Metasploitable 2 Installation

Activities

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.
    a. Name: **Metasploitable 2**
    b. Type: **Linux**
    c. Version: **Other Linux (64-bit)**
    d. Memory size: **256 MB**
    e. Hard disk: Use an existing virtual hard disk file. Browse to where you unzipped the Metasploitable 2 download.

    f. Attach: **Metasploitable.vmdk**

4. Connect this VM to your EthicalHacking NAT Network.
5. Start the new VM.
6. Logon with Username: **msfadmin** password: **msfadmin**
7. Run **ip a** to find the IP address of the Metasploitable server.
8. To get out of the Metasploitable server to your computer → press the right CTRL key
9. Connect your Kali Linux VM to your EthicalHacking NAT network.
10. Ping the server from your Kali machine.
11. Go to the web server on the Metasploitable server from Kali by typing in the IP address of the Metasploitable server into a browser address bar.
12. Capture a screenshot of the Metaploitable server.
13. Shut down Metasploitable: **sudo poweroff**

Assignment Submission

Attach the screenshot showing the Metasploitable 2 server to the assignment in Blackboard.