



Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals
Lab File – CA 11

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

Perform a practical to hack Metasploitable2 using Kali Linux.

Requirements :

- Virtualisation Software
- Kali Linux 2022.1
- Basics of Metasploit
- Internet Connection

Objectives :

To use modules and exploits to hack metasploitable2.

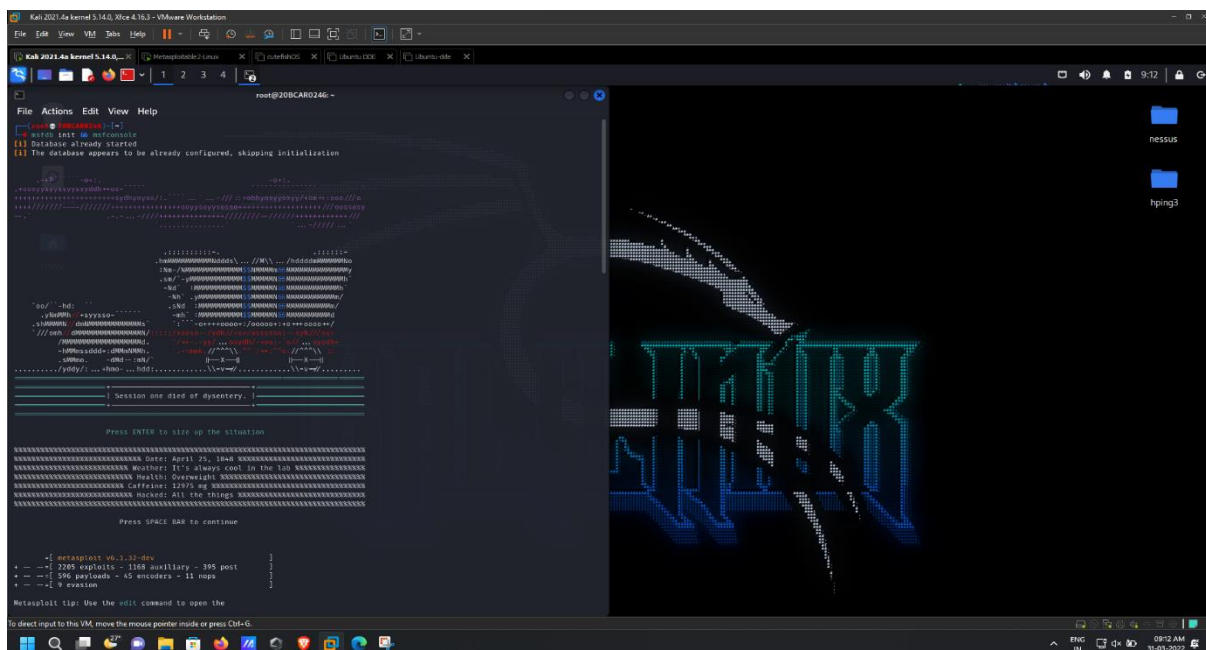
Procedure :

Introduction

Metasploit Framework is an open-source project that facilitates the task of attackers, exploit, aids in penetration testing, IDS sign development and payload writers. A major advantage of the framework is the modular approach, allowing the combination of any exploit with any payload.

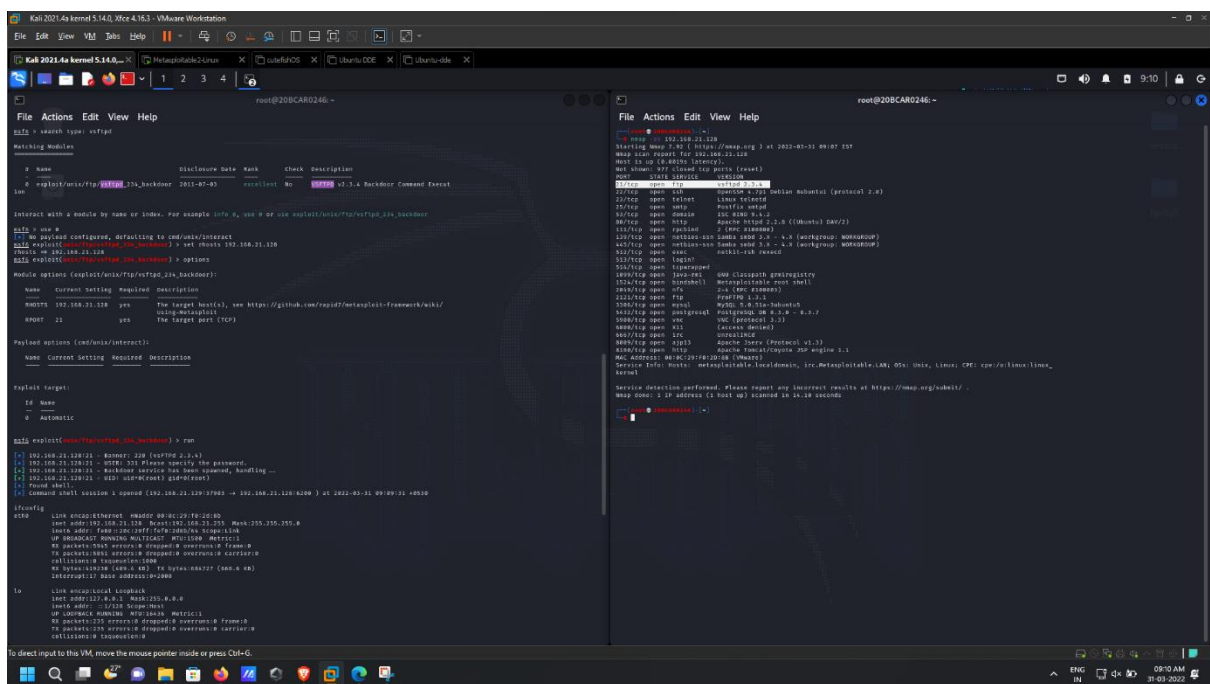
Basics

- 1> Since Metasploit comes pre-installed in Kali Linux, we are going to begin with searching it in Applications button and start with sudo password. Another way, is using the command `msfdb init && msfconsole` in the root terminal.



The window appears like this.

4> Hit Run. Try with `ipconfig` to cross-check if hacked or not.



In this practical, we were successfully able to get the shell access of the Metasploitable2 in Kali Linux using Metasploit framework. Using NMAP scan on the target helps us to get all the open ports on the target machine. Using MSFCONSOLE gives us the advantage of performing the exploits on the open ports of the target. In this lab, we were able to exploit backdoor command execution in VSFTPD v2.3.4. There are many more modules available in the Metasploit framework, which can be used to exploit other identified vulnerabilities.