Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals

Lab File – CA 05

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

Information Gathering Using Metasploit in Kali Linux

Requirements :

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

Objectives :

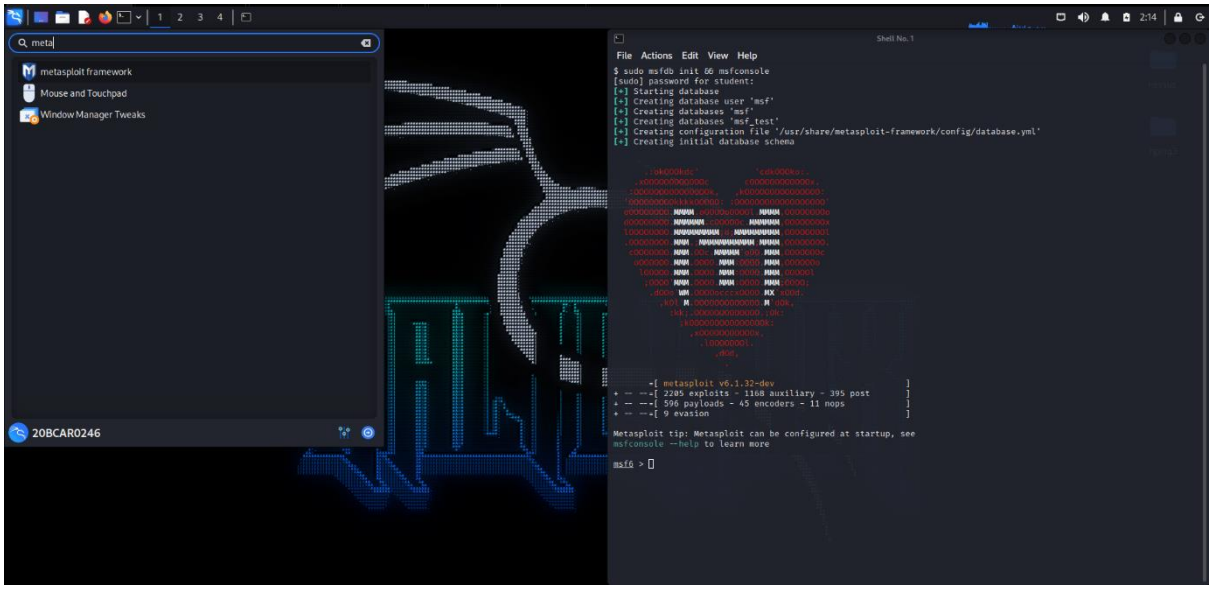
To Run Scans, like:

- ✓ Nmap Scan
- ✓ Axuiliary Scan

Procedure :

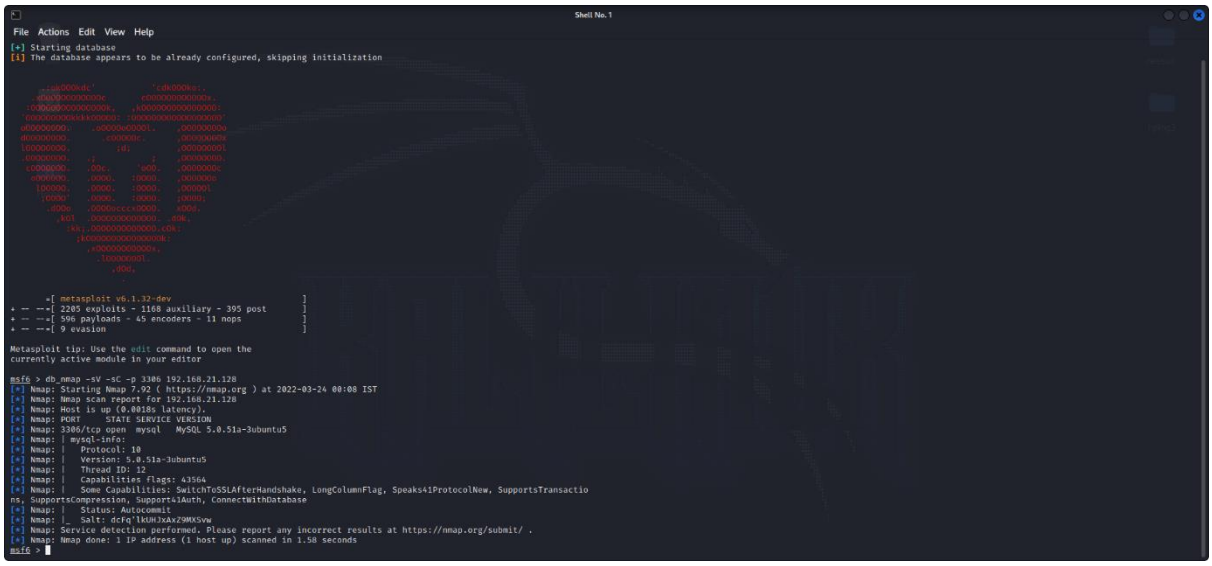
Basics

Since Metasploit comes pre-installed in Kali Linux, we are going to begin with searching it in Applications button and start with sudo password.

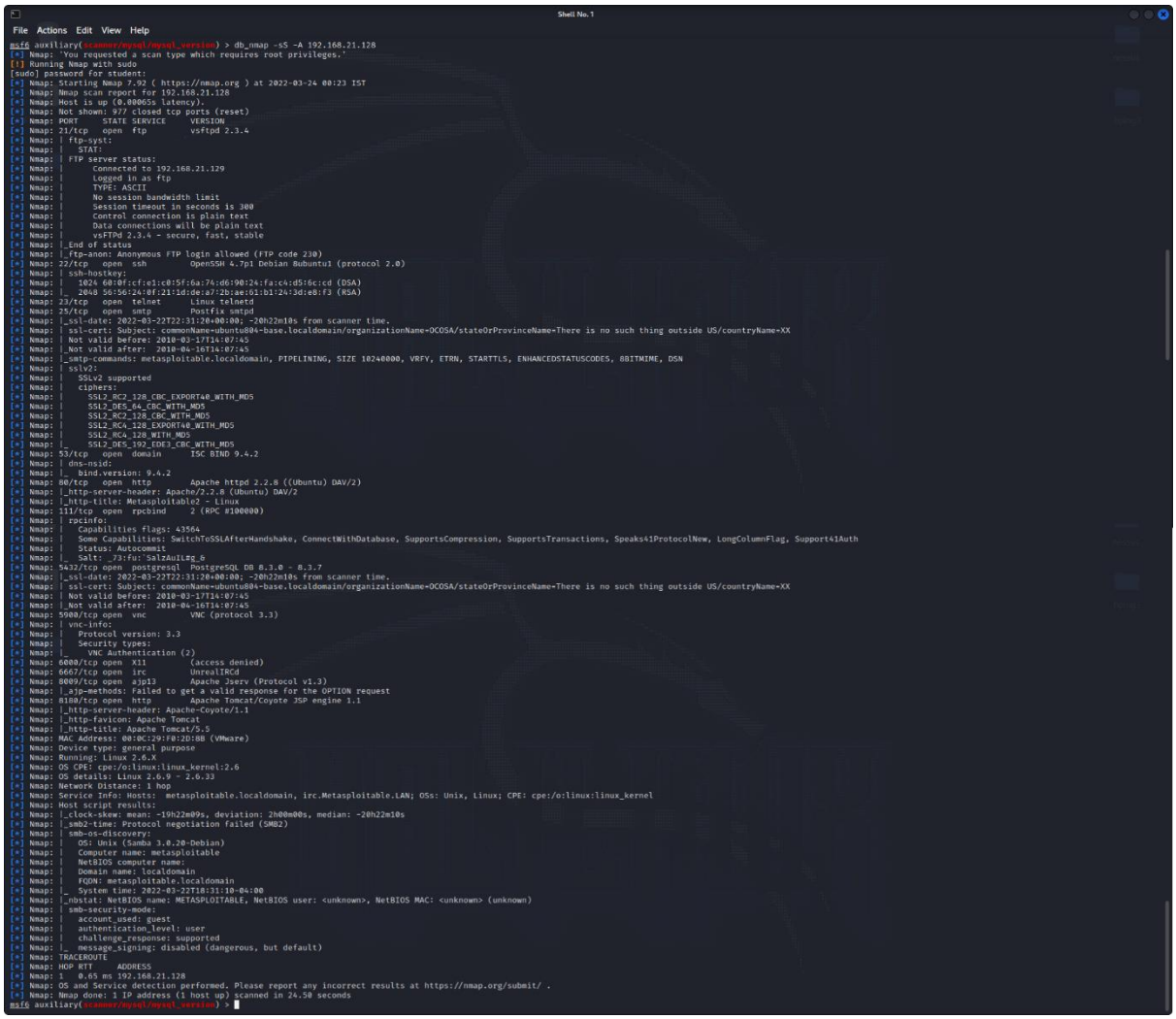


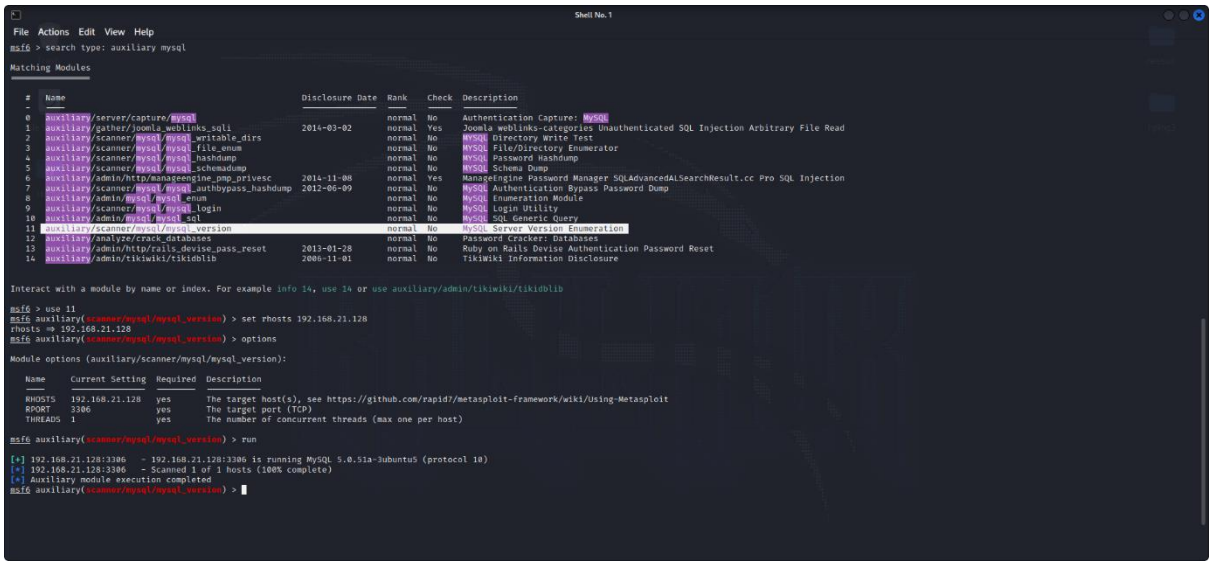
The window appears like this.

Command: db_nmap -sV -sC -p 3306 <IP Address>



Command: db_nmap -sS -A <IP Address>





Conclusion :

By using metasploit framework we learnt how to perform reconnaissance and information gathering on a host running mysql server and enumerate database running on the target machine.

The main purpose to perform information gathering / Reconnaissance of mysql version enumeration so that exploitation can be performed.

With the help of metasploitable2 and Metasploit framework we had demonstrated and learned lot to perform the mysql reconnaissance and information gathering with msfconsole and enumerate the database running on the target.