Metasploitable 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

Downloading and Setting Up Metasploitable 2

The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

The compressed file is about 800 MB and can take up to 30 minutes to download. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see its contents.

Powering on Metasploitable 2

Once the VM is available on your desktop, open the device, and run it with VMWare Player. Alternatively, you can also use VMWare Workstation or VMWare Server.

Logging in to Metasploitable 2

The login for Metasploitable 2 is `msfadmin:msfadmin` .

Identifying Metasploitable 2's IP Address

After you log in to Metasploitable 2, you can identify the IP address that has been assigned to the virtual machine. Just enter `ifconfig` at the prompt to see the details for the virtual machine.

```
msfadmin@metasploitable:~$ ifconfig
```

The command will return the configuration for eth0. You'll need to take note of the inet address. This will be the address you'll use for testing purposes.

Help with Metasploitable 2

For more information on Metasploitable 2, check out this handy guide written by HD Moore.