Hacking lab setup and installation of kali linux and metasploitable machines.

Prepared By- Ayush Mathur

Executive Summary:

We are going to set up a hacker lab so we need one hacker machine like linux and 1 victim machine . Now we are going to download linux and metasploitable 2.

Assessment criteria:

1- Virtualbox (how to install linux)

Step 1: Download 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. 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.

2 – metasploitable 2 (how to install)

As of my last update, Metasploitable 2 is a deliberately vulnerable virtual machine designed for practicing penetration testing and learning about security vulnerabilities. Here's a general guide on how to set it up in VMware:

1. Download Metasploitable 2:

You can find the Metasploitable 2 VM on various sources online. It's important to download it from a trusted source. The file will typically be in OVA format, compatible with VMware.

2. Install VMware:

If you haven't already, download and install VMware Workstation Player or VMware Workstation Pro. Both are suitable for running virtual machines on your system.

3. Import Metasploitable 2 into VMware:

- Open VMware.
- Go to "File" > "Open" or "Import".
- Browse to the location where you downloaded the Metasploitable 2 OVA file.
- Select the file and follow the prompts to import it.

4. Configure Virtual Machine Settings:

- Once imported, select the Metasploitable 2 virtual machine from the library.
- Check its settings, such as RAM allocation, CPU cores, network adapter settings, etc. You can adjust these based on your system resources and requirements.

5. Network Configuration:

- Metasploitable 2 has intentionally vulnerable services running on it, so it's important to isolate it from your main network.
- Configure the network adapter of the Metasploitable 2 VM to use a "Host-only" or "NAT" network in VMware settings. This prevents it from being directly accessible from the internet or your main network.

6. Start the Virtual Machine:

- Once configured, start the Metasploitable 2 VM from VMware.

7. Accessing Metasploitable 2:

- After booting up, the VM will show you an IP address. Note down this IP address as you'll need it to connect to the Metasploitable 2 instance.
- You can then use various penetration testing tools and techniques to exploit the vulnerabilities present on the Metasploitable 2 system.

8. Security Precautions:

- **Since Metasploitable 2 is intentionally vulnerable, ensure that you use it responsibly and only in a controlled environment.**
- **Never expose Metasploitable 2 to an untrusted network or the internet without proper precautions.**