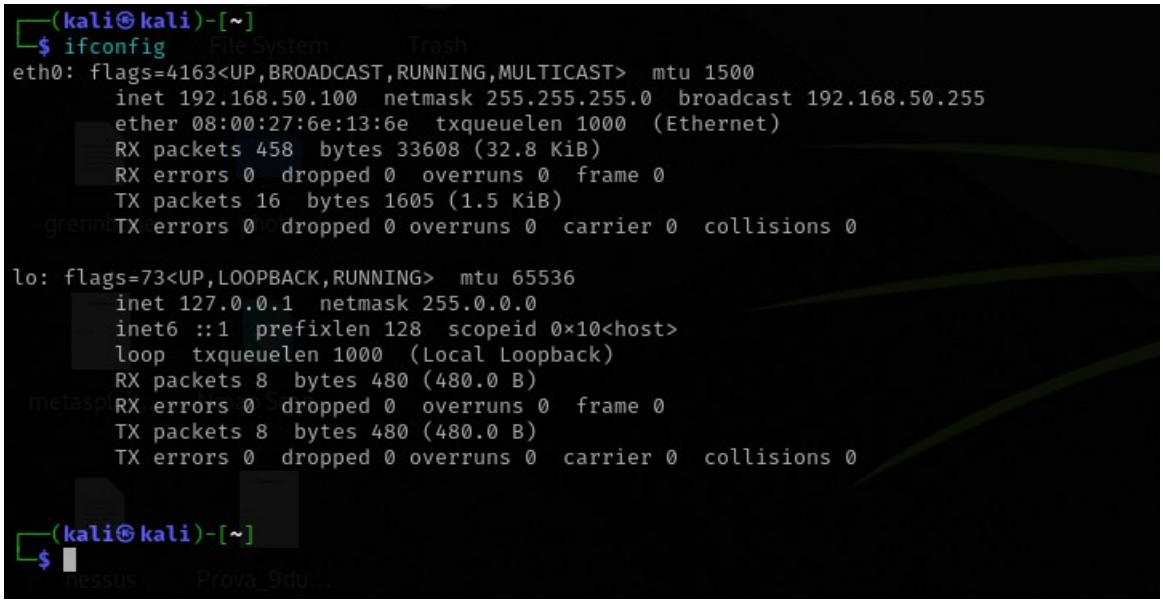
Hacking Windows

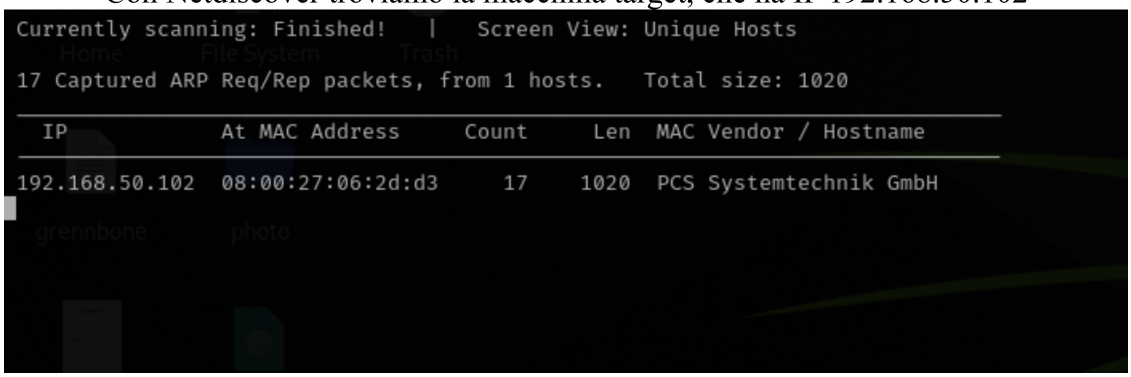
L'esercizio prevede di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit. Una volta ottenuta la sessione, si dovrà:
- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast

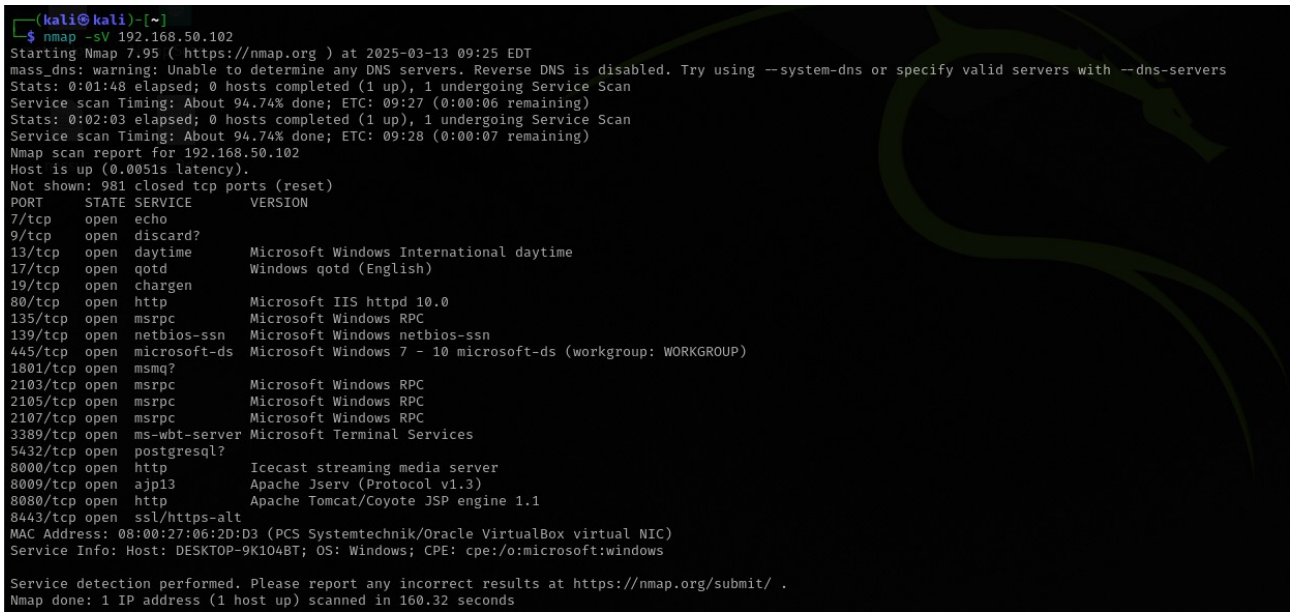


(configurazione di rete della macchina attaccante)

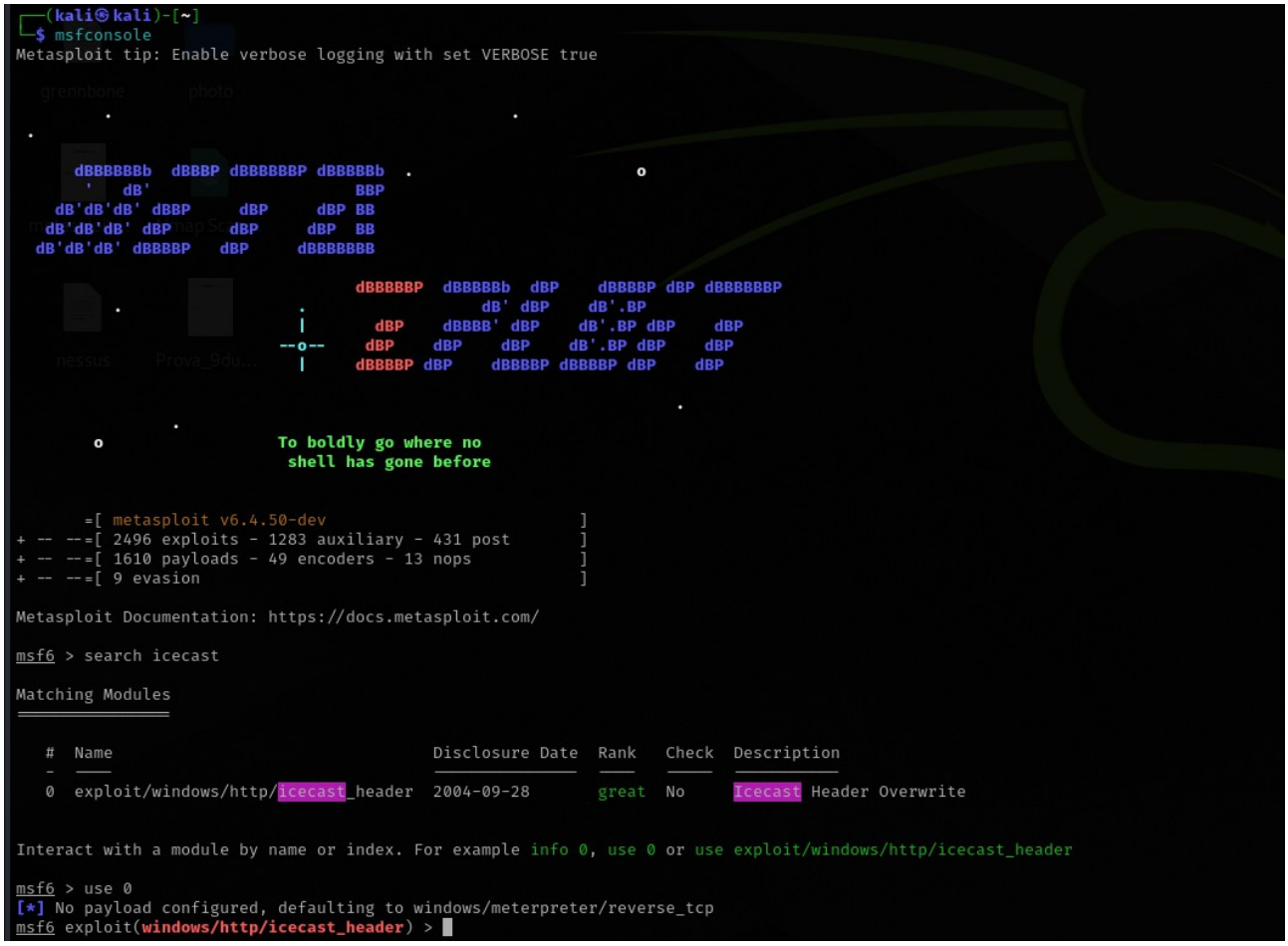
Con Netdiscover troviamo la macchina target, che ha IP 192.168.50.102



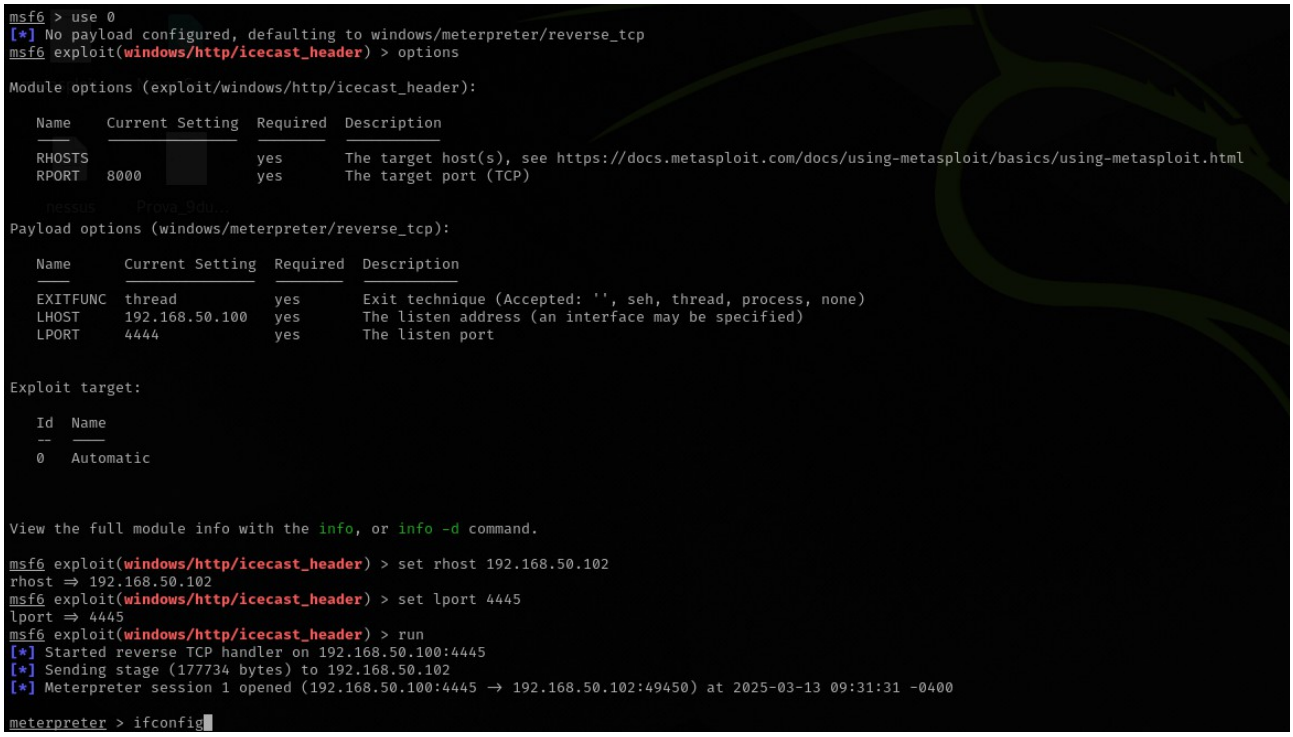
Con il comando nmap -sV 192.168.50.102 vediamo che il servizio Icecast Streaming media server è attivo, sarà il servizio che utilizzeremo per effettuare l'attacco.



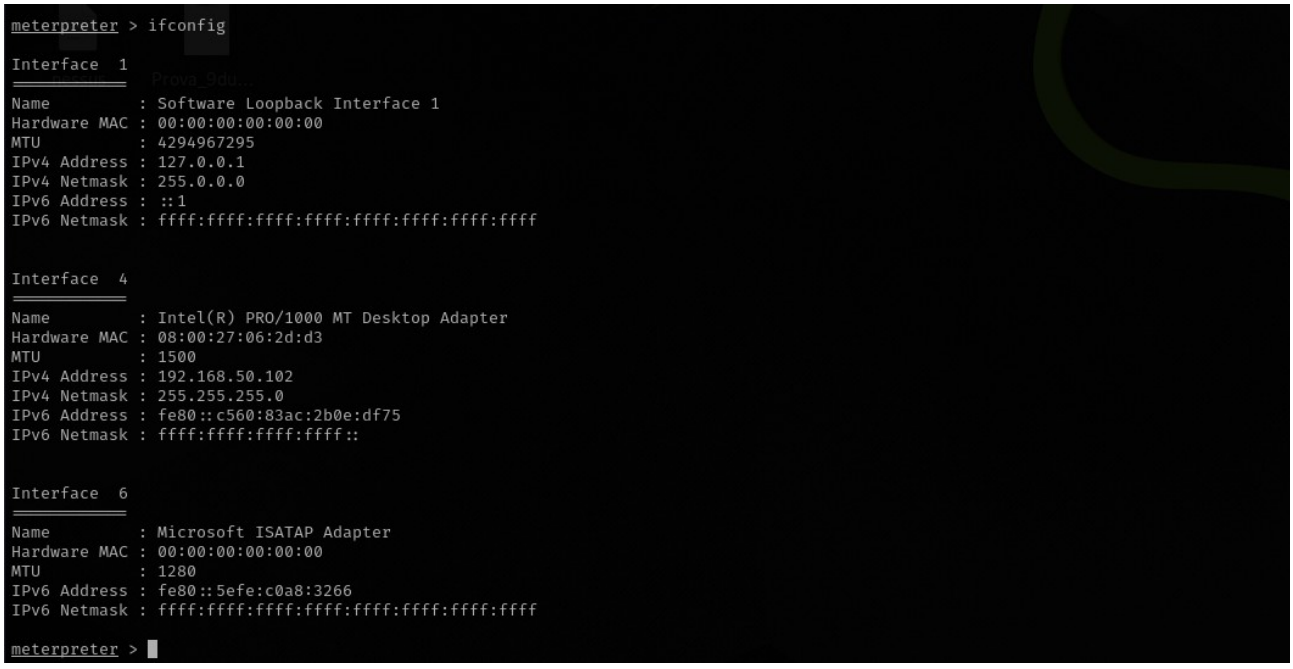
Su Metasploit cerchiamo un exploit che possa aiutarci con il servizio Icecast



Dopo aver configurato l'exploit con l'IP target su RHOSTS, lo lanciamo con il comando run.



L'exploit ha successo e si apre una sessione Meterpreter. Con il comando ifconfig riusciamo a vedere l'IP della vittima.



Con il comando screenshot riusciamo a salvare sulla nostra macchina una fotografia della macchina target.