Assignment 4

Mercy Ikem

8859960

PROG8291

Prof. Sajad Shahid

21st July 2024

Table of Contents

[**ASSIGNMENT 4** 2](#_Toc172281302)

[**Description** 2](#_Toc172281303)

[**Preparation** 2](#_Toc172281304)

[**Observation & Screenshot** 2](#_Toc172281305)

[WINDOWS 6](#_Toc172281306)

[**Reflection** 7](#_Toc172281307)

# **ASSIGNMENT 4**

## **Description**

In this lab, I set up three virtual machines, Kali Linux, ccVW (Windows), and Metasploitable. I added my name and my student ID’s last three digits to most of them for identification purposes. I established connectivity between them and used kali linux on both ccVW and Metasploitable to exploit vulnerabilities.

## **Preparation**

In this lab, I will use Oracle VirtualBox, metasploitable VM image, Kali Linux, and ccVW (Widows) images. I made sure they were all connected to the same network. I learnt how to use Oracle VirtualBox’s VM management interface. Finally, I went over the fundamentals of virtualization and networking. I used nmap to search for port and msfconsole.

## **Observation & Screenshot**

A screenshot of a computer

Description automatically generated

Figure 1 shows i can sucessfully ping my metasploitable machine from my kali linux.

A screenshot of a computer

Description automatically generated

Figure 2 shows that i could successfully ping my windows machine from my kali linux.

A screenshot of a computer

Description automatically generated

Figure 3 shows the IP address of my metasploitable machine.

A computer screen shot of a black screen

Description automatically generated

Figure 4 shows the IP address of my windows machine.

A screenshot of a computer

Description automatically generated

Figure 5 shows that i performed a port scan on my metaploitable using nmap of my kali linux.

A screenshot of a computer

Description automatically generated

Figure 6 shows the it displaying exploitation options on my kali machine.

A screenshot of a computer

Description automatically generated

Figure 7 shows i successfully exploited the Metasploitable machine and ran remote code through my kali Linux machine.

## WINDOWS

A screenshot of a computer

Description automatically generated

Figure 8 shows that i performed port scan on my windows machine using nmap on my kali machine.

A computer screen shot of a black screen

Description automatically generated

Figure 9 shows it displaying exploitation options on my kali linux.

A screenshot of a computer

Description automatically generated

Figure 10 shows i initated the exploitation process.

## **Reflection**

While examining Metasploitable, I noticed a lot of open ports when I used **nmap**, but I just concentrated on FTP and further scanned to find its vulnerability. I used the **unix/ftp/vsftpd backdoor exploit** with msfconsole to take total control of the Metasploitable instance. After switching to the windows virtual machine, even with multiple open ports, running a script that was vulnerable to the eternalblue exploit was discovered. I found and ran the relevant payload using **msfconsole,** which allowed me to successfully enter the Windows VM. The importance of careful reconnaissance, careful exploit selection, and efficient payload execution in penetration testing scenarios is highlighted by this procedure.