# Install Metasploitable 2

Activities

[Install Metasploitable 2 1](#_Toc90794199)

[How to Create Screenshots 1](#_Toc90794200)

[Install Metasploitable 2 1](#_Toc90794201)

[Assignment Submission 2](#_Toc90794202)

Time needed: 30 Minutes

# Install Metasploitable 2

Time Required: 30 minutes

Objective: Install Metasploitable 2

Description: In this activity, you will install a Linux distribution that is designed to be use as a practice machine for penetration testing.

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

1. Download **Metasploitable 2**:  
   <https://sourceforge.net/projects/metasploitable/>
2. Extract the zip file.
3. Start VirtualBox. Create a new Virtual Machine.
   1. Name: **Metasploitable 2**
   2. Type: **Linux**
   3. Version: **Other Linux (64-bit)**
   4. Memory size: **512 MB**
   5. Hard disk: Use an existing virtual hard disk file. Browse to where you unzipped the Metasploitable 2 download.
   6. Attach: **Metasploitable.vmdk**
4. Start the new VM.
5. Logon with Username: **msfadmin** password: **msfadmin**
6. Run **ip a** to find the IP address of the Metasploitable server
7. Ping the server from your Kali machine.
8. Insert a screenshot.

Click or tap here to enter text.

1. Go to the web server on the Metasploitable server from Kali by typing in the IP address into a browser address bar.
2. Insert a screenshot of your options.
3. Shut down Metasploitable: **sudo poweroff**

Click or tap here to enter text.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.