

Cybersecurity Lab Setup Documentation

Week 1: Introduction to Cybersecurity and Virtualization

Task Overview

The objective was to set up a virtual cybersecurity lab using virtualization software. This included creating virtual machines for Kali Linux and Metasploitable, configuring networking, and performing initial reconnaissance on Metasploitable.

Steps Performed

Step 1: Install Virtualization Software

Installed Oracle VirtualBox on the host machine.

Step 2: Download Required Files

Downloaded the latest version of Kali Linux ISO from the official website.
Downloaded Metasploitable from the official repository.

Step 3: Create Virtual Machines

Kali Linux VM Setup:

1. Opened VirtualBox and created a new virtual machine named "Kali Linux."
2. Allocated resources:
 - RAM: 4 GB
 - Disk Space: 50 GB
3. Attached the downloaded Kali Linux ISO file to the virtual CD/DVD drive.
4. Installed Kali Linux by following the installation instructions.

Metasploitable VM Setup:

1. Created a new virtual machine named "Metasploitable."
2. Allocated resources:
 - RAM: 512 MB
 - Disk Space: 8 GB
3. Attached the downloaded Metasploitable ISO file to the virtual CD/DVD

drive.

4. Started the Metasploitable VM and verified default credentials:

- Username: msfadmin
- Password: msfadmin

Step 4: Configure Networking

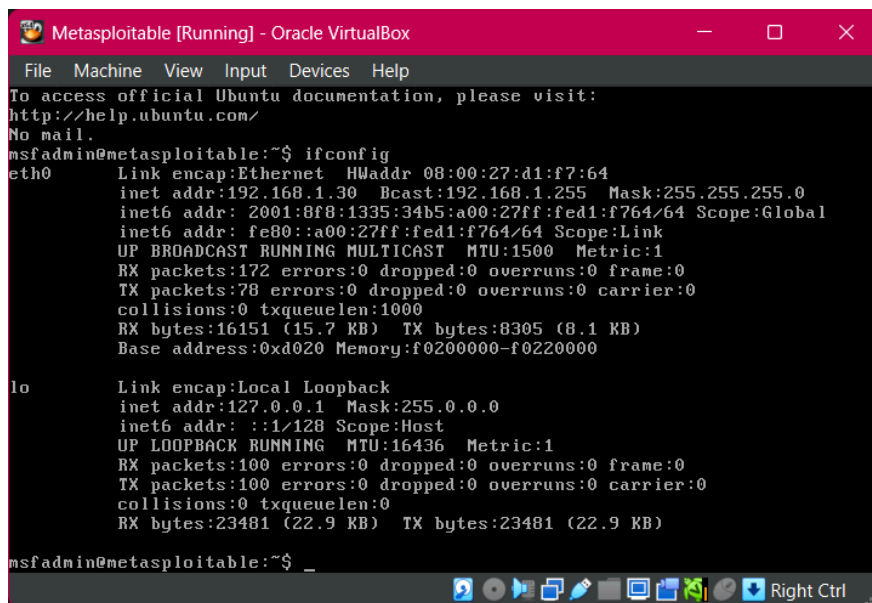
Set both Kali Linux and Metasploitable VMs to use a bridged network adapter to allow communication between the VMs.

Step 5: Identify Metasploitable's IP Address

1. Logged into the Metasploitable VM.

2. Ran the command:

`ifconfig`



```
Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d1:f7:64
          inet addr:192.168.1.30  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr:  2001:8f8:1335:34b5:a00:27ff:fed1:f764/64  Scope:Global
          inet6 addr:  fe80::a00:27ff:fed1:f764/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:172 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16151 (15.7 KB)  TX bytes:8305 (8.1 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr:  ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$ _
```

3. Noted the IP address of the eth0 interface (e.g., 192.168.1.29).

Step 6: Perform Initial Reconnaissance

1. Logged into the Kali Linux VM.

2. Used nmap to scan Metasploitable:

`nmap -A 192.168.1.29`

3. Collected details about open ports and services.

Findings from Reconnaissance

Scan Results for Metasploitable (IP: 192.168.1.29):

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 08:00:27:D1:F7:64 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Deliverables

1. A fully functional cybersecurity lab with Kali Linux and Metasploitable.
2. Documentation of the setup process, including configuration details.
3. A report on initial reconnaissance findings:
 - Open ports and services.
 - Observations on potential vulnerabilities.

Conclusion

The lab setup was completed successfully, and reconnaissance on Metasploitable was performed. The findings provide a foundation for further cybersecurity testing and learning.