

Department of

Bachelor of Computer Applications

**Ethical Hacking Fundamentals**

Lab File – CIA 02

**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

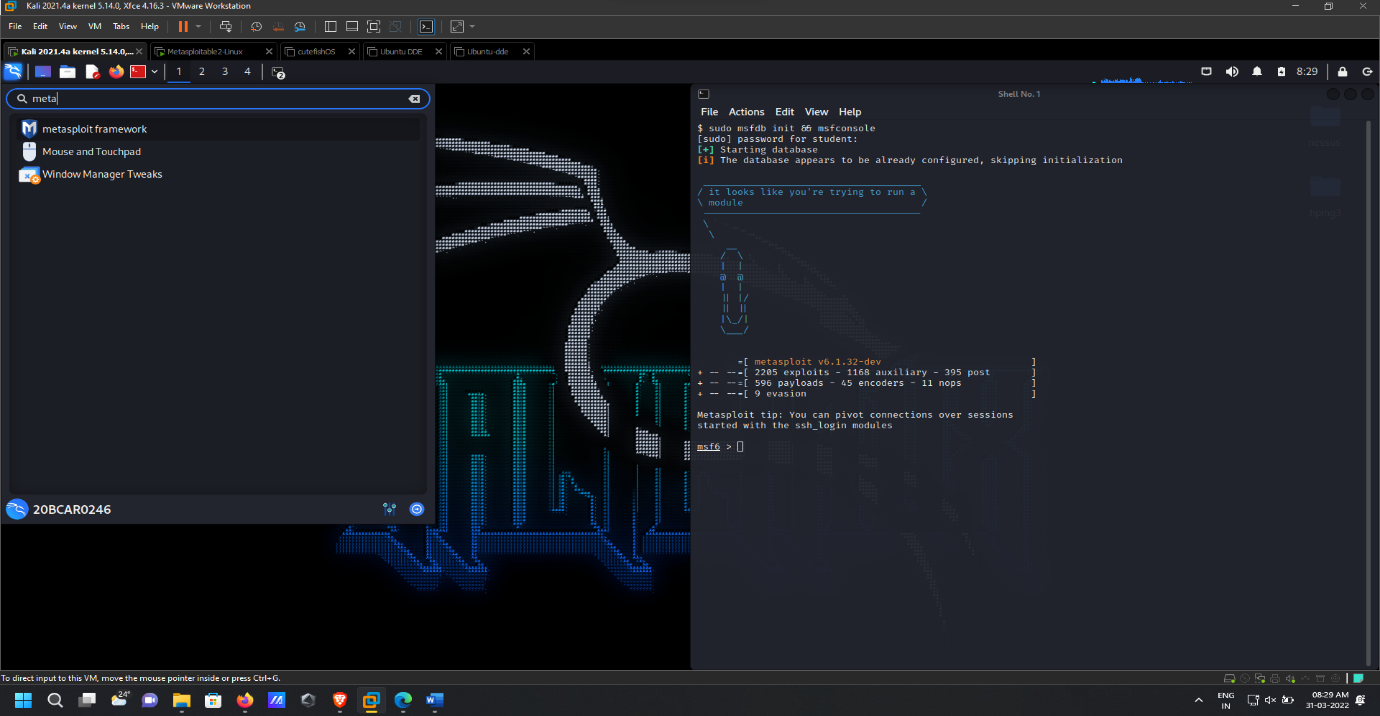
**Procedure :**

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

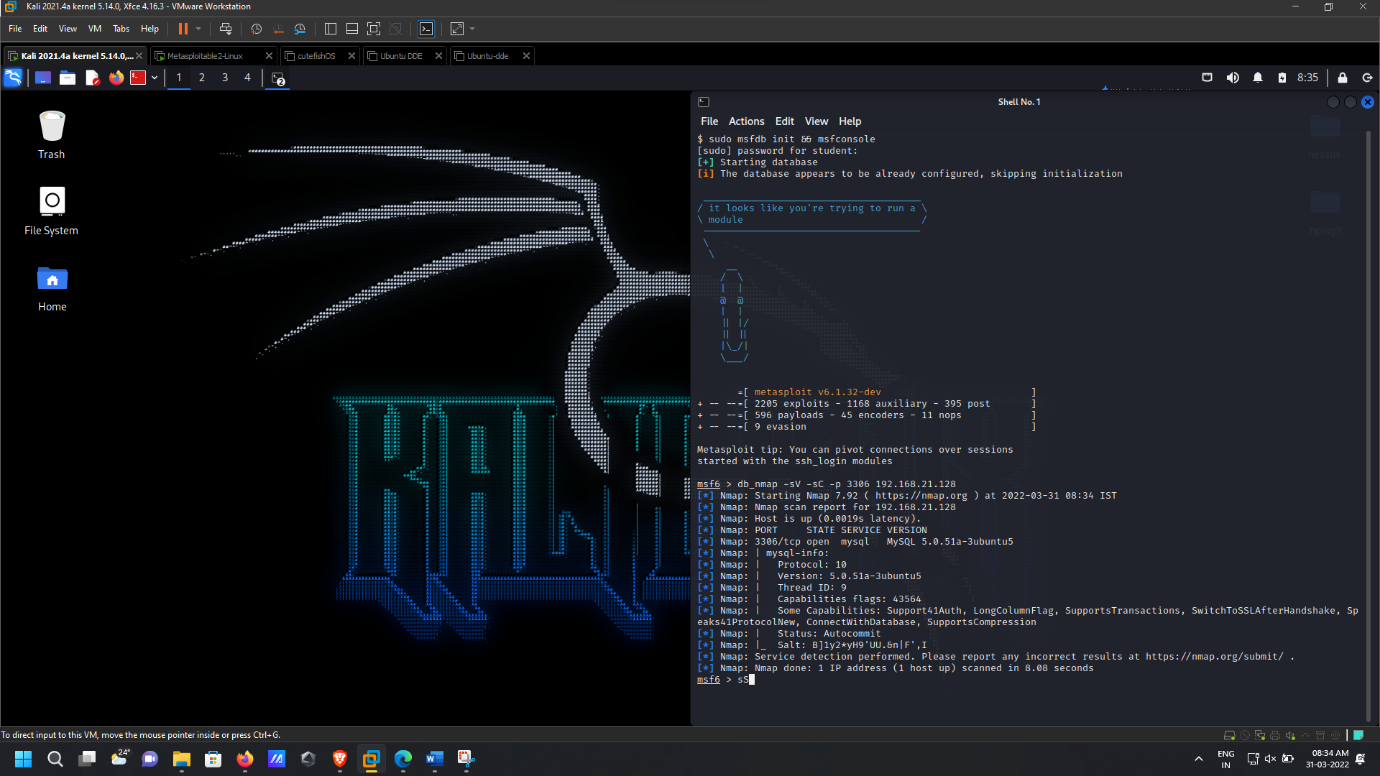
Since Metasploit comes pre-installed in Kali Linux, we are going to begin with searching it in Applications button and start with sudo password.



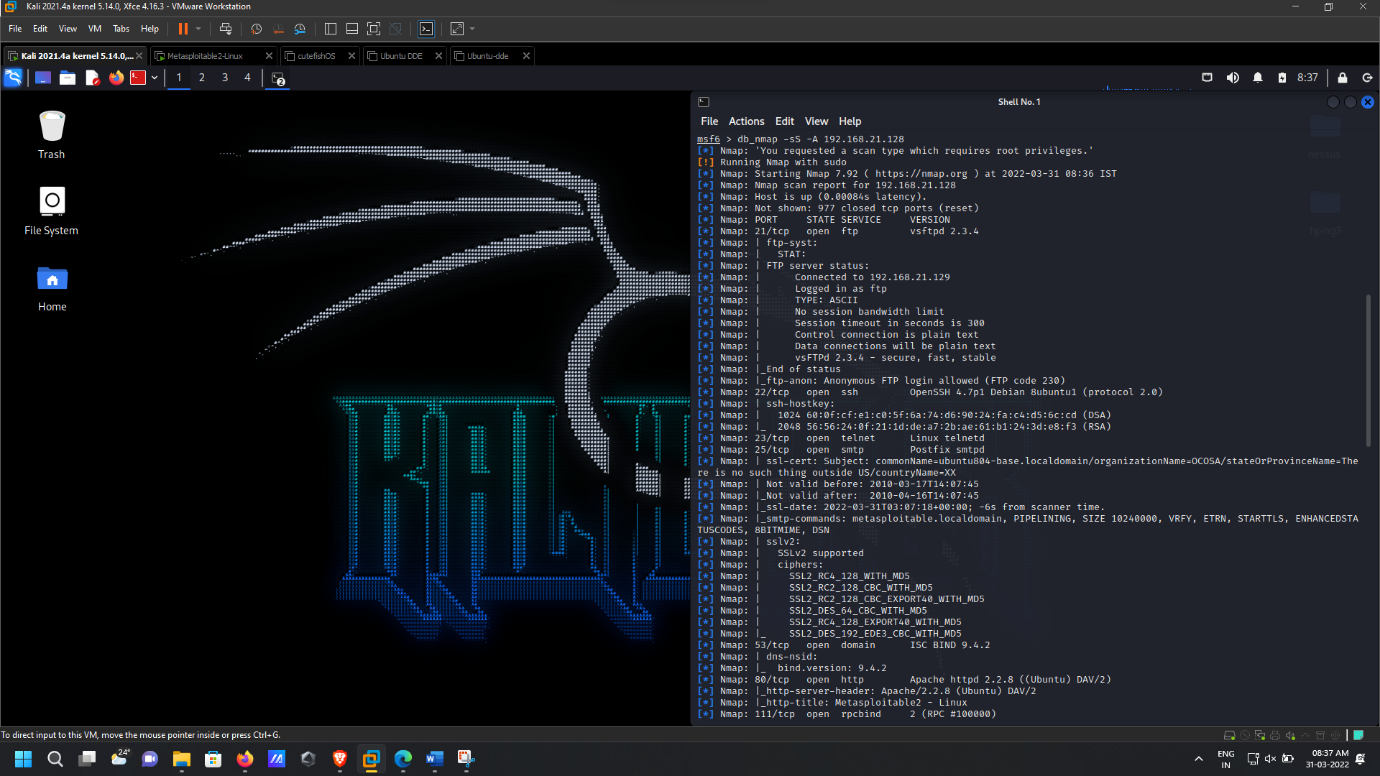
The window appears like this.

Nmap Scans

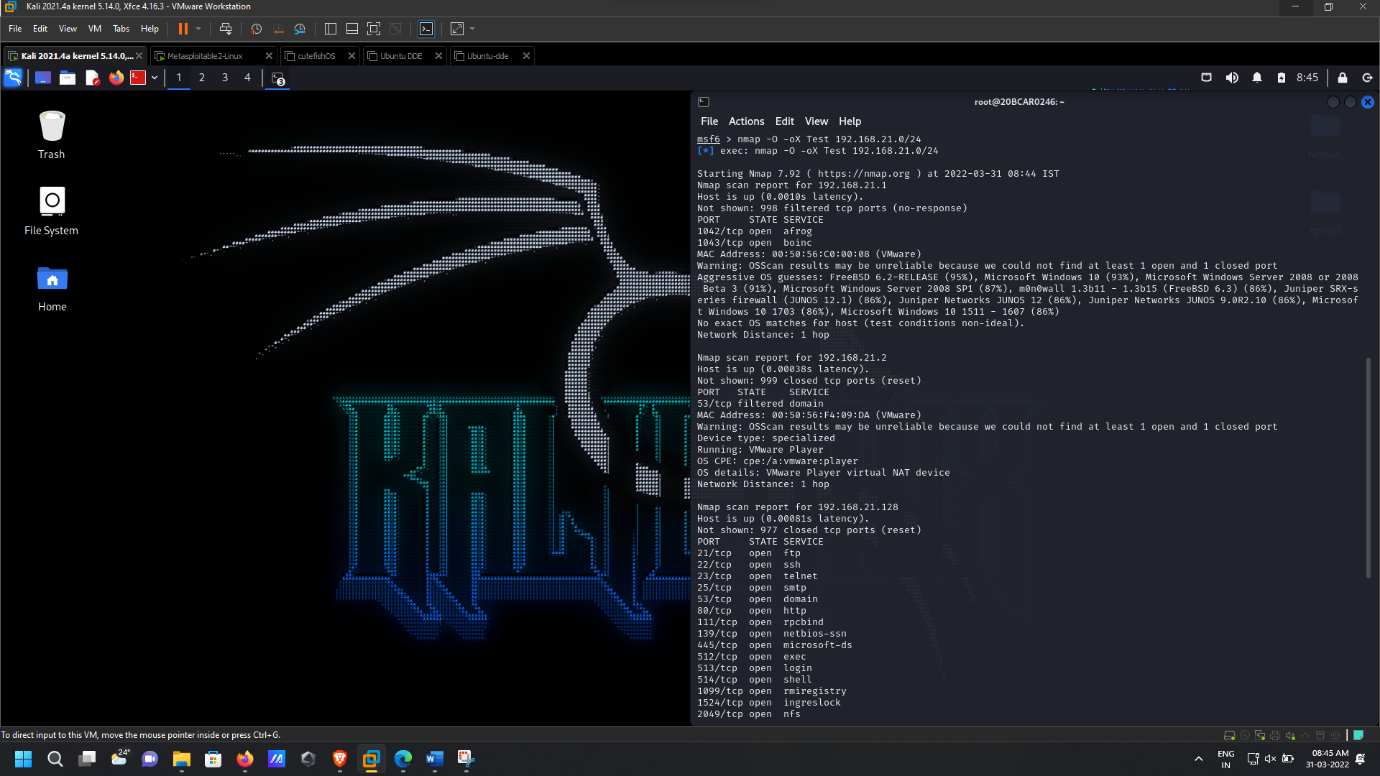
Command: db\_nmap -sV -sC -p 3306 <IP Address>



Command: db\_nmap -sS -A <IP Address>

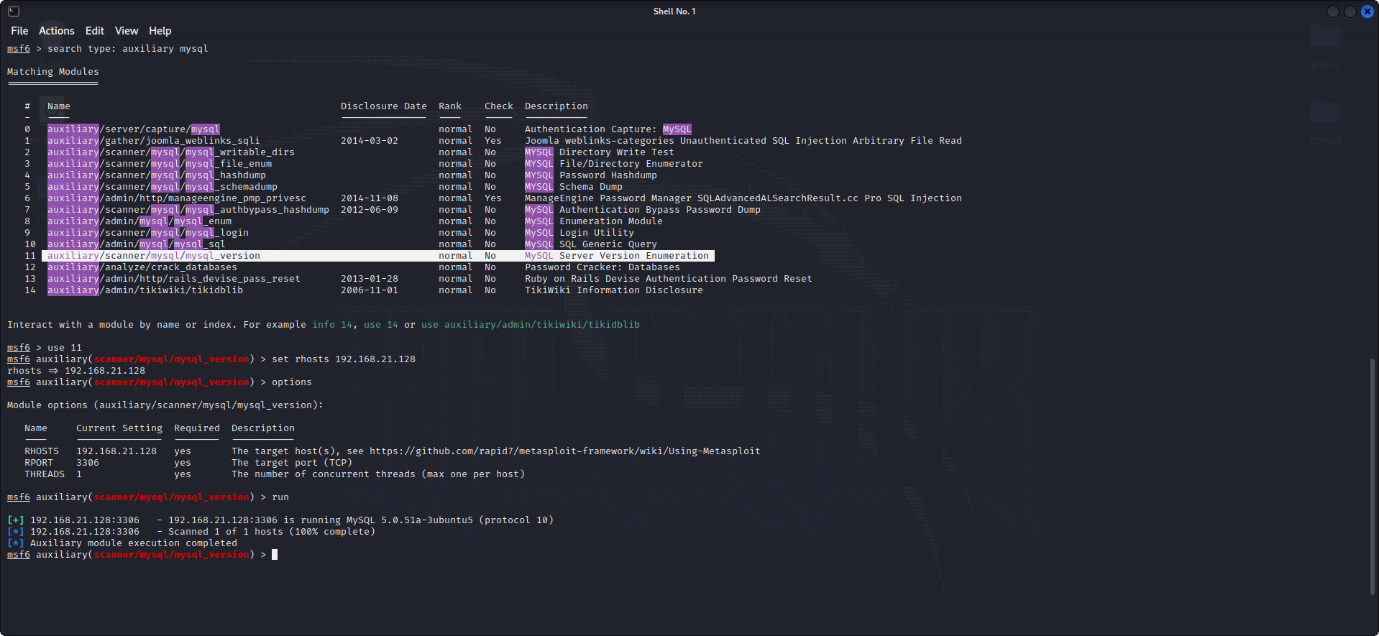


Command: nmap -O -oX <filename> <IP Address>

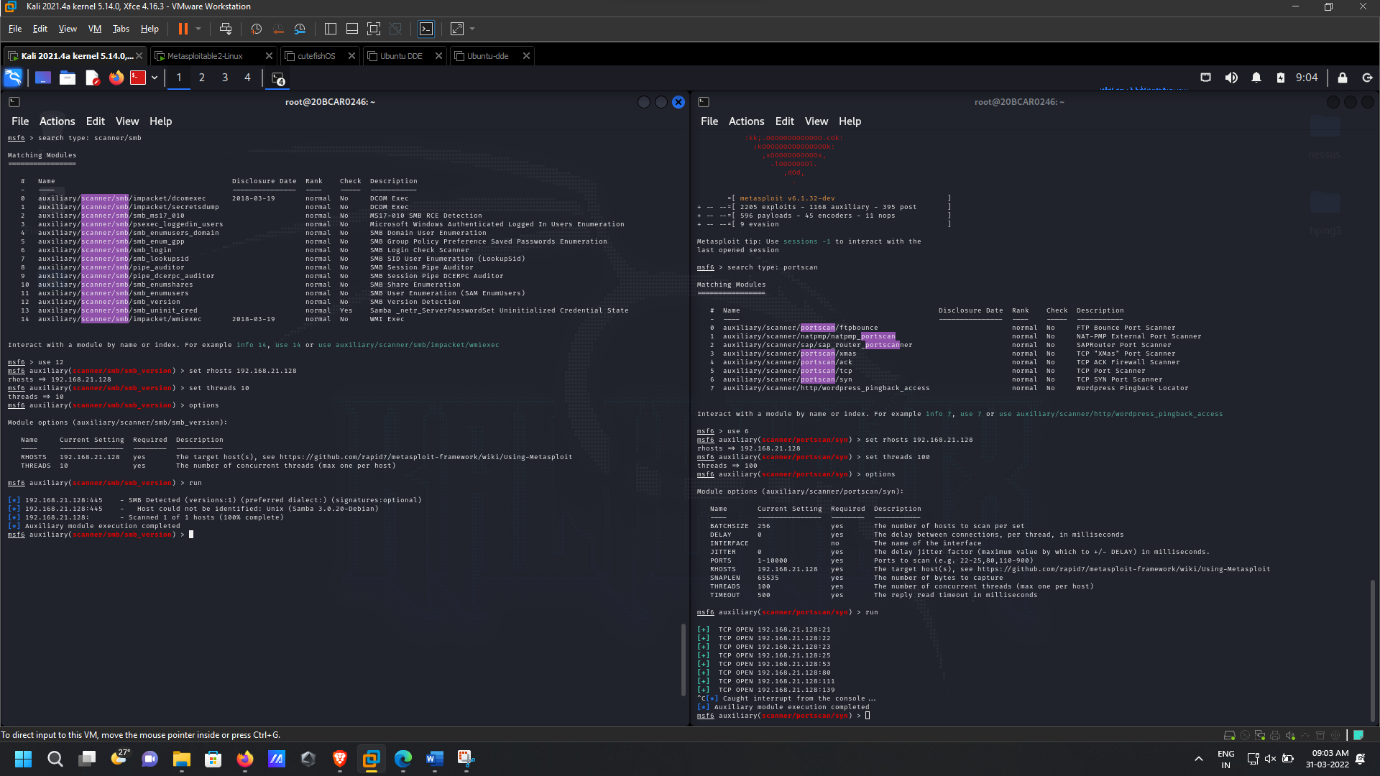


Axuiliary Scan

The steps to be followed to get the desired result are as mentioned in the picture:



For mysql



For portscan/syn & smb/smb\_version

**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.