S7-L4

TRACCIA

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

● Vedere lʼ indirizzo IP della vittima.

● Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast già presente nella iso.

SVOLGIMENTO

Molto semplicemente una volta che ci siamo accertati che la macchina di windows 10 pro abbia il programma di icecast e che la nostra macchina kali e windows pingano possiamo procedere con :

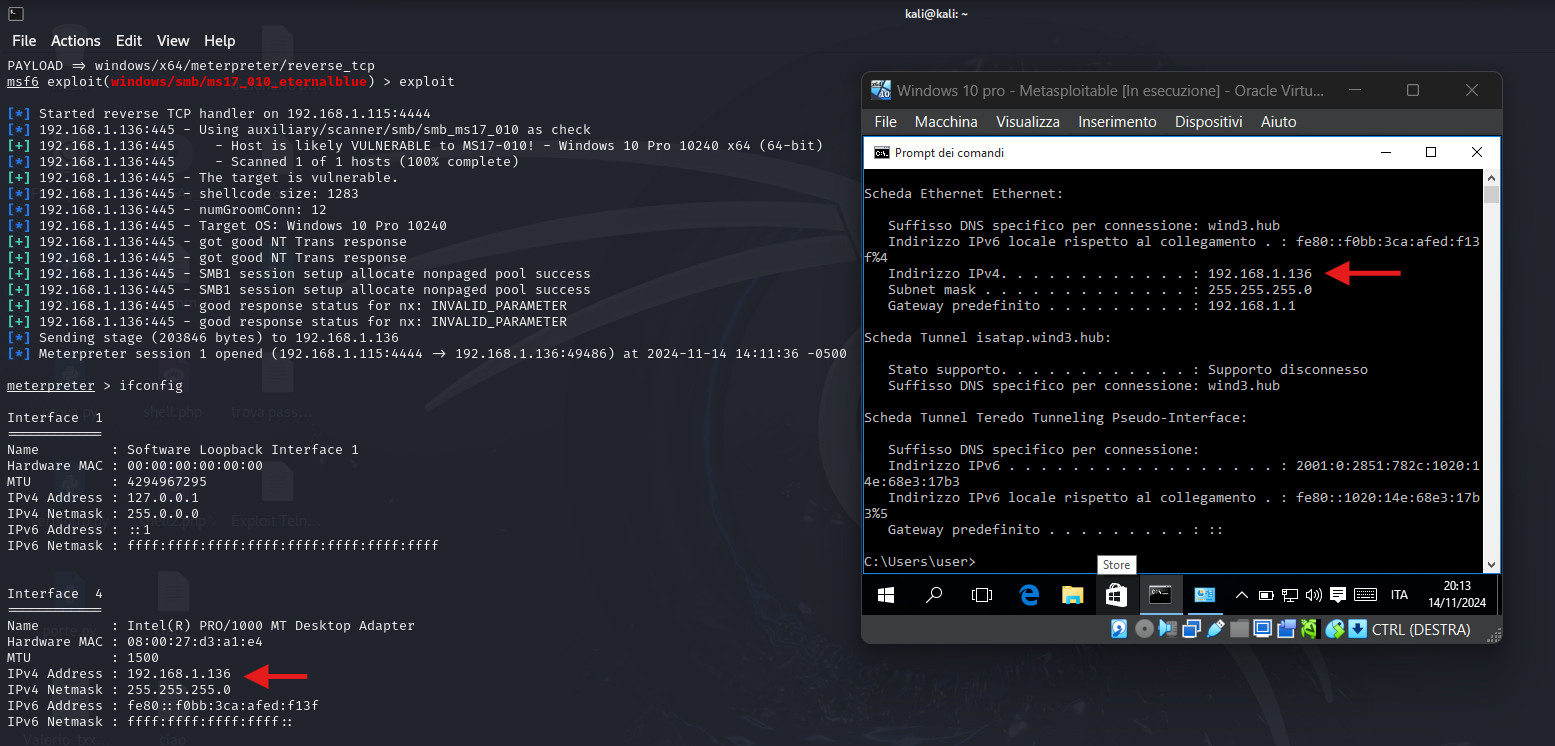
search icecast

potremmo usare l’exploit che ci ha trovato e da li inserire sulle opzioni l’ip della macchina vittima e manderemo l’attacco con il comando :

exploit

adesso per vedere l’ip potremmo sulla nostra macchina basterà mandare il comando:

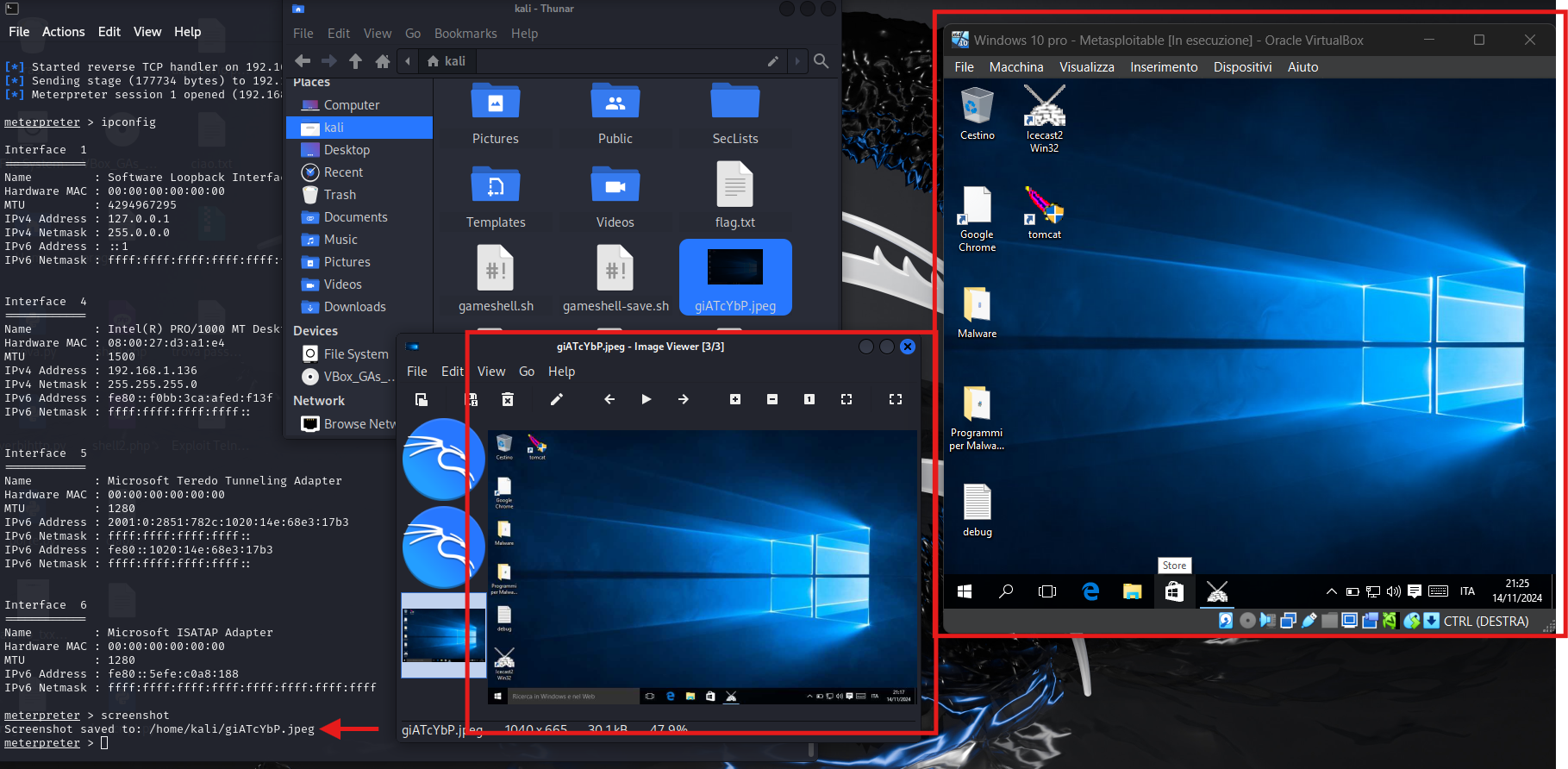
ifconfig



Adesso per vedere lo screenshot della macchina vittima basterà mandare il comando:

screenshot

e da qui ci verrà fornito il percorso per trovare lo screenshot della vittima.



Icecast è un software open-source per la creazione di server di streaming audio e video, particolarmente utilizzato per la trasmissione di contenuti audio come radio online. Sviluppato dalla Xiph.org Foundation, supporta vari formati di streaming, inclusi MP3, Ogg Vorbis\*,Opus e WebM, ed è compatibile con molti player multimediali. Icecast consente la creazione di flussi live o registrati, rendendolo popolare per le stazioni radio Internet e i servizi di trasmissione audio.

Funziona su una varietà di sistemi operativi (Linux, Windows e macOS) e consente agli amministratori di gestire più flussi, configurare mount points (punti di connessione per stream separati) e impostare restrizioni di accesso. Tuttavia, versioni più vecchie di Icecast sono vulnerabili ad alcuni exploit di sicurezza, motivo per cui viene spesso utilizzato come esempio in esercitazioni di penetration testing.