

# Assignment 2

## Hacker lab setup

### TASKS:

The given tasks is to download one attacker machine which I've downloaded was KALI Linux and a Victim machine which is Metasploitable 2.

There are several methods to download these OS. The method which I've chosen was to install a virtualbox and then installing the Kali Linux and Metasploitable 2.

### STEPS:

Here are the steps which I've followed while installing Kali Linux and Metasploitable2.

#### Step 1 - Download the VirtualBox:

Go to the Virtualbox website and download the version of virtualBox appropriate for your operating system. Follow the installation instructions provided for your platform.

#### Step 2 - Download a Linux Distribution:

Choose a Linux distribution that you want to install. Popular choices include Ubuntu, Fedora, Debian, and CentOS. The Linux I've downloaded was Kali Linux. Download the ISO image of the distribution from their respective websites.

#### Step 3 - 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, select the type as "Linux," and choose the version that matches your Linux distribution (e.g., Ubuntu 64-bit).
4. Allocate the amount of RAM you want to assign to the virtual machine. It's recommended to allocate at least 1-2 GB, depending on your system's resources.
5. Create a virtual hard disk. Choose the default options unless you have specific requirements.

#### Step 4 - Configure Virtual Machine Settings:

1. Select the virtual machine you just created and click on "Settings."
2. Under the "System" tab, make sure the boot order includes "Optical" before "Hard Disk."
3. Under the "Storage" tab, click on the empty disk next to "Controller: IDE" or "Controller: SATA," then click the disk icon and choose "Choose a disk file." Browse to the Linux ISO you downloaded earlier.
4. Optionally, you can adjust other settings like network adapters, display, etc., according to your needs.

#### Step 5 - Install Linux:

1. Start the virtual machine by selecting it from the VirtualBox manager and clicking on the "Start" button.
2. The virtual machine will boot from the Linux ISO you attached. Follow the

installation prompts provided by the Linux distribution's installer.

3. When prompted, select the option to install Linux, and follow the on-screen instructions to complete the installation process.
4. After installation, the virtual machine will likely prompt you to restart. Go ahead and restart it.
5. After rebooting, you should be greeted with your Linux distribution's login screen.

## **Download Metasploitable 2:**

### **1. Install VirtualBox:**

If you haven't already, download and install VirtualBox from the official website: [VirtualBox Downloads](#).

### **2. Import Metasploitable into Virtual Box:**

- Launch VirtualBox.
- Go to "File" > "Import Appliance".
- Browse and select the downloaded Metasploitable 2 VM file.
- Click "Next" and then "Import".

### **3. Configure Metasploitable 2 VM:**

- Once imported, select the newly imported VM in VirtualBox.
- Click on "Settings".
- Adjust settings if necessary, such as RAM and CPU allocation. Metasploitable 2 doesn't require high specifications, but you may adjust based on your system resources.
- Ensure the network settings are as per your requirement. Typically, you would want it to be on NAT or Bridged network mode for internet access.
- Click "OK" to save the settings.

### **4. Start Metasploitable 2 VM:**

- Select the Metasploitable 2 VM from the VirtualBox main window.
- Click on the "Start" button.

### **5. Explore and Use Metasploitable 2:**

- Once the VM boots up, you'll see instructions for accessing it.
- Follow the instructions to log in and start using Metasploitable 2.
- Metasploitable 2 is intentionally vulnerable, so be cautious while using it and avoid exposing it to the internet without proper precautions.

### **6. Update and Secure:**

- After you have it running, ensure that you don't connect it to any network where it could be accessed by unauthorized individuals.
- Metasploitable 2 is intentionally insecure and should only be used in controlled environments for testing and learning purposes.
- If there are any available updates or patches for the VM, make sure to apply them to minimize security risks.

That's it! You should now have Metasploitable 2 running in VirtualBox on your system. Remember to use it responsibly and ethically for educational and testing purposes only.

Here, after setting the attacker machine and vulnerable machine, we can use these machines to test and exploit the methods in the following tasks.

### The following is the sample of running Kali Linux and Metasploitable 2.

