Installing metasploitable2 Assignment Report

Prepared by: Adarsh Tiwari

Date: 29/02/2024

Client: XYZ Corporation

Executive Summary:

Metasploitable2 is a vulnerable Linux machine. Which can be used by students and learners to practice the basic cyber security attacks and vulnerabilities

1. Download Metasploitable 2:

2. Extract the downloaded file:
The file will likely be in a compressed format (e.g., .zip). Extract it using a suitable tool like WinRAR or 7Zip.

3. Open VirtualBox and create a new VM:
Launch VirtualBox. Click the "New" button to create a new virtual machine.

4. Configure VM settings:

Provide a name for your VM (e.g., "Metasploitable2").
Select "Linux" as the type and "Other Linux (32-bit)" as the version (assuming the downloaded image is 32-bit).
Allocate memory (RAM) based on your system resources, typically 1024 MB (1 GB) is sufficient.
Create a virtual hard disk, choose "VDI (VirtualBox Disk Image)" as the type and dynamically allocated storage for flexibility.

5. Import the downloaded appliance (optional):

If the downloaded file is a pre-configured appliance file (.ova), you can import it directly into VirtualBox by selecting "Import Appliance" from the "File" menu.

6. Start the VM:

Select the created VM and click the "Start" button.

7. Login and configure Metasploitable 2:

During the first boot, follow the on-screen instructions to complete the setup process. This might involve setting a username and password.

Once logged in, update the system and install any necessary packages following the official documentation (no longer available online, search at your own risk).