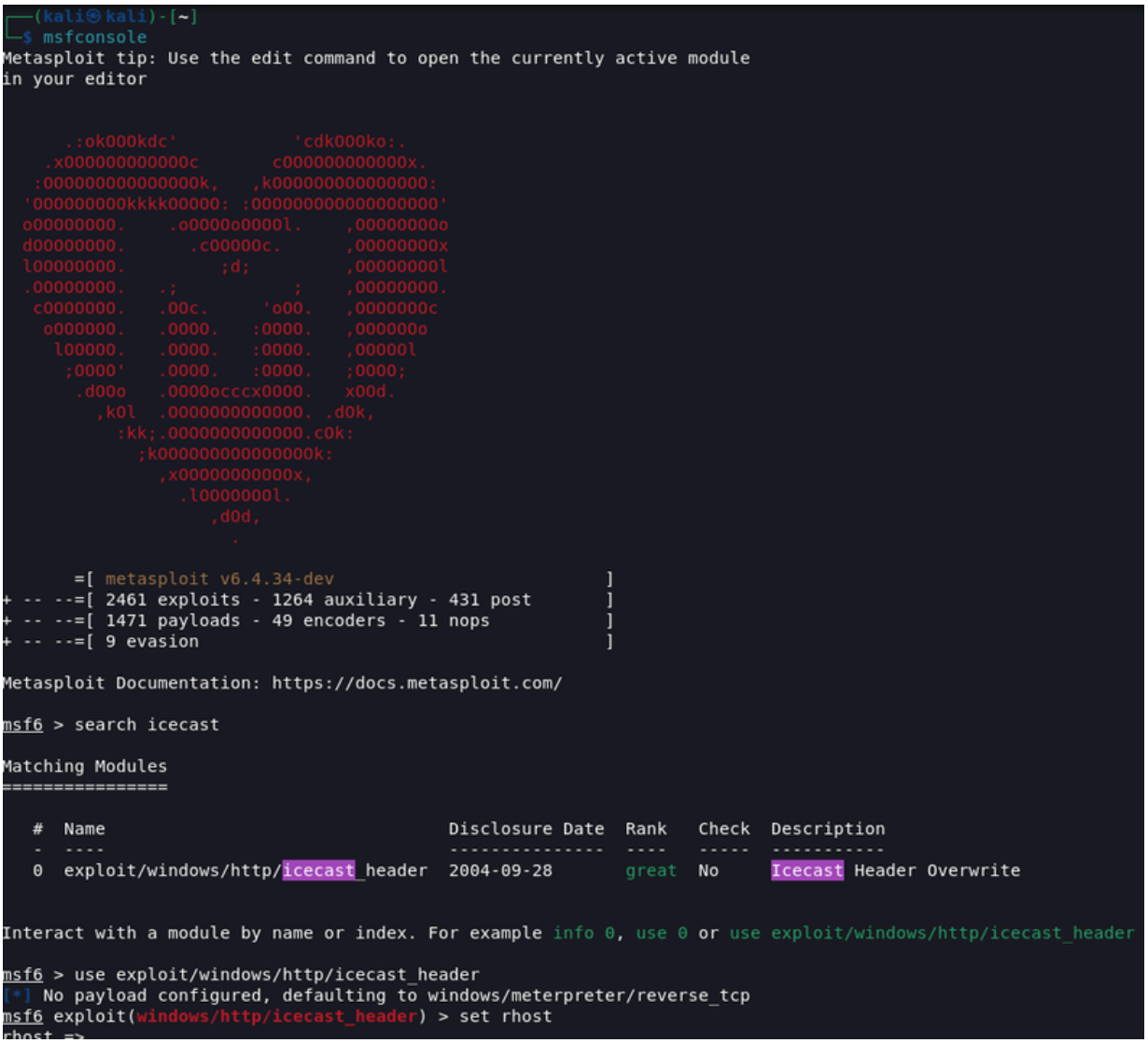
Ottenimento di una sessione Meterpreter sul target Windows 10 con Metasploit.

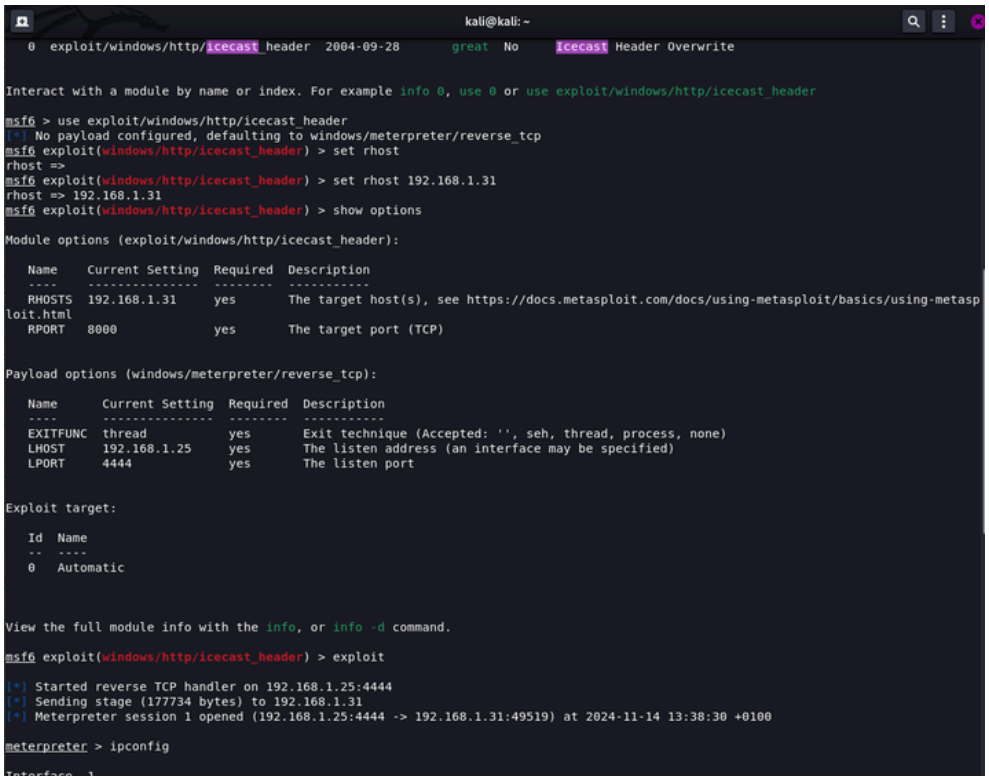
Una volta ottenuta la sessione:

- Vedremo l' indirizzo IP della vittima.
- Recupereremo uno screenshot tramite la sessione Meterpreter.

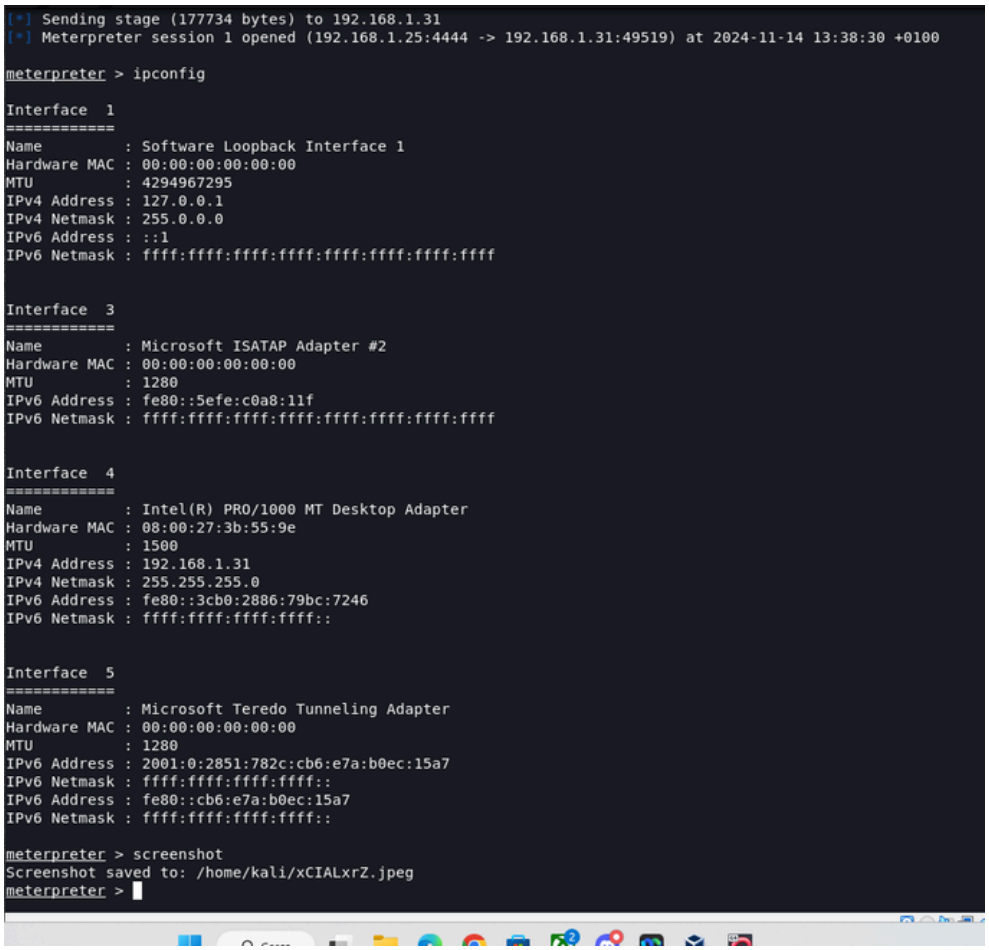
Accediamo a Metasploit su Linux, utilizziamo il comando **search icecast** per trovare l'exploit desiderato e, una volta individuato, lo avviamo con il comando **use.**



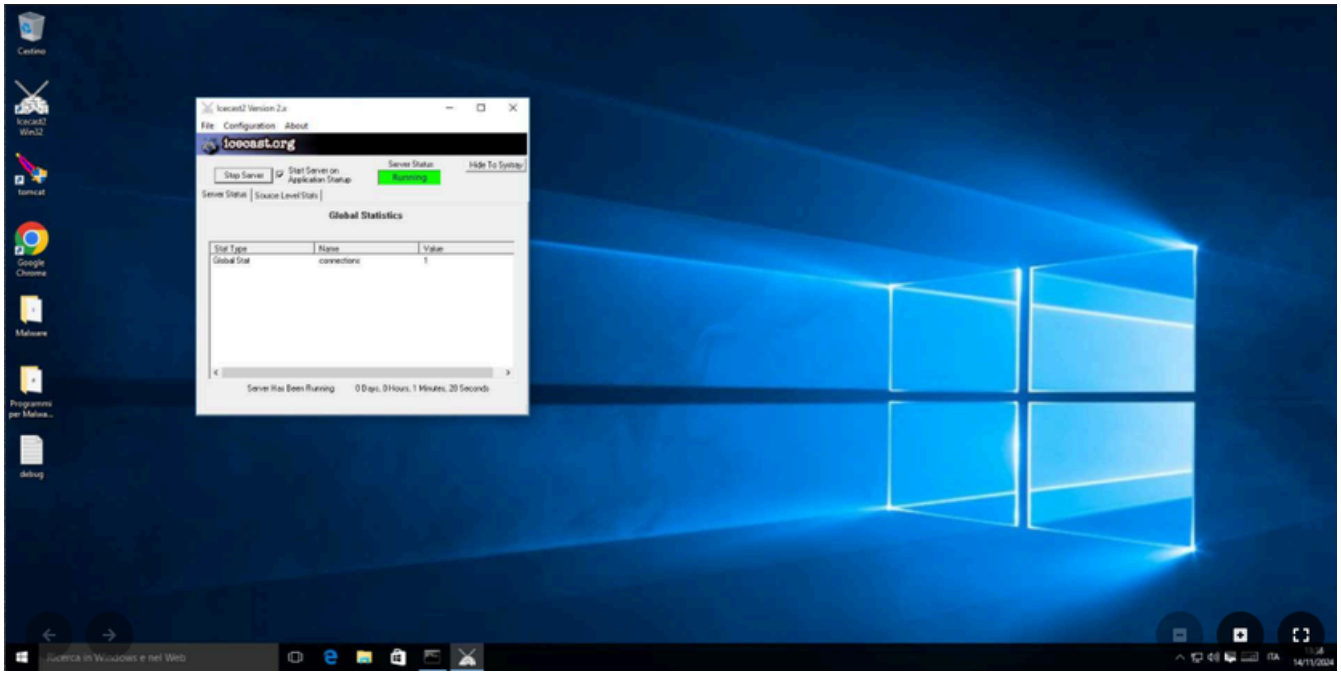
Settiamo RHOST e L HOST con il comando **set**
subito dopo lanciamo il nostro **Exploit**



Una volta acquisito il comando Meterpreter potremo lanciare il comando **ipconfig**
per vedere l'indirizzo IP della nostra macchina Windows 10



Utilizziamo il comando screenshot per acquisire un'immagine della schermata della macchina attaccata. Con il payload di Icecast, possiamo ottenere una visuale della pagina in esecuzione sul sistema compromesso.



Conclusioni

Il payload di Icecast sfrutta una vulnerabilità nel server di streaming multimediale Icecast, consentendo all'attaccante di eseguire codice arbitrario sul sistema target. Questa exploit viene tipicamente utilizzata per ottenere accesso remoto non autorizzato, aprendo una shell di comando o una sessione Meterpreter per eseguire comandi e raccogliere informazioni sul sistema compromesso.