Cybersecurity Lab Setup Documentation

Index

1. Introduction

This document provides a step-by-step guide to setting up a virtual cybersecurity lab using **Kali Linux** and **Metasploitable** on a virtualization platform (VMware/VirtualBox). The lab will allow for penetration testing and cybersecurity practice.

Setting up a cybersecurity lab provides a controlled environment for ethical hacking, penetration testing, and security research.

Kali Linux is a widely used penetration testing operating system, while Metasploitable is a intentionally vulnerable machine designed for security testing.

By following this guide, you will learn how to install and configure these virtual machines, establish a network for testing, and conduct basic reconnaissance to identify potential weaknesses. This lab setup will provide hands-on experience with essential cybersecurity tools, helping you develop practical skills in ethical hacking and security analysis.

2. Prerequisites

Before proceeding, ensure you have the following:

- A system with **at least 8GB RAM** and **100GB free disk space**
- Virtualization software: **VirtualBox** or **VMware Workstation**
- Kali Linux ISO file: Download from Official Site
- Metasploitable VM file: Download from official site

3. Setting Up Virtualization Software

Installing VirtualBox/VMware

1. Download and install **VirtualBox** from VirtualBox Official Site.
2. If using **VMware Workstation**, install it from VMware Official Site.
3. Verify installation by launching the software.

4. Setting Up Kali Linux

Creating a Virtual Machine

1. Open **VirtualBox/VMware** and select **New VM**.
2. Name it "Kali Linux", set **Type: Linux**, and **Version: Debian (64-bit)**.

3. Allocate **4GB RAM** and **50GB virtual hard disk** (VDI/VMDK format, dynamically allocated).
4. Attach the **Kali Linux ISO** under the virtual CD/DVD drive.
5. Start the VM and follow the **on-screen installation instructions**.
6. Create a username/password and install the system.

Updating Kali Linux

After installation, update the system:

```
sudo apt update && sudo apt upgrade -y
```

Install required tools:

```
sudo apt install nmap net-tools metasploit-framework -y
```

5. Setting Up Metasploitable

Creating a Metasploitable VM

1. Open **VirtualBox/VMware** and create a **New VM**.
2. Name it "Metasploitable", set **Type: Linux**, and **Version: Ubuntu (32-bit)**.
3. Allocate **512MB RAM** and **8GB virtual hard disk**.
4. Attach the **Metasploitable ISO** under the virtual CD/DVD drive.
5. Start the VM and log in using the default credentials:

```
Username: msfadmin
Password: msfadmin
```

6. Configuring Networking

Setting Up a Bridged Network

To allow communication between Kali Linux and Metasploitable:

1. Open VirtualBox/VMware settings for **both VMs**.
2. Under **Network**, select **Bridged Adapter**.

3. Restart both VMs and find their IP addresses:

```
ifconfig    # On Metasploitable
ip a        # On Kali Linux
```

4. Note the **IP addresses**.

7. Performing Initial Reconnaissance

Finding Open Ports and services on Metasploitable

From Kali Linux, run an Nmap scan to detect open ports and services:

```
nmap -A –T4 <Metasploitable-IP>
```

We will get the open ports and services in Metasploit like this :

```
┌──(root㉿vbox)-[/home/kali]
└─# sudo nmap -A -T4 192.168.1.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 16:51 IST
Warning: 192.168.1.3 giving up on port because retransmission cap hit (6).
Stats: 0:04:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 88.83% done; ETC: 16:56 (0:00:01 remaining)
Nmap scan report for 192.168.1.3
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
110/tcp  open  pop3?
| fingerprint-strings:
|   NULL:
|_    -ERR Can not connect to e-mail server. Error:100502
111/tcp  open  rpcbind     2 (RPC #100000)
```