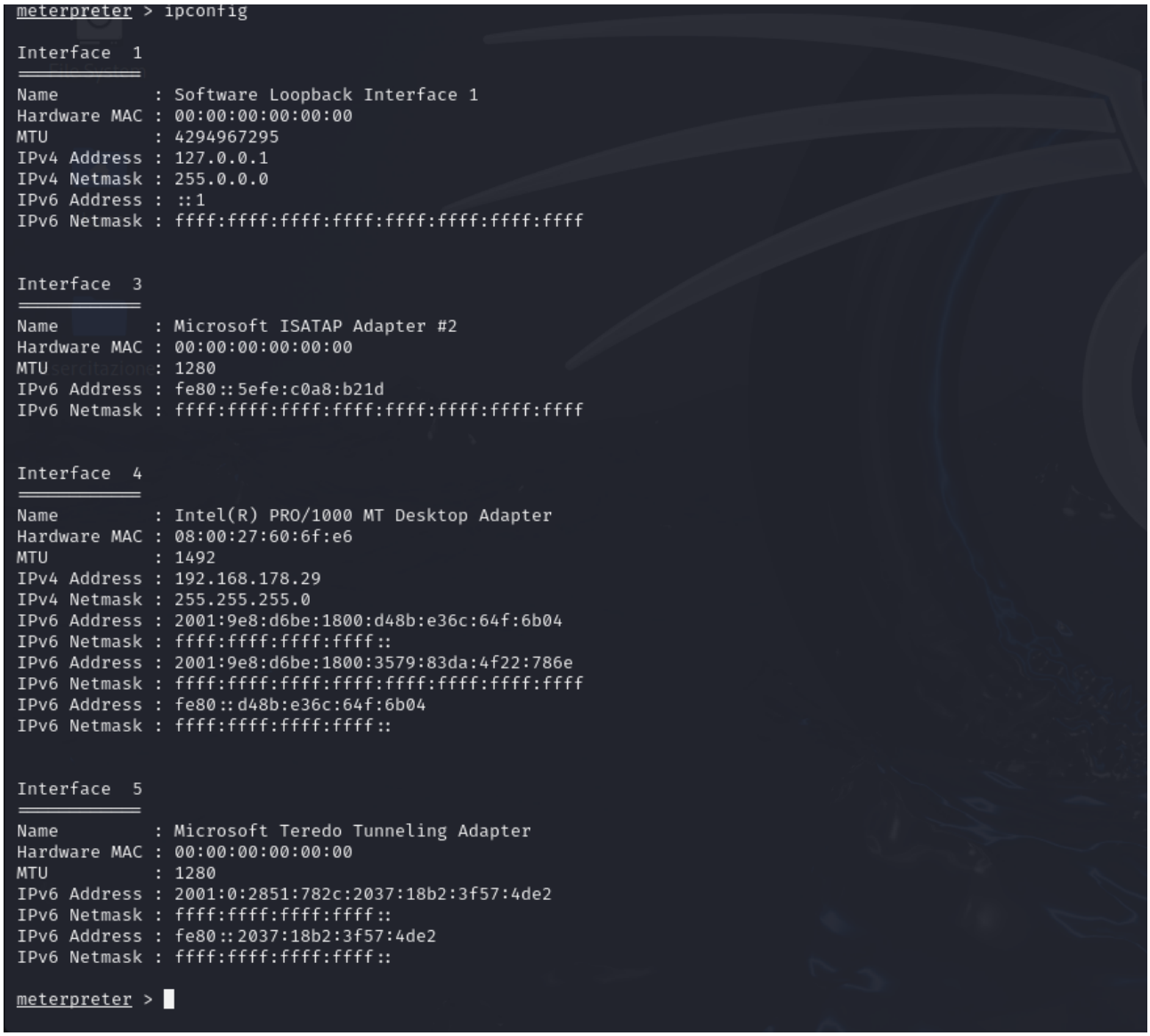
Metasploit Windows

Nell'esercitazione odierna è stato effettuato un attacco verso una macchina **VM windows 10**. Mentre le esercitazioni erano rivolte verso i sistemi Linux, oggi è invece ci si è concentrati su un sistema Windows, sfruttando una vulnerabilità presente nel software Icecast.

Una volta individuato sul tool metasploit, tramite il comando **search Icecast**, l'exploit da utilizzare, esso è stato settato correttamente inserendo rhost lhost e la porta da utilizzare. Una volta scelto e settato il payload si è in seguito proceduto con l'attacco.

Icecast è un software libero per creare server di media streaming che permette di inviare flussi di dati audio/video ai dispositivi che ne fanno richiesta, ad esempio, permettendo di creare una Web radio.

Questo software presenta però una vulnerabilità che potrà essere sfruttata tramite il **Tool Metasploit**.



Una volta fatto partire l'exploit l'attacco inizierà fornendo a noi attaccanti una sessione di **meterpreter** dalla quale potremo impartire comandi alla macchina bersaglio come ad esempio **ipconfig**, per poter appurare che l'attacco ha avuto successo.

Da notare che avendo effettuato un attacco per entrare tramite il software Icecast, nel momento in cui esso verrà terminato la nostra sessione verrà terminata, ragion per cui sarebbe ottimale eseguire il

comando **migrate** in modo da spostarsi su un'applicazione o file system che sia più "stabile", che non possa venire chiusa da un momento all'altro. La funzione ideale sarebbe quella di spostarsi su un file come *System*, ma che per il quale si dovrà avere l'autorità di root, la quale per essere raggiunta, necessita l'utilizzo di più exploit volti ad effettuare una **privilege escalation.**

Nell'esercitazione odierna sono stati visti un po' di comandi tramite **meterpreter**, tra cui il comando **screenshot**, con il quale abbiamo salvato una immagine del Desktop della macchina vittima.