Complete Setup Guide: Metasploitable 2 in VirtualBox with Kali Linux

Step 1: Download VirtualBox

Visit the official VirtualBox website at https://www.virtualbox.org. Download the version that matches your operating system (Windows, macOS, or Linux). Once downloaded, open the installer and follow the on-screen instructions using the default options. After installation, launch VirtualBox to verify it's working correctly.

Step 2: Download Metasploitable 2

Navigate/Click to https://download.vulnhub.com/metasploitable/metasploitable-linux-2.0.0.zip to download Metasploitable 2. This will download a ZIP file containing the virtual machine. Once downloaded, extract the contents to a folder on your computer. You should see a VMDK file which is the virtual disk for the VM.

Step 3: Import Kali Linux into VirtualBox

If you don’t already have Kali Linux installed in VirtualBox, download the official .ova file from https://www.kali.org/get-kali/. In VirtualBox, go to File > Import Appliance, select the Kali .ova file, and follow the prompts. This will set up a ready-to-use Kali VM in VirtualBox.

Step 4: Create VM for Metasploitable 2

To create the Metasploitable 2 VM, click on 'New' in VirtualBox. Enter the name 'Metasploitable2'. Set the Type to 'Linux' and Version to 'Ubuntu (32-bit)'. Click Next and allocate at least 512MB of RAM. In the hard disk step, choose 'Use an existing virtual hard disk file', then browse to and select the extracted VMDK file from Step 2.

Step 5: Set Network: Adapter 1 (Host-only), Adapter 2 (NAT cyberlabs)

Before starting the VMs, configure the network for proper communication. For both Kali and Metasploitable2, go to Settings > Network. For Adapter 1, choose 'Host-only Adapter'. This allows internal communication between the two VMs. For Adapter 2, choose 'NAT

Network' and select the pre-configured 'cyberlabs'. This setup provides internet access if needed while isolating the lab environment from your host system.

Step 6: Start Kali and Metasploitable 2

Start the Kali Linux VM and let it boot up. Log in using username: kali and password: kali. Do the same for Metasploitable 2 by selecting it and clicking Start. When prompted on the terminal screen, log in using username: msfadmin and password: msfadmin. You should now be inside the Metasploitable terminal.

Step 7: Ping Metasploitable 2 from Kali

To test if both machines are connected, open a terminal in Kali. First, find Metasploitable's IP address by typing `ifconfig` in the Metasploitable terminal. Then, in Kali, type `ping `. If you receive replies, the connection is successful and your lab environment is properly set up.

Step 8: Login to Metasploitable 2 using msfadmin/msfadmin

After logging into Metasploitable 2, you will be presented with a command-line terminal. This indicates that the system is up and ready for testing. This machine is intentionally vulnerable for ethical hacking practice. It is unsafe to connect Metasploitable to a public network.