**Name: Bhavsar Dhwani**

**Student Id : 8867285**

**Date: 01/23/2024**

**Assignment 1**

# Subject: Computer and Application Security

**Task 1**

**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated

First screenshot shows the ip address of metaspoitable and another screenshot shows the ip address of kali using ifconfig command.

**Task 2**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In these two screenshots ,two virtual machines are communicating with each other using ping command.

**Task 3**

A screenshot of a computer

Description automatically generated

It shows the description about vsftpd version 2.3.4.

**Task 4**

A screenshot of a computer

Description automatically generated

This command is use to exploit targeting a specific vulnerability in the vsftpd 2.3.4 server.

**Task 5**

A screenshot of a computer

Description automatically generated

This command displays current configurations, available payload options and targeted exploit.

**Task 6**

**A screenshot of a computer

Description automatically generated**

This command is use to specify the target ip address for particular exploit.

**Task 7**

A screenshot of a computer

Description automatically generated

This command is used to execute the selected exploit.

**Task 8**

* What worked well for you

By doing this assignment, I got chance to enhance my knowledge about kali and Metasploitable and the use of VMWare in cyber security.

* What didn’t work well and how you resolved the issue(s)

Initially , It was confusing to use kali and Metasploitable framework together in VMWare as I don’t have much knowledge regarding this software. But after learning through webpages and videos provided on econestoga, It became interesting for me to learn more about cyber security.

* What is one thing that you were able to learn or accomplish through this Assignment that you did not know prior to starting.

By doing this assignment, I learned more regarding kali and it’s command as I was unaware of this before.

**References:**

<https://www.geeksforgeeks.org/how-to-link-kali-linux-with-metasploitable-2/>

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/