Subject: Cybersecurity Lab Setup and Exploitation - Internship Report

PREPARED BY: DAFE FRANK

I am excited to share the successful completion of my first internship task involving the setup and exploitation of a cybersecurity lab environment. In this report, I will provide a comprehensive overview of the steps I took, the tools used, and the outcomes achieved.

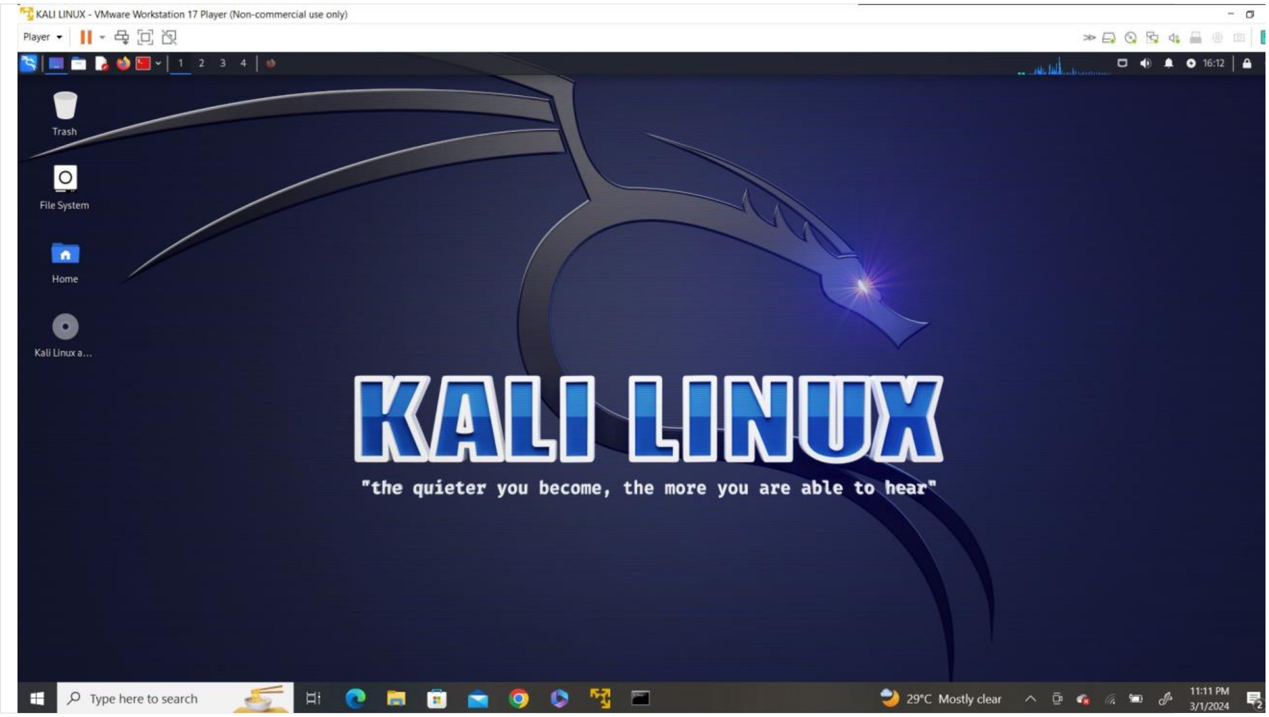
## Task Overview:

The primary objective was to establish a hacker lab environment for practicing cybersecurity skills. The setup included configuring Kali Linux as the attacker machine using VMware Workstation Player and Metasploitable 2 as the victim machine.

## Steps Taken:

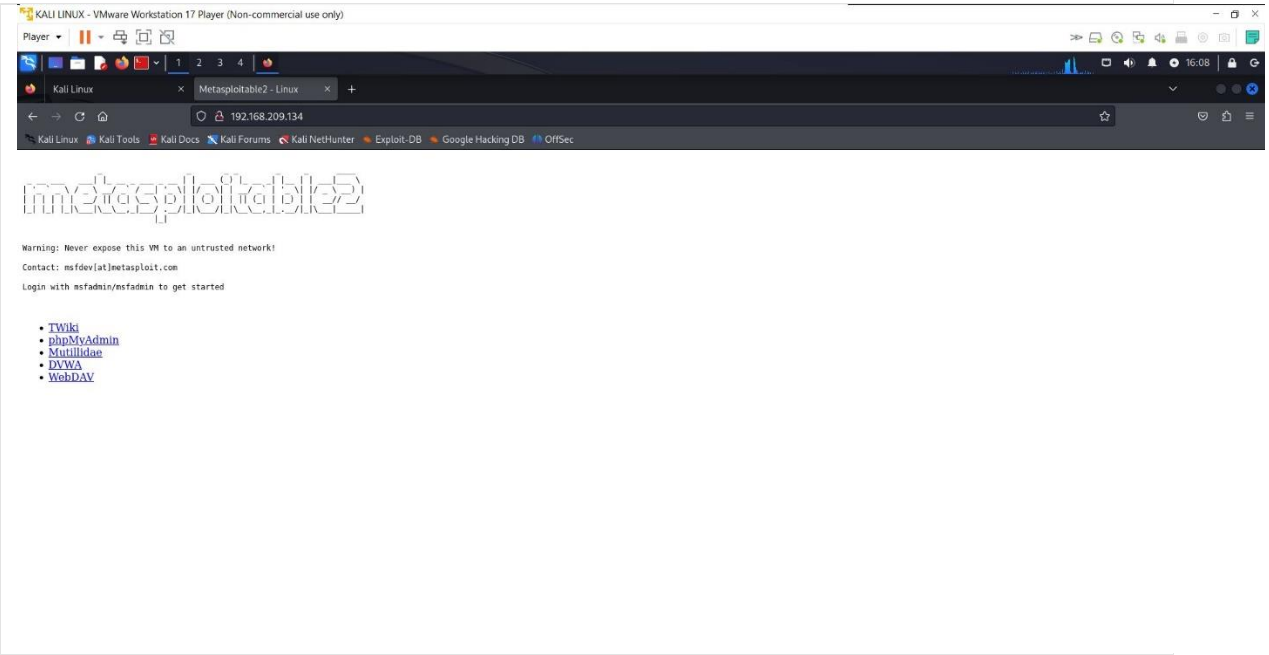
1. Installing Kali Linux on VMware Workstation Player:

- Downloaded and installed VMware Workstation Player from the official website.
- Selected Kali Linux as the attacker machine, downloading the ISO image from the Kali Linux website.
- Created a new virtual machine, specifying the Linux distribution, and allocated appropriate resources.
- Configured the virtual machine settings, including RAM and CPU allocation.
- Installed Kali Linux by booting from the ISO, following the on-screen instructions.


KALI LINUX - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
Kali Linux a...
16:12
KALI LINUX
"the quieter you become, the more you are able to hear"
Type here to search
29°C Mostly clear
11:11 PM
3/1/2024

## 2. Setting Up Metasploitable 2:

- Downloaded Metasploitable 2 from a reputable source.
- Installed VMware Workstation Player.
- Imported Metasploitable 2 into VMware using the provided OVA file.
- Configured the virtual machine settings, ensuring network isolation for security.
- Started the virtual machine and noted its IP address.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

3. Exploitation and Penetration Testing:

- Utilized Kali Linux tools, including Metasploit, Nmap, and other penetration testing tools.
- Explored and identified vulnerabilities on the intentionally insecure Metasploitable 2 environment.
- Executed penetration testing scenarios, demonstrating the ability to exploit vulnerabilities in a controlled environment.

## Challenges Faced:

During the setup and exploitation process, I encountered challenges related to:

- **Network Configuration:** Ensuring proper isolation between the attacker and victim machines.
- **Tool Familiarity:** Gaining proficiency with various penetration testing tools and understanding their optimal usage.

## Learning Outcomes:

This task provided valuable insights into the following areas:

- **Hands-on Experience:** Practical application of theoretical cybersecurity concepts.
- **Tool Proficiency:** Enhanced proficiency with tools such as Metasploit and Nmap.
- **Vulnerability Identification:** Ability to identify and exploit vulnerabilities in a controlled environment.

## Conclusion:

The successful completion of this task signifies a foundational step in developing practical cybersecurity skills. The hands-on experience gained during the setup and exploitation of the lab environment has deepened my understanding of penetration testing methodologies and tools.

I look forward to further tasks and challenges that will contribute to my growth and development in the field of cybersecurity.

Thank you for the opportunity, and I welcome any feedback or additional guidance.