JGi JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

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

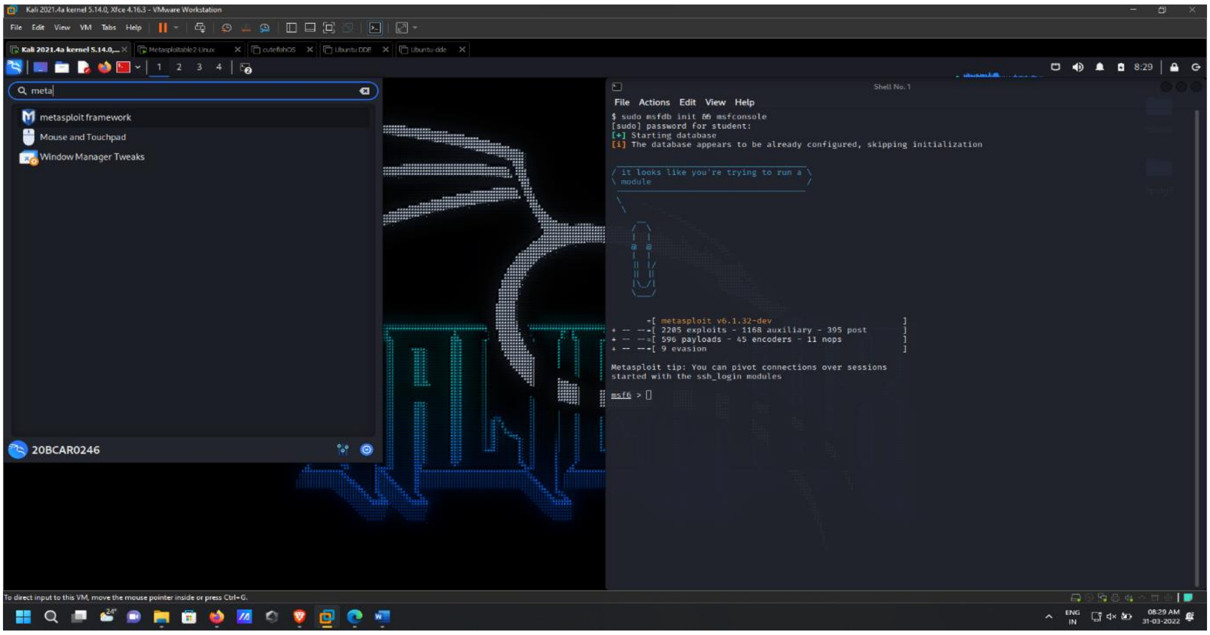
Procedure :

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

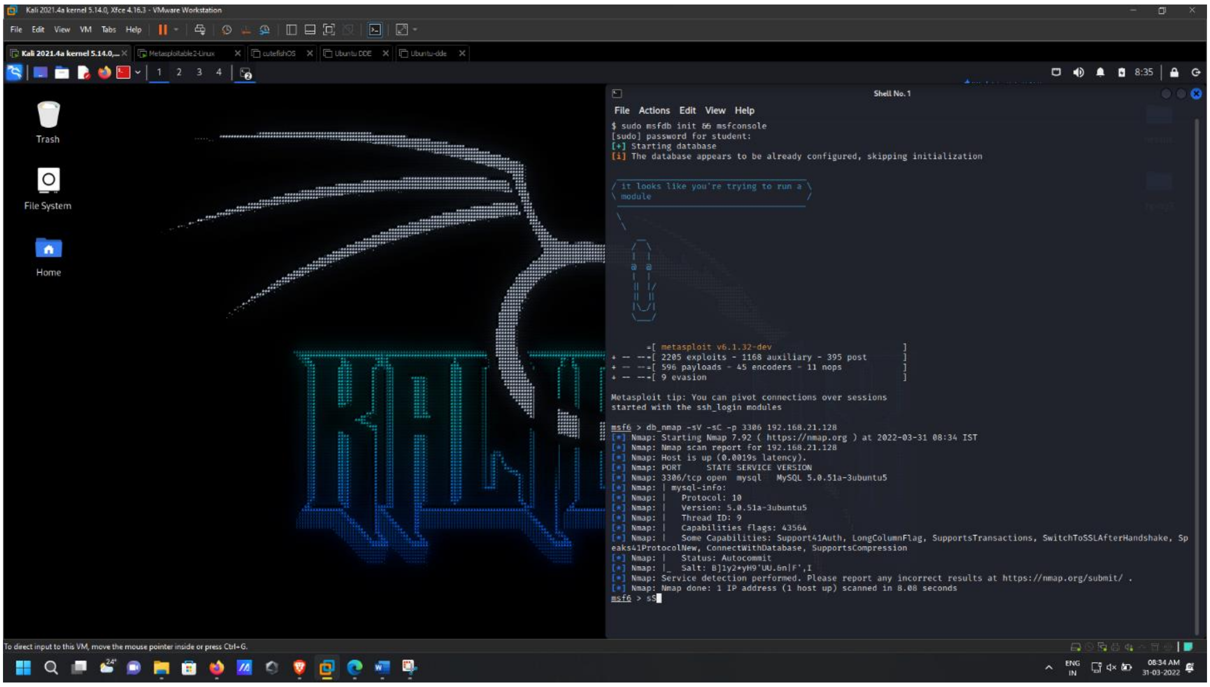
Since Metasploit comes pre-installed in Kali Linux, we are going to begin with searching it in Applications button and start with sudo password.


Kali 2021.4a kernel 5.14.0, Xfce 4.16.3 - VMware Workstation
File Edit View VM Tabs Help
Kali 2021.4a kernel 5.14.0,...
Metasploitable2-Linux
cutefishOS
Ubuntu DDE
Ubuntu-dde
meta
metasploit framework
Mouse and Touchpad
Window Manager Tweaks
20BCAR0246
Shell No. 1
File Actions Edit View Help
8:29

```
$ sudo msfdb init && msfconsole
[sudo] password for student:
[+] Starting database
[i] The database appears to be already configured, skipping initialization

 ___________________________________
/ it looks like you're trying to run a \
\ module                             /
 -----------------------------------
  \
   \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


         =[ metasploit v6.1.32-dev                          ]
+ -- --=[ 2205 exploits - 1168 auxiliary - 395 post       ]
+ -- --=[ 596 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > 
```

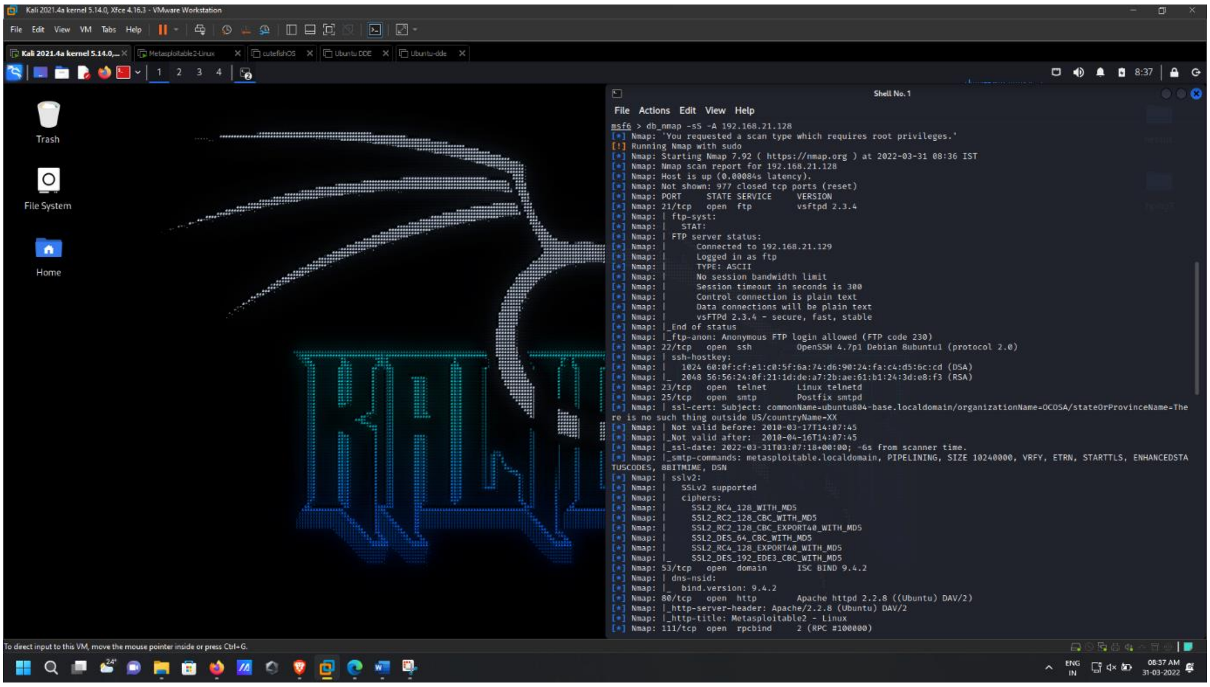
The window appears like this.

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



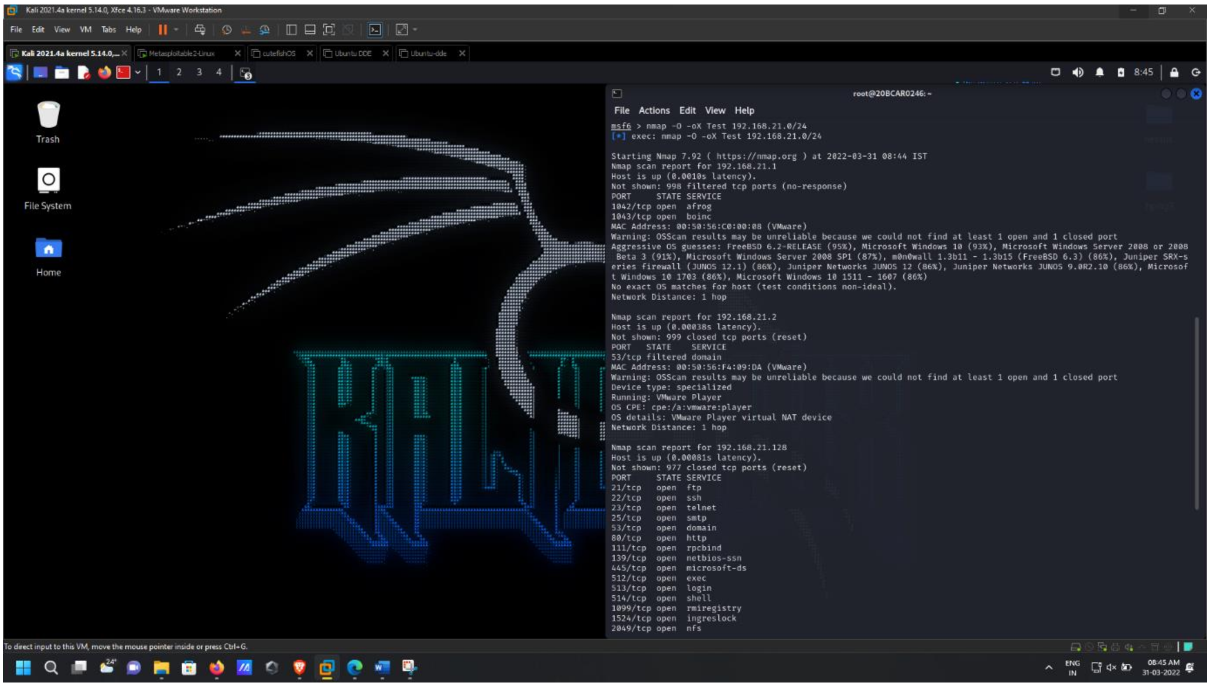
```
$ sudo msfdb init && msfconsole
[sudo] password for student:
[+] Starting database
[i] The database appears to be already configured, skipping initialization

 ___________________________________
/ it looks like you're trying to run a \
\ module                                /
 -----------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.1.32-dev                          ]
+ -- --=[ 2205 exploits - 1168 auxiliary - 395 post       ]
+ -- --=[ 596 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > db_nmap -sV -sC -p 3306 192.168.21.128
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 08:34 IST
[*] Nmap: Nmap scan report for 192.168.21.128
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: PORT     STATE SERVICE VERSION
[*] Nmap: 3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
[*] Nmap: | mysql-info:
[*] Nmap: |   Protocol: 10
[*] Nmap: |   Version: 5.0.51a-3ubuntu5
[*] Nmap: |   Thread ID: 9
[*] Nmap: |   Capabilities flags: 43564
[*] Nmap: |   Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHandshake, Sp
eaks41ProtocolNew, ConnectWithDatabase, SupportsCompression
[*] Nmap: |   Status: Autocommit
[*] Nmap: |_  Salt: B]1y2*yH9'UU.&n|F',I
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.08 seconds
msf6 > sS
```

Command: `db_nmap -sS -A <IP Address>`



```
msf6 > db_nmap -sS -A 192.168.21.128
[*] Nmap: 'You requested a scan type which requires root privileges.'
[!] Running Nmap with sudo
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 08:36 IST
[*] Nmap: Nmap scan report for 192.168.21.128
[*] Nmap: Host is up (0.00084s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 192.168.21.129
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
[*] Nmap: |_End of status
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
[*] Nmap: |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
[*] Nmap: | Not valid before: 2010-03-17T14:07:45
[*] Nmap: |_Not valid after:  2010-04-16T14:07:45
[*] Nmap: |_ssl-date: 2022-03-31T03:07:18+00:00; -6s from scanner time.
[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTA
TUSCODES, 8BITMIME, DSN
[*] Nmap: | sslv2:
[*] Nmap: |   SSLv2 supported
[*] Nmap: |   ciphers:
[*] Nmap: |     SSL2_RC4_128_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
[*] Nmap: |     SSL2_DES_64_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC4_128_EXPORT40_WITH_MD5
[*] Nmap: |_    SSL2_DES_192_EDE3_CBC_WITH_MD5
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: |_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
[*] Nmap: |_http-title: Metasploitable2 - Linux
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
```

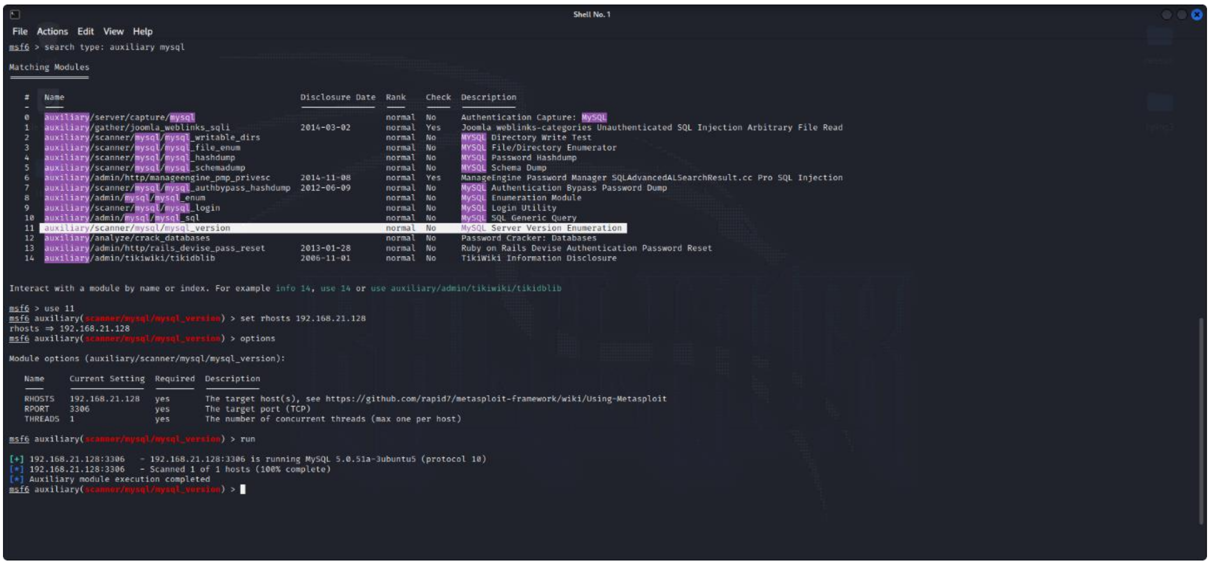
Command: `nmap -O -oX <filename> <IP Address>`


Kali 2021.4a kernel 5.14.0, Xfce 4.16.3 - VMware Workstation
Trash
File System
Home
root@20BCAR0246: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
msf6 > nmap -O -oX Test 192.168.21.0/24
[*] exec: nmap -O -oX Test 192.168.21.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 08:44 IST
Nmap scan report for 192.168.21.1
Host is up (0.0010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Windows 10 (93%), Microsoft Windows Server 2008 or 2008
 Beta 3 (91%), Microsoft Windows Server 2008 SP1 (87%), m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3) (86%), Juniper SRX-s
eries firewall (JUNOS 12.1) (86%), Juniper Networks JUNOS 12 (86%), Juniper Networks JUNOS 9.0R2.10 (86%), Microsof
t Windows 10 1703 (86%), Microsoft Windows 10 1511 - 1607 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.21.2
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:F4:09:DA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

Nmap scan report for 192.168.21.128
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```

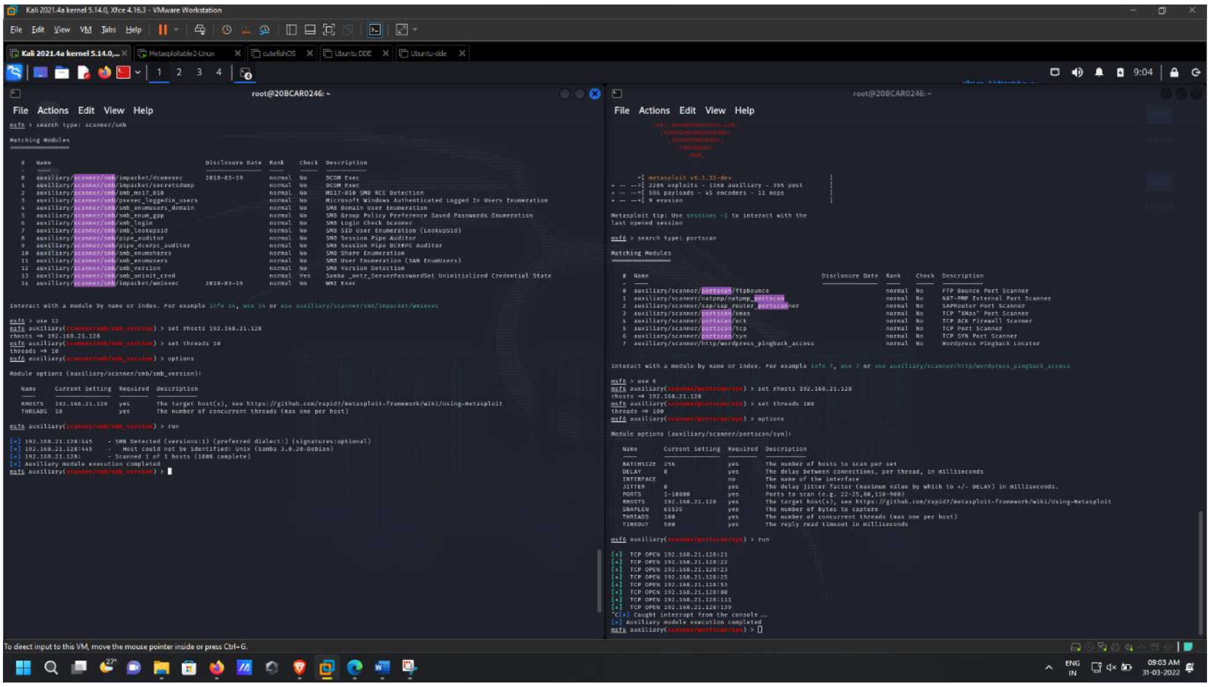
Axuiliary Scan

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



```
msf6 > search type: auxiliary mysql

Matching Modules
================

   #   Name                                              Disclosure Date  Rank    Check  Description
   -   ----                                              ---------------  ----    -----  -----------
   0   auxiliary/server/capture/mysql                                     normal  No     Authentication Capture: MySQL
   1   auxiliary/gather/joomla_weblinks_sqli             2014-03-02       normal  Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
   2   auxiliary/scanner/mysql/mysql_writable_dirs                        normal  No     MYSQL Directory Write Test
   3   auxiliary/scanner/mysql/mysql_file_enum                            normal  No     MYSQL File/Directory Enumerator
   4   auxiliary/scanner/mysql/mysql_hashdump                             normal  No     MYSQL Password Hashdump
   5   auxiliary/scanner/mysql/mysql_schemadump                           normal  No     MYSQL Schema Dump
   6   auxiliary/admin/http/manageengine_pmp_privesc     2014-11-08       normal  Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   7   auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09       normal  No     MySQL Authentication Bypass Password Dump
   8   auxiliary/admin/mysql/mysql_enum                                   normal  No     MySQL Enumeration Module
   9   auxiliary/scanner/mysql/mysql_login                                normal  No     MySQL Login Utility
   10  auxiliary/admin/mysql/mysql_sql                                    normal  No     MySQL SQL Generic Query
   11  auxiliary/scanner/mysql/mysql_version                              normal  No     MySQL Server Version Enumeration
   12  auxiliary/analyze/crack_databases                                  normal  No     Password Cracker: Databases
   13  auxiliary/admin/http/rails_devise_pass_reset      2013-01-28       normal  No     Ruby on Rails Devise Authentication Password Reset
   14  auxiliary/admin/tikiwiki/tikidblib                2006-11-01       normal  No     TikiWiki Information Disclosure


Interact with a module by name or index. For example info 14, use 14 or use auxiliary/admin/tikiwiki/tikidblib

msf6 > use 11
msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 192.168.21.128
rhosts => 192.168.21.128
msf6 auxiliary(scanner/mysql/mysql_version) > options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.21.128   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.21.128:3306   - 192.168.21.128:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.21.128:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > 
```

For `mysql`


Kali 2021.4a kernel 5.14.0, Xfce 4.16.3 - VMware Workstation
File Edit View VM Tabs Help
Kali 2021.4a kernel 5.14.0,...
Metasploitable2-Linux
cutefishOS
Ubuntu DDE
Ubuntu-dde
root@20BCAR0246: ~
File Actions Edit View Help
9:04
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG IN
09:03 AM
31-03-2022

```
msf6 > search type: scanner/smb

Matching Modules
================

   #   Name                                           Disclosure Date  Rank    Check  Description
   -   ----                                           ---------------  ----    -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec        2018-03-19       normal  No     DCOM Exec
   1   auxiliary/scanner/smb/impacket/secretsdump                      normal  No     DCOM Exec
   2   auxiliary/scanner/smb/smb_ms17_010                              normal  No     MS17-010 SMB RCE Detection
   3   auxiliary/scanner/smb/psexec_loggedin_users                     normal  No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   auxiliary/scanner/smb/smb_enumusers_domain                      normal  No     SMB Domain User Enumeration
   5   auxiliary/scanner/smb/smb_enum_gpp                              normal  No     SMB Group Policy Preference Saved Passwords Enumeration
   6   auxiliary/scanner/smb/smb_login                                 normal  No     SMB Login Check Scanner
   7   auxiliary/scanner/smb/smb_lookupsid                             normal  No     SMB SID User Enumeration (LookupSid)
   8   auxiliary/scanner/smb/pipe_auditor                              normal  No     SMB Session Pipe Auditor
   9   auxiliary/scanner/smb/pipe_dcerpc_auditor                       normal  No     SMB Session Pipe DCERPC Auditor
   10  auxiliary/scanner/smb/smb_enumshares                            normal  No     SMB Share Enumeration
   11  auxiliary/scanner/smb/smb_enumusers                             normal  No     SMB User Enumeration (SAM EnumUsers)
   12  auxiliary/scanner/smb/smb_version                               normal  No     SMB Version Detection
   13  auxiliary/scanner/smb/smb_uninit_cred                           normal  Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   14  auxiliary/scanner/smb/impacket/wmiexec         2018-03-19       normal  No     WMI Exec


Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 > use 12
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.21.128
rhosts => 192.168.21.128
msf6 auxiliary(scanner/smb/smb_version) > set threads 10
threads => 10
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.21.128   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  10               yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.21.128:445    - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.21.128:445    -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.21.128:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > 
```

```
       =[ metasploit v6.1.32-dev                          ]
+ -- --=[ 2205 exploits - 1168 auxiliary - 395 post       ]
+ -- --=[ 596 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > search type: portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                               normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                                    normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                                     normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                                     normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                                     normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access                   normal  No     Wordpress Pingback Locator


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > use 6
msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.21.128
rhosts => 192.168.21.128
msf6 auxiliary(scanner/portscan/syn) > set threads 100
threads => 100
msf6 auxiliary(scanner/portscan/syn) > options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS     192.168.21.128   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    100              yes       The number of concurrent threads (max one per host)
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf6 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.21.128:21
[+]  TCP OPEN 192.168.21.128:22
[+]  TCP OPEN 192.168.21.128:23
[+]  TCP OPEN 192.168.21.128:25
[+]  TCP OPEN 192.168.21.128:53
[+]  TCP OPEN 192.168.21.128:80
[+]  TCP OPEN 192.168.21.128:111
[+]  TCP OPEN 192.168.21.128:139
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) > 
```

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.