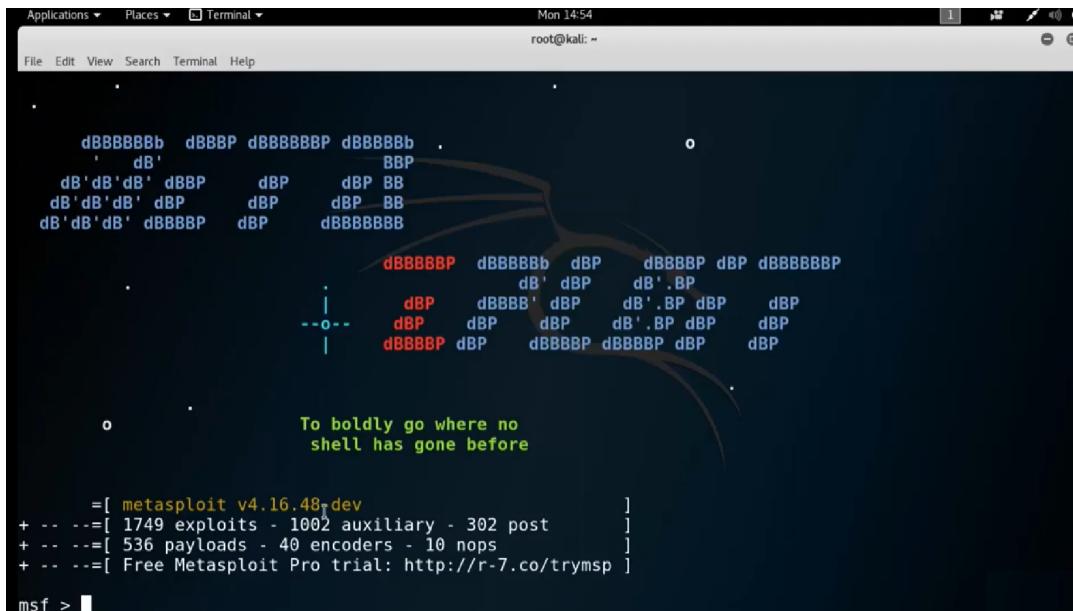


Information Gathering

- Start Kali Linux OS
- Start Metasploit in Kali Linux and perform information gathering.

1. Open the terminal and type “**msfconsole**” and hit enter to start Metasploit in Kali Linux.

(Now it will start Metasploit framework into kali linux OS)



```
Applications ▾ Places ▾ Terminal ▾ Mon 14:54
root@kali: ~

File Edit View Search Terminal Help

dBBBBBBb dBBBBP dBBBBBBB dBBBBBb .
' dB' .BP
dB'dB'dB' dBp dBP dB' BB
dB'dB'dB' dBp dBP dB' BB
dB'dB'dB' dBp dBP dB' BB
dB'dB'dB' dBp dBBBBBP . o
dBBBBBP dBBBBBBb dBp dBBBBBP dBp dBBBBBBBp
dBP dB' dBp dB' .BP
dBP dBBBB' dBp dB' .BP dBp dBp
dBP dBp dBp dB' .BP dBp dBp
dBP dBp dBp dBBBBP dBp dBp dBp
o To boldly go where no
shell has gone before

=[ metasploit v4.16.48 dev
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post      ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops      ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]]

msf > [
```

Metasploit have started and here we can type various commands for Metasploit.

2. Now we are going to gather basic information of a web site.

For this we are going to use the sample website www.vulnweb.com which is used for testing purpose.

Type: “**whois vulnweb.com**” and hit enter.

```

root@kali: ~
File Edit View Search Terminal Help
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2018-10-01T18:55:13Z <<<

Please email the listed admin email address if you wish to raise a legal issue.

Whois History: 525 records have been archived since 2010-06-15
http://www.domaintools.com/research/whois-history/?page=results&Affiliate_ID=1001861&q=vulnweb.com

The Data in EuroDNS WHOIS database is provided for information purposes only.
The fact that EuroDNS display such information does not provide any guaranteee
expressed or implied on the purpose for which the database may be used, its
accuracy or usefulness. By submitting a WHOIS query, you agree that you will
use this Data only for lawful purposes and that, under no circumstances will
you use this Data to:

(1) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via e-mail (spam); or
(2) enable high volume, automated, electronic processes that apply to EuroDNS
(or its systems). EuroDNS reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by the above policy.

For more information on Whois status codes, please visit: https://www.icann.org/resources/pages/epp-sta

```

Here we can get the basic information about the website.

2. Now we are going to gather information about FTP

Type: “**search ftp**” and hit enter

```

root@kali: ~
File Edit View Search Terminal Help
post/multi/gather/netrc_creds                               normal    UNIX Gather .netrc C
credentials
post/windows/gather/credentials/bulletproof_ftp             normal    Windows Gather Bullet
tProof FTP Client Saved Password Extraction
post/windows/gather/credentials/coreftp                   normal    Windows Gather CoreF
TP Saved Password Extraction
post/windows/gather/credentials/filezilla_server          normal    Windows Gather FileZ
illa FTP Server Credential Collection
post/windows/gather/credentials/flashfxp                 normal    Windows Gather Flash
XP Saved Password Extraction
post/windows/gather/credentials/ftpnavigator            normal    Windows Gather FTP N
navigator Saved Password Extraction
post/windows/gather/credentials/ftpx                    normal    Windows Gather FTP E
plorer (FTPX) Credential Extraction
post/windows/gather/credentials/idm                  normal    Windows Gather Inter
net Download Manager (IDM) Password Extractor
post/windows/gather/credentials/smrtftp                normal    Windows Gather Smart
FTP Saved Password Extraction
post/windows/gather/credentials/total_commander        normal    Windows Gather Total
Commander Saved Password Extraction
post/windows/gather/credentials/wsftp_client           normal    Windows Gather WS_FT
Saved Password Extraction
post/windows/manage/pxeexploit                         normal    Windows Manage PXE E
xploit Server

```

It will find out exploits and auxiliaries regarding FTP we can use one of these information to find out the version of the FTP server.

We are going to use auxiliary/scanner/ftp/ftp_version

Type: **use auxillary/scanner/ftp/ftp_version**

Type: **show options**

```
File Edit View Search Terminal Help
root@kali: ~
xplorer (FTPX) Credential Extraction
  post/windows/gather/credentials/idm
  net Download Manager (IDM) Password Extractor
    post/windows/gather/credentials/smrtftp
  FTP Saved Password Extraction
    post/windows/gather/credentials/total_commander
  Commander Saved Password Extraction
    post/windows/gather/credentials/wsftp_client
  P Saved Password Extraction
    post/windows/manage/pxeexploit
xploit Server

msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):
Name      Current Setting      Required  Description
-----  -----
FTPPASS   mozilla@example.com  no        The password for the specified username
FTPUSER   anonymous            no        The username to authenticate as
RHOSTS    192.168.0.6          yes       The target address range or CIDR identifier
RPORT    21                     yes       The target port (TCP)
THREADS   1                     yes       The number of concurrent threads
```

Type: **set RHOSTS <target Ip address>**

Type: **run**

```
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS 192.168.0.6
RHOSTS => 192.168.0.6
msf auxiliary(scanner/ftp/ftp_version) > run

[+] 192.168.0.6:21 - FTP Banner: '220-FileZilla Server 0.9.60 beta\x0d\x0a220-written by Tim Kosse (tim.kosse@filezilla-project.org)\x0d\x0a220 Please visit https://filezilla-project.org/\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/ftp_version) >
```

It will display the ftp server running in the host machine.