable 2

1. With Metasploitable 2 selected in the VirtualBox Manager, click on "Start."
2. The Metasploitable 2 virtual machine will boot up. You'll see various startup messages.
3. Once the boot process is complete, you'll be presented with the Metasploitable 2 login screen.

Step 5: Explore and Practice

1. Log in to Metasploitable 2 using the default credentials.
2. You can now explore the vulnerable services and applications on Metasploitable 2. Use security tools like Metasploit to practice penetration testing in a controlled environment.