Internship Assessment: Setting Up Hacker Lab with Linux and Metasploitable 2- Week 2

Intern Name: PRASAD PUND

Objective:

The objective of this report is to provide a comprehensive guide on setting up a hacker lab environment using VMware Workstation Player, including the installation of Linux and Metasploitable 2 virtual machines (VMs). This guide aims to facilitate practical learning in penetration testing and security vulnerability assessment.

1. Setting Up Linux VM:

1.1. Download VMware Workstation Player:

Obtain VMware Workstation Player from the VMware website and install it on your system.

1.2. Download Linux ISO:

Choose a Linux distribution debian and download the ISO image from the respective website.

1.3. Create a New Virtual Machine:

Launch VMware Workstation Player and navigate to "File" -> "New Virtual Machine."

Select "Typical" configuration type.

1.4. Select Installer Disk Image (ISO):

Browse and select the downloaded Linux ISO file.

Proceed with the installation wizard.

1.5. Choose Linux Operating System:

VMware Player will automatically detect the operating system, or you can manually select the Linux version.

1.6. Name Your Virtual Machine:

Provide a name and location for the virtual machine files.

1.7. Specify Disk Capacity:

Choose disk size and storage options as per your requirements.

1.8. Customize Hardware (Optional):

Adjust hardware settings such as RAM, CPU cores, and network adapters if needed.

1.9. Install Linux:

Start the virtual machine and follow on-screen instructions to install Linux.

Configure language, timezone, keyboard layout, disk partitioning, and user account.

Complete the installation and restart the virtual machine.

2. Setting Up Metasploitable 2:

2.1. Download Metasploitable 2:

Obtain the Metasploitable 2 VM from a trusted source. Ensure it's in OVA format compatible with VMware.

2.2. Install VMware:

If not installed, download and install VMware Workstation Player or VMware Workstation Pro.

2.3. Import Metasploitable 2 into VMware:

Open VMware and import the Metasploitable 2 OVA file.

Follow the prompts to complete the import process.

2.4. Configure Virtual Machine Settings:

Adjust settings such as RAM allocation, CPU cores, and network adapter to suit your requirements.

2.5. Network Configuration:

Configure the network adapter of Metasploitable 2 VM to use "Host-only" or "NAT" network for isolation.

2.6. Start the Virtual Machine:

Launch the Metasploitable 2 VM from VMware.

2.7. Accessing Metasploitable 2:

Note down the assigned IP address displayed on the VM.

Utilize penetration testing tools and techniques to exploit vulnerabilities on Metasploitable 2.

2.8. Security Precautions:

Use Metasploitable 2 responsibly and only in a controlled environment.

Avoid exposing it to untrusted networks or the internet without proper precautions.

Adhere to ethical guidelines and legal regulations while using vulnerable systems.

Conclusion:

This report provides a step-by-step guide for setting up a hacker lab environment using VMware Workstation Player. By following these instructions, users can install Linux and Metasploitable 2 VMs, facilitating hands-on practice in penetration testing and security assessment.