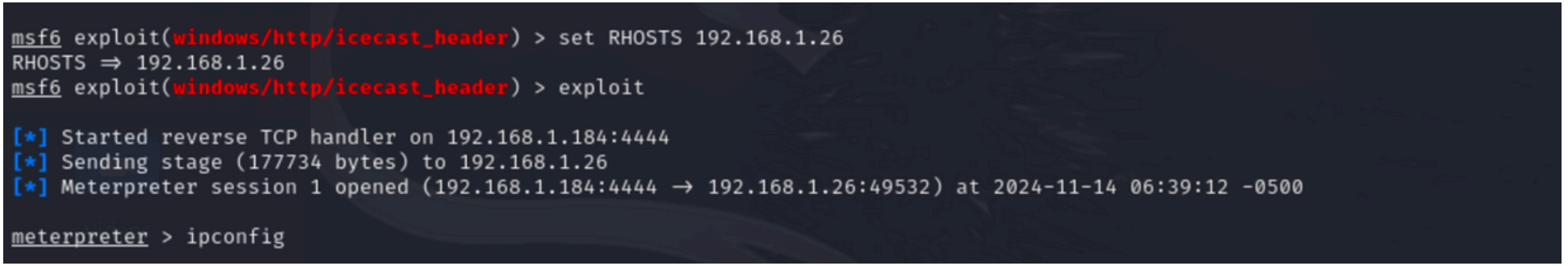
ESERCIZIO S7/L4

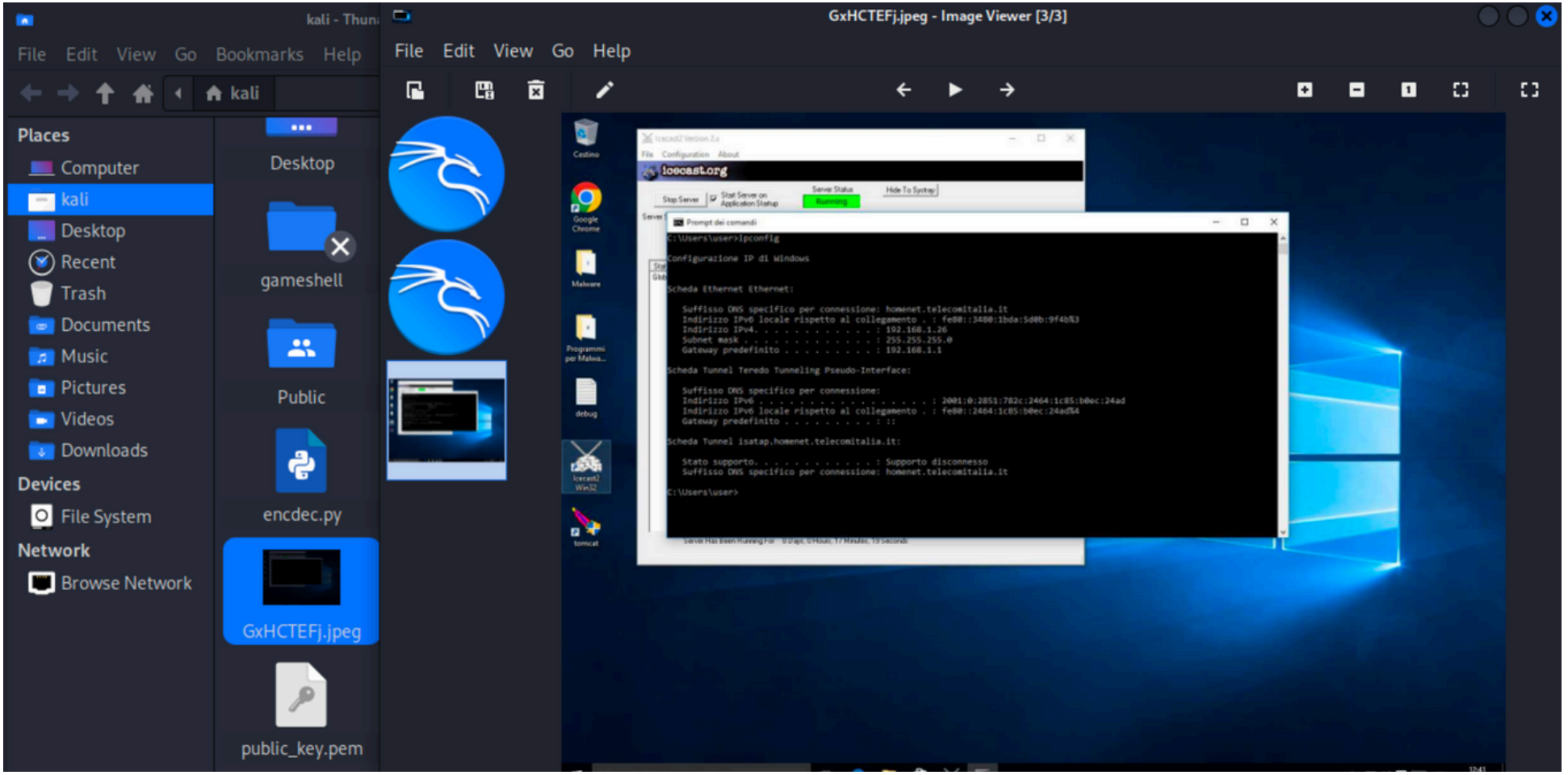
L’esercizio di oggi consisteva nelll’ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit, per poi visualizzare l’indirizzo IP vittima e recuperare uno screenshot tramite la sessione Meterpreter.
il programma da exploitare è Icecast che è un software open-source per lo streaming audio in tempo reale su Internet. Viene utilizzato per creare e gestire stazioni radio online, ma può essere utilizzato anche per lo streaming di altri contenuti audio
Per un attaccante, prendere il controllo di una macchina che sta eseguendo Icecast può essere vantaggioso per diversi motivi, sia per sfruttare la vulnerabilità del sistema che per utilizzare il server compromesso a scopi malevoli.

Una volta lanciato Metasploit con il comando << msfconsole >> andiamo a cercare, con il comando << search icecast >> gli exploit disponibili per il programma in esecuzione che vogliamo attaccare, in questo caso icecast. (Immagine pagina 1)



Andiamo a settare IP della vittima con << set RHOSTS 192.1687.1.26 >> che sarebbe l'indirizzo IP della macchina di windows 10, e lanciamo l'attacco con il comando exploit.

Con << ipconfig >> vediamo l'indirizzo IP della vittima e ci da la conferma che siamo ddentro la sessione della macchina Windows. A questo punto con il comando << screenshot >> effettuiamo uno scatto del Desktop della vittima come possiamo vedere nell'immagine nella pagina successiva.



Conclusione

In questo esercizio, abbiamo sfruttato una vulnerabilità in Icecast per ottenere l'accesso remoto a una macchina Windows 10, utilizzando il framework Metasploit per lanciare un attacco e ottenere una sessione di Meterpreter. Una volta acquisito l'accesso, abbiamo eseguito due operazioni principali: visualizzare l'indirizzo IP della vittima e recuperare uno screenshot tramite la sessione Meterpreter.