

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 :**

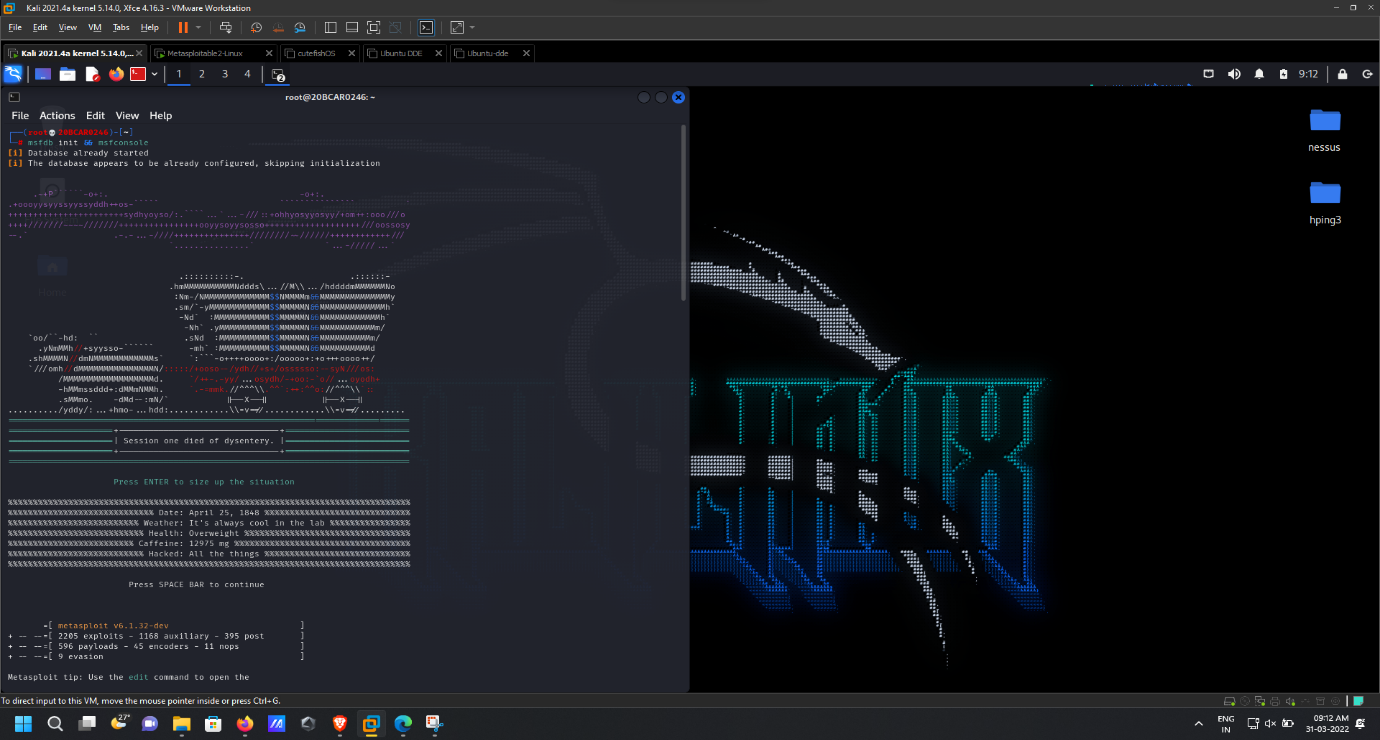
Introduction

Metasploit Framework is an open-source project that facilities the task of attackers, exploit, aids in penetration testing, IDS sign development and paylod 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.

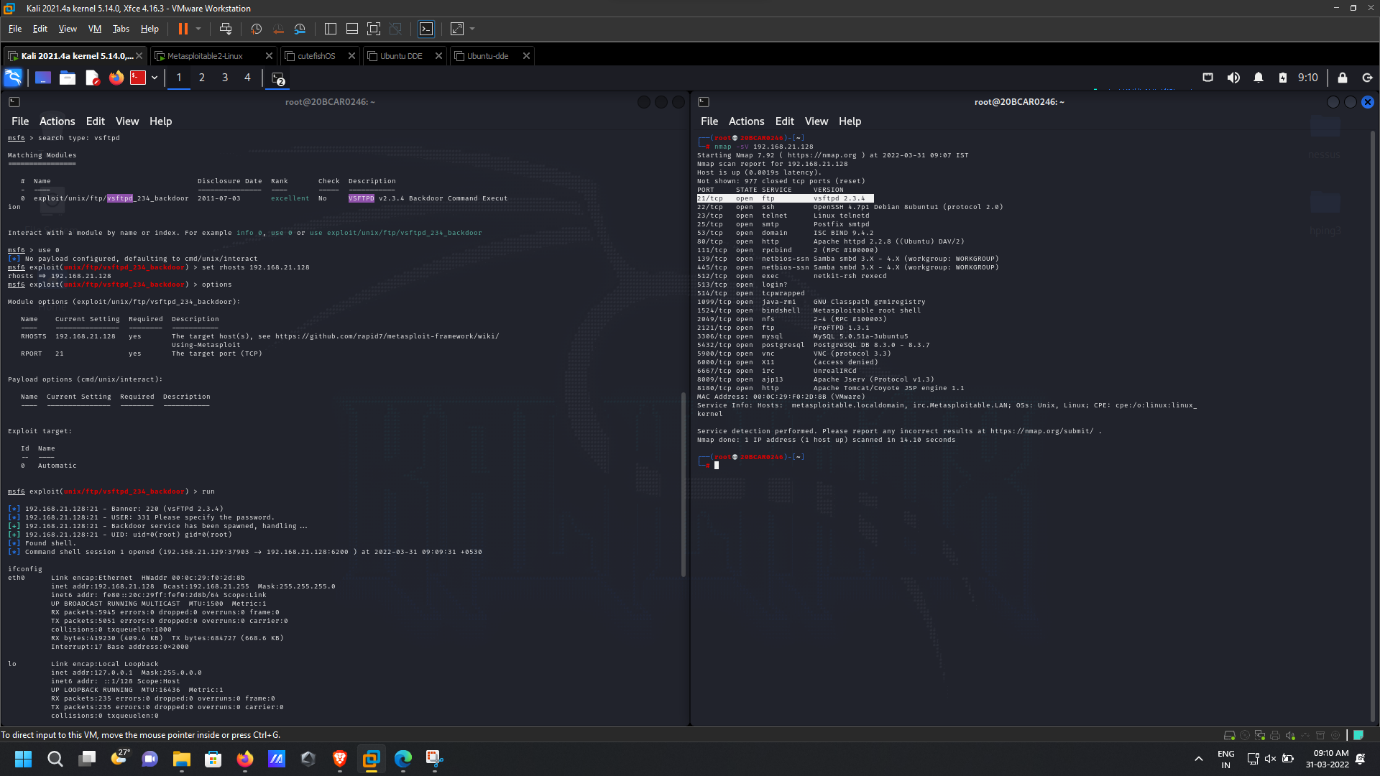


The window appears like this.

1. In Terminal, if we move to /usr/share/metasploit-framework/modules we can check the exploits database. Run nmap -sV <IP Address> to detect vulnerabilities in metasploitable2.
2. As we can see in the above image, port number 21/tcp is open and is providing FTP service, with the version, vsftpd 2.3.4.

So, now, we will search for the exploits for this service, and configure it accordingly to hack metasploitable2.

1. Hit Run. Try with ipconfig to cross-check if hacked or not.



**Conclusion :**

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.