



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 :

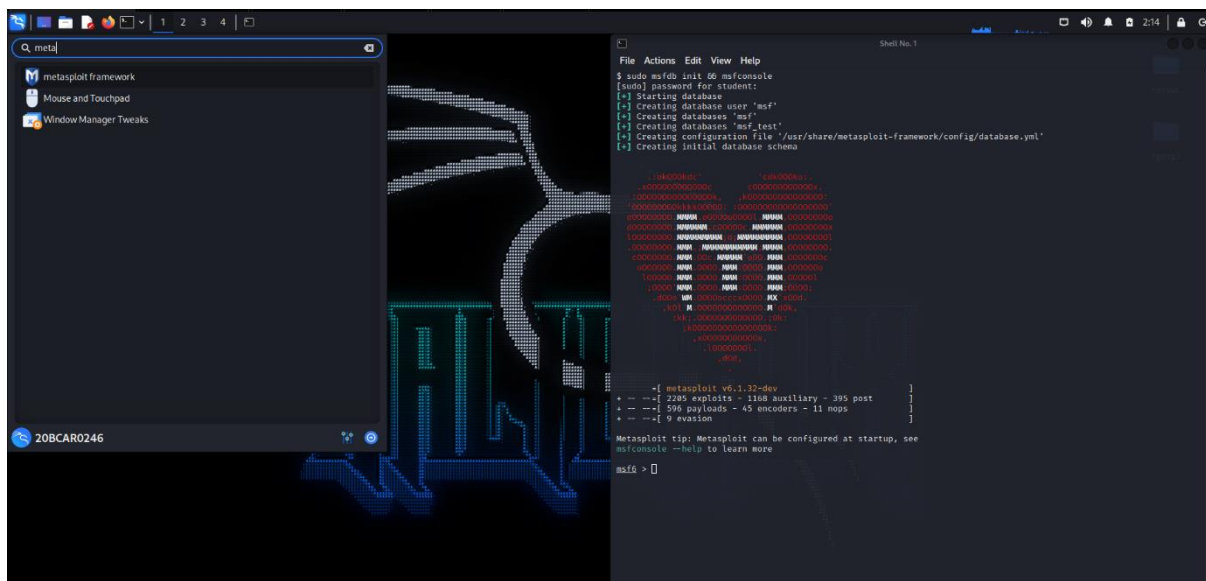
To Run Scans, like:

- ✓ Nmap Scan
- ✓ Auxiliary 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.

Nmap Scans

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

```
File Actions Edit View Help
[+] Starting database
[!] The database appears to be already configured, skipping initialization

...[snipped]...

+--[ 2285 exploits - 1168 auxiliary - 395 post
+--[ 596 payloads - 45 encoders - 11 nops
+--[ 9 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > db_nmap -sV -sC -p 3306 192.168.21.128
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 08:08 IST
[*] Nmap: Nmap scan report for 192.168.21.128
[*] Nmap: Host is up (0.0018s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 3306/tcp open  mysql      MySQL 5.8.51a-3ubuntu5
[*] Nmap: | mysql-info:
[*] Nmap: |   Protocol: 10
[*] Nmap: |   Version: 5.8.51a-3ubuntu5
[*] Nmap: |   Thread ID: 12
[*] Nmap: |   Capabilities Flags: 43564
[*] Nmap: |   Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew, SupportsTransaction
[*] Nmap: |   ns, SupportsCompression, Supports1Auth, ConnectWithDatabase
[*] Nmap: |   Status: Autocommit
[*] Nmap: |   Salt: dcfa'lkUxXaXZ9WKSvW
[*] 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 1.58 seconds
msf6 >
```

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

```
File Actions Edit View Help
msf6 auxiliary> db_nmap -sS -A <IP Address> > db_nmap -sS -A 192.168.21.128
[!] Running Nmap with sudo
[!] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 08:23 IST
[*] Nmap: Nmap scan report for 192.168.21.128
[*] Nmap: Host is up (0.00005s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp open  ftp
[*] 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 68:0f:cfe:1e:05:5f:6a:74:d6:90:24:fa:c4:d5:9c:cd (DSA)
[*] Nmap: |   2048 56:56:24:0f:23:1d:de:e7:2b:ae:d1:b1:24:3d:e6:f3 (RSA)
[*] Nmap: 23/tcp open  telnet   Linux telnetd
[*] Nmap: 25/tcp open  smtp      Postfix smtpd
[*] Nmap: |_ssl-date: 2022-03-22T22:31:20+00:00 -20h22m18s from scanner time.
[*] Nmap: |_ssl-cert: Subject: commonName=ubuntu084-base.localdomain/organizationName=OCOSA/statedProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Not valid before: 2018-08-17T16:07:45
[*] Nmap: | Not valid after: 2018-08-10T16:07:45
[*] Nmap: |_smtp-command: setmailinfo,localdomain, PIPELINING, SIZE 1024000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
[*] Nmap: |_sslv2:
[*] Nmap: |_sslv2 supported
[*] Nmap: |_ciphers:
[*] Nmap: |   SSL2_RCA_128_CBC_EXPORT40_WITH_MD5
[*] Nmap: |   SSL2_DES_64_CBC_WITH_MD5
[*] Nmap: |   SSL2_RCA_128_CBC_WITH_MD5
[*] Nmap: |   SSL2_RCA_128_EXPORT40_WITH_MD5
[*] Nmap: |   SSL2_RCA_128_WITH_MD5
[*] Nmap: |   SSL2_DES_192_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)
[*] Nmap: | rpcinfo:
[*] Nmap: |   Capabilities Flags: 43564
[*] Nmap: |   Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression, SupportsTransactions, Speaks41ProtocolNew, LongColumnFlag, Supports1Auth
[*] Nmap: |   Status: Autocommit
[*] Nmap: |   Salt: 73f0:Sa1Za1l1g:6
[*] Nmap: 5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: |_ssl-date: 2022-03-22T22:31:20+00:00 -20h22m18s from scanner time.
[*] Nmap: |_ssl-cert: Subject: commonName=ubuntu084-base.localdomain/organizationName=OCOSA/statedProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Not valid before: 2018-08-17T16:07:45
[*] Nmap: | Not valid after: 2018-08-10T16:07:45
[*] Nmap: 5986/tcp open  vnc       VNC (protocol 3.3)
[*] Nmap: | vnc-info:
[*] Nmap: |   Protocol version: 3.3
[*] Nmap: |   Security types:
[*] Nmap: |     VNC Authentication (2)
[*] Nmap: 6000/tcp open  x11      (access denied)
[*] Nmap: 6667/tcp open  irc      UnrealIRCd
[*] Nmap: 8080/tcp open  http     Apache Jserv (Protocol v1.3)
[*] Nmap: |_ajp-methods: failed to get a valid response for the OPTIONS request
[*] Nmap: 8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-server-header: Apache/2.2.8
[*] Nmap: |_http-favicon: Apache Tomcat
[*] Nmap: |_http-title: Apache Tomcat/2.5
[*] Nmap: MAC Address: 08:0C:29:F8:2D:08 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: -19h22m09s, deviation: 2h00m00s, median: -20h22m18s
[*] Nmap: |_sm2-time: Protocol negotiation failed (SM2)
[*] Nmap: |_smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |   Computer name: metasploitable
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: metasploitable.localdomain
[*] Nmap: |_system-time: 2022-03-22T18:31:19-04:00
[*] Nmap: |_hosts: netBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: |_smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_message_signing: disabled (dangerous, but default)
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1    0.45 ms  192.168.21.128
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 24.58 seconds
msf6 auxiliary>
```

Axuiiliary Scan

```
File Actions Edit View Help
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.sql     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_schema_dump normal No     MySQL Schema Dump
6  auxiliary/admin/http/manasengine_one_privsec 2014-11-08      normal Yes  Manasengine 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 2011-01-28      normal No     Ruby on Rails Devise Authentication Password Reset
14 auxiliary/admin/tikiwiki/tikiwiki        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/tikiwiki
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
PORT      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-Jubuntu5 (protocol 10)
[*] 192.168.21.128:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_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.