ESERCIZIO S7 L4

EPICODE

Esercizio
Hacking Windows

Traccia:

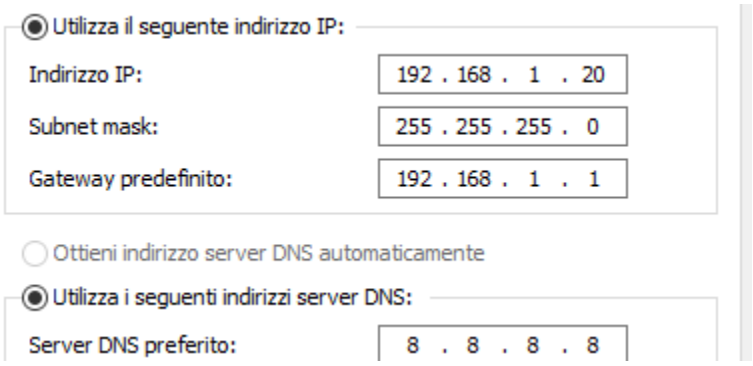
Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit.
Una volta ottenuta la sessione, si dovrà:

- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast già presente nella iso.

SVOLGIMENTO

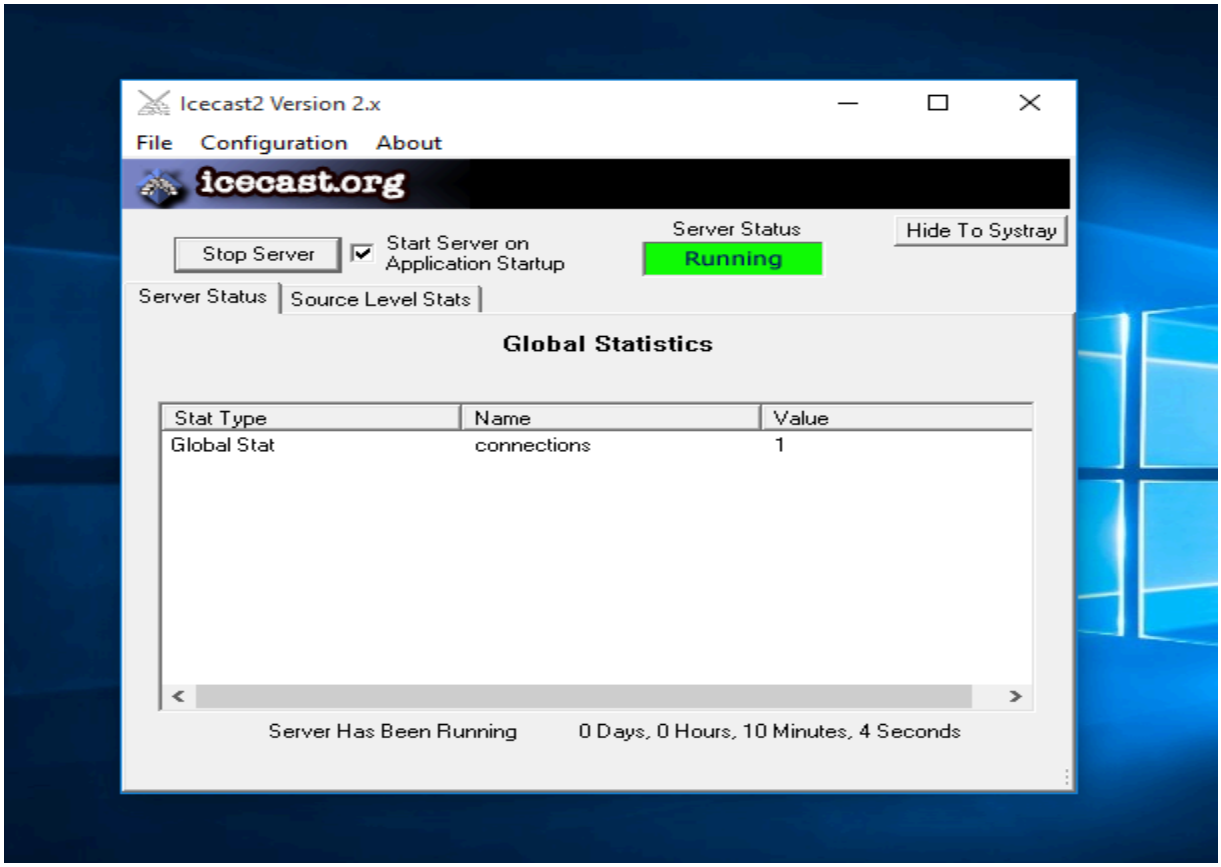
Come passo iniziale configuro la macchina target Windows 10 Pro Metasploitable sulla stessa rete interna della macchina attaccante Kali (IP 192.168.1.25) da GUI >>> Impostazioni di rete >>> inserendo l' IP **192.168.1.20**



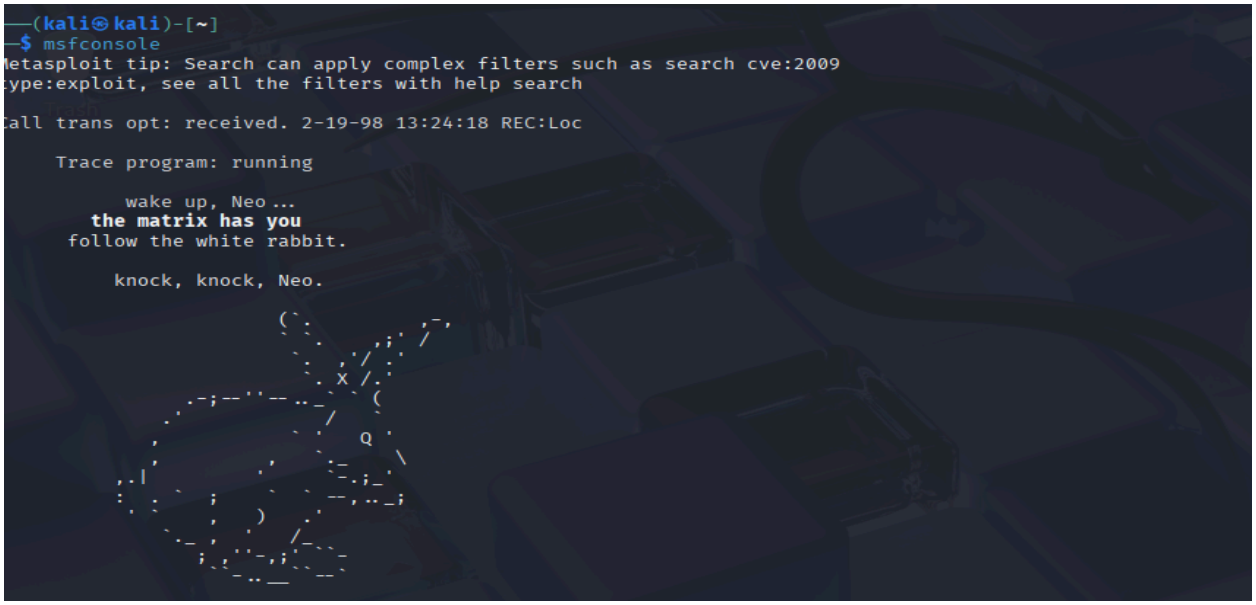
Successivamente testo la comunicazione tra le macchina con il comando **ping**:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=1.56 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=128 time=0.872 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=128 time=0.613 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=128 time=0.623 ms
```

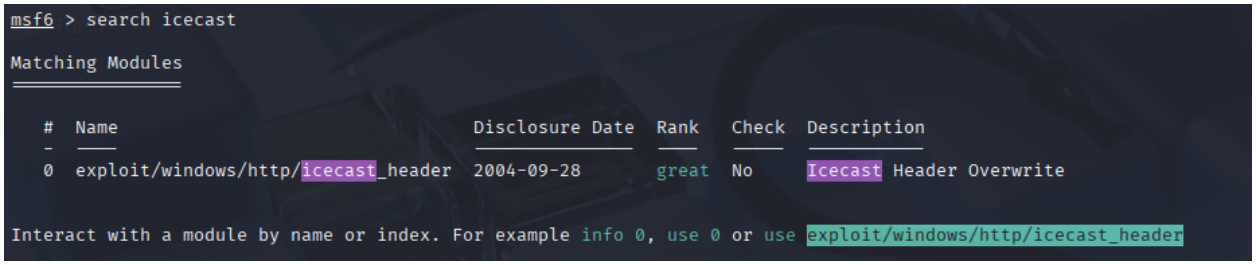
Intanto dall macchina target Windows 10 avvio correttamente il programma Icecast :



Passo adesso sulla macchina attaccante Kali Linux ed apro la console Metasploit Framework con il comando **msfconsole** :

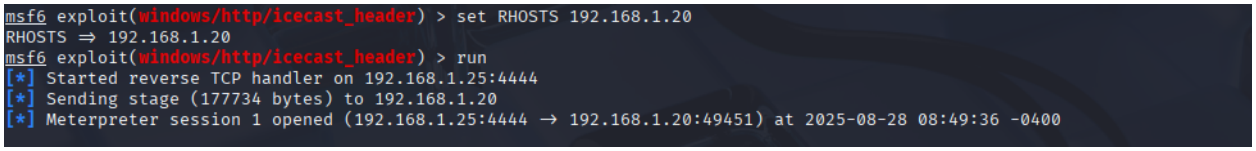


Successivamente, seguendo la richiesta della traccia vado a cercare exploit specifici per **Icecast** con il comando **search** :

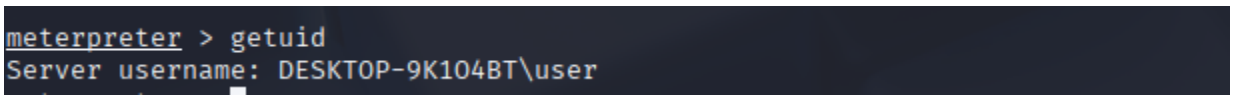


A questo punto, digito **show options** per visualizzare le opzioni, scelgo di utilizzare **exploit/windows/http/icecast_header** con il commando **use** e configuro le opzioni per poi ottenere una sessione Meterpreter con **set RHOSTS + IP macchina target (192.168.1.20)** :

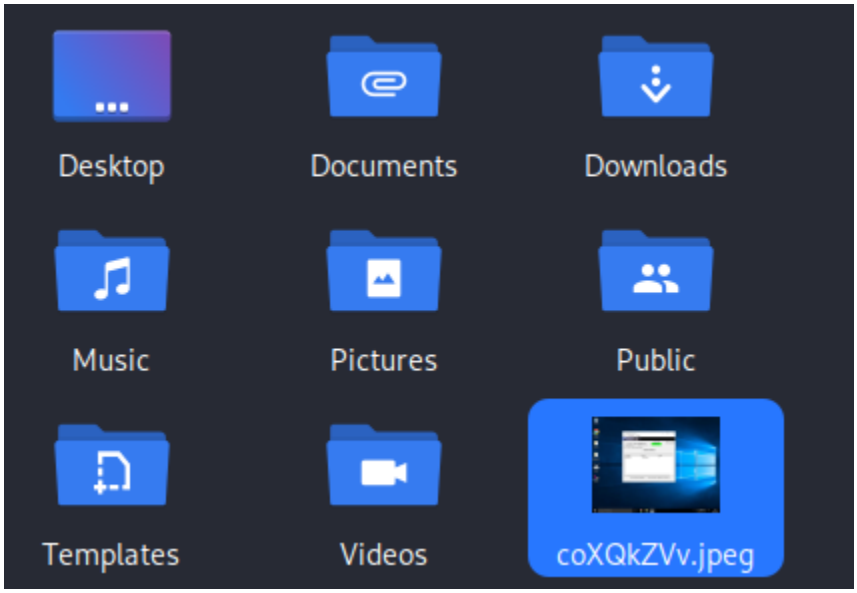
Avvio l'exploit con il comando **run** :

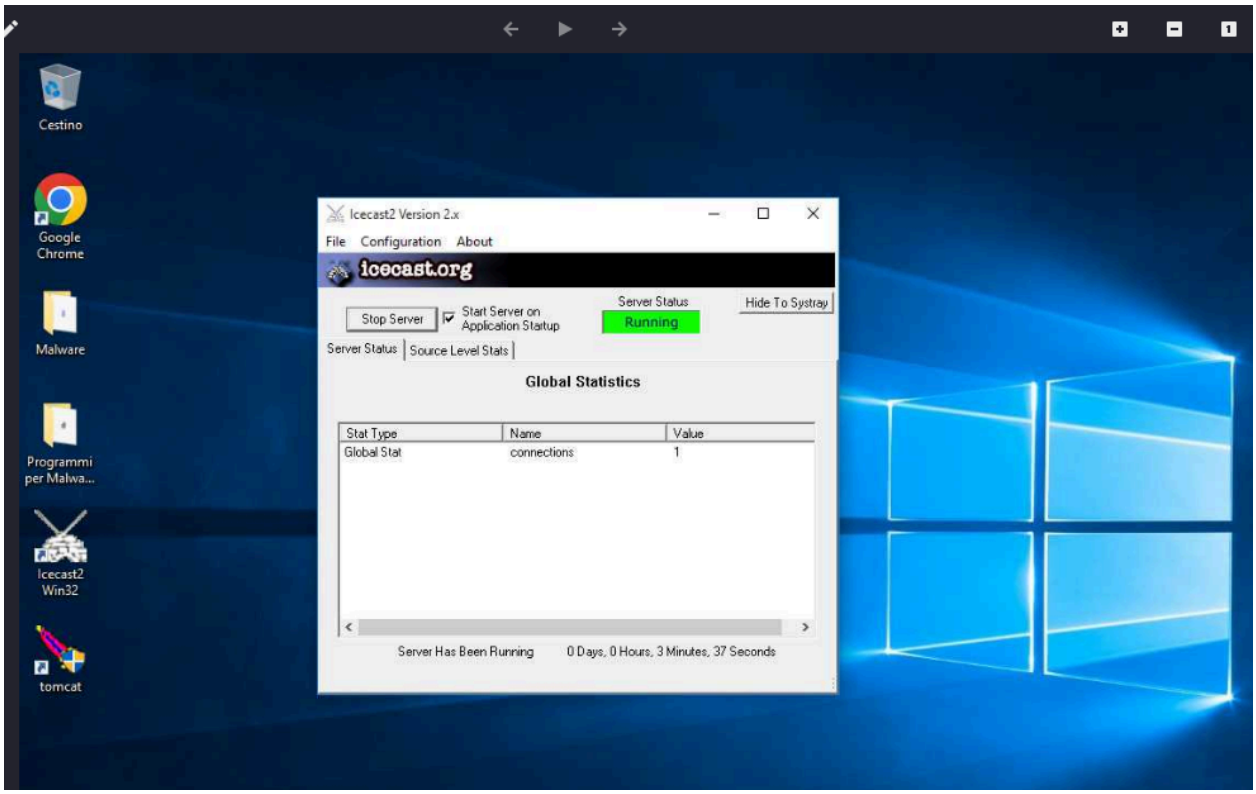


Una volta aperta la sessione di Meterpreter digito **getuid** per mostrare l'utente con cui sto eseguendo la sessione sulla macchina compromessa e inserisco il comando **screenshot** per ottenere lo screenshot della pagina corrente della macchina target Windows 10 :

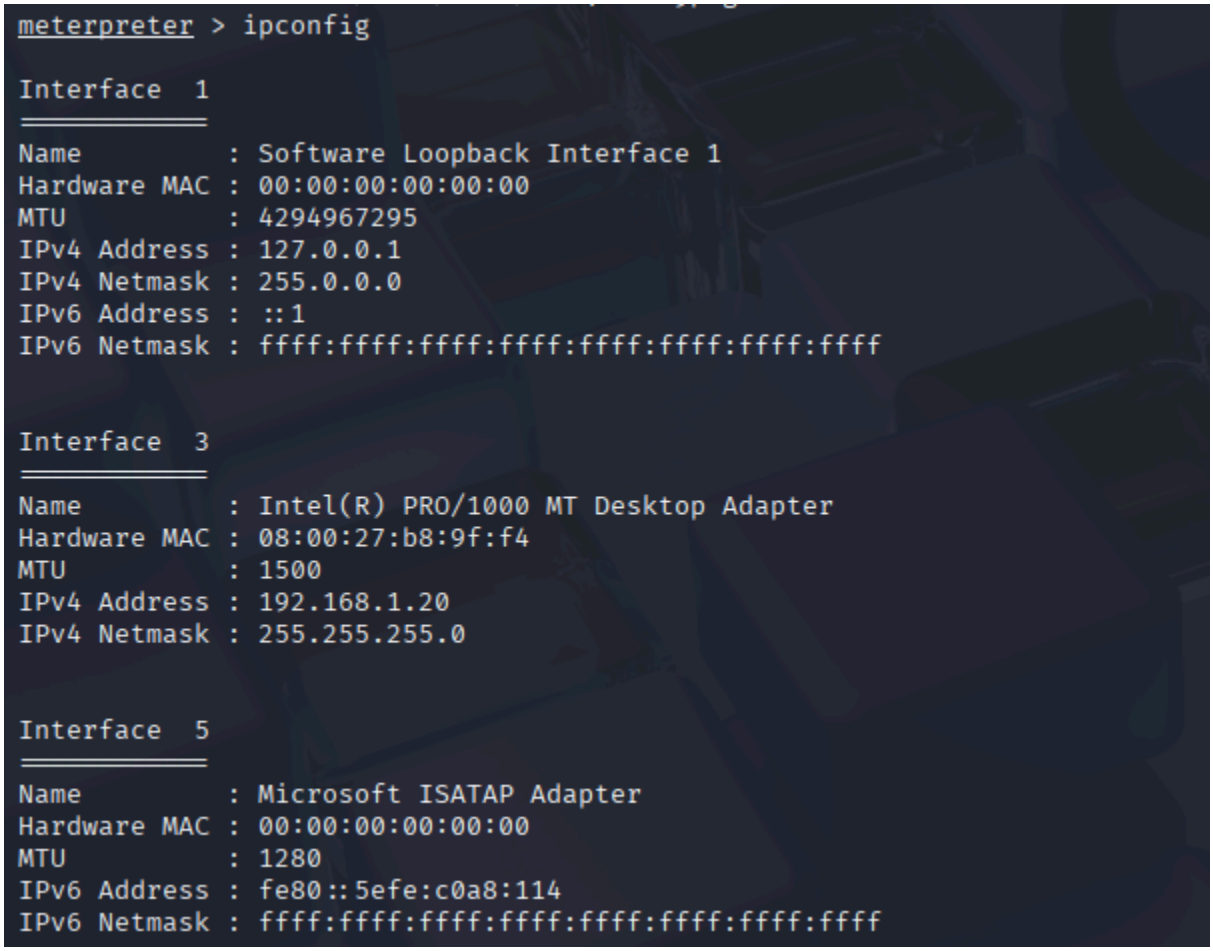


Ora, avrò il file dello screenshot della macchina target salvato nella macchina attaccante Kali :





Come ultimo step a conferma di avere i comandi di windows 10 utilizzo il comando **ipconfig**



CONCLUSIONE

Con questa esercitazione ho potuto mettere in pratica l'utilizzo di Metasploit per sfruttare una vulnerabilità su Windows 10, ottenendo una sessione Meterpreter. Ho imparato a interagire con la macchina compromessa verificando l'indirizzo IP della vittima e recuperando uno screenshot tramite la sessione. L'attività mi ha permesso di comprendere meglio il flusso di un attacco in ambiente controllato e di familiarizzare con alcuni comandi di Meterpreter.