S7_L3

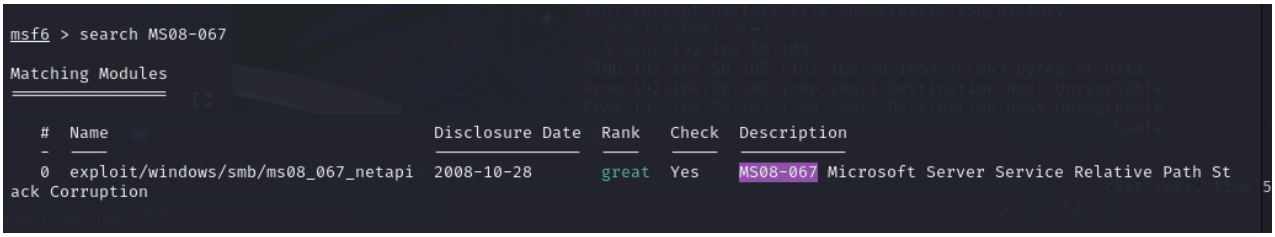
Esercizio

Viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

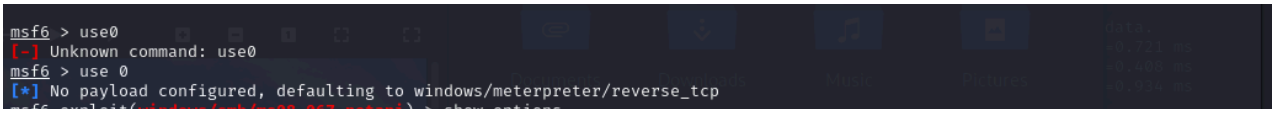
- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Esecuzione

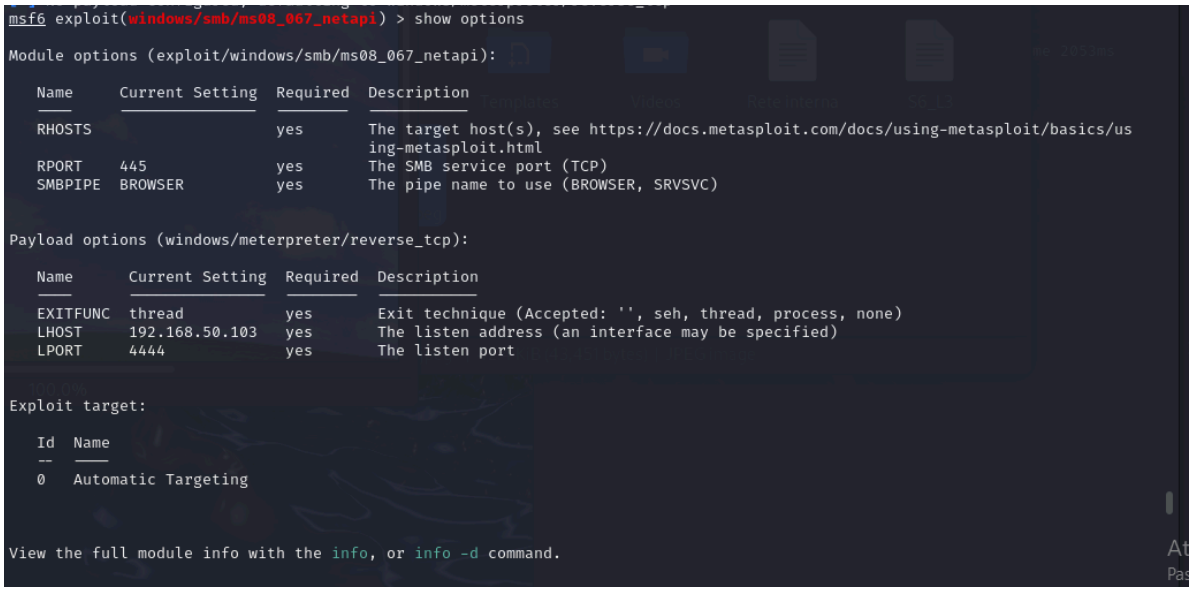
- Dopo aver avviato con successo metasplotable sulla macchina virtuale kali con il comando “msfconsole” abbiamo individuato il modello del exploit tramite la ricerca “search MS08-067”.



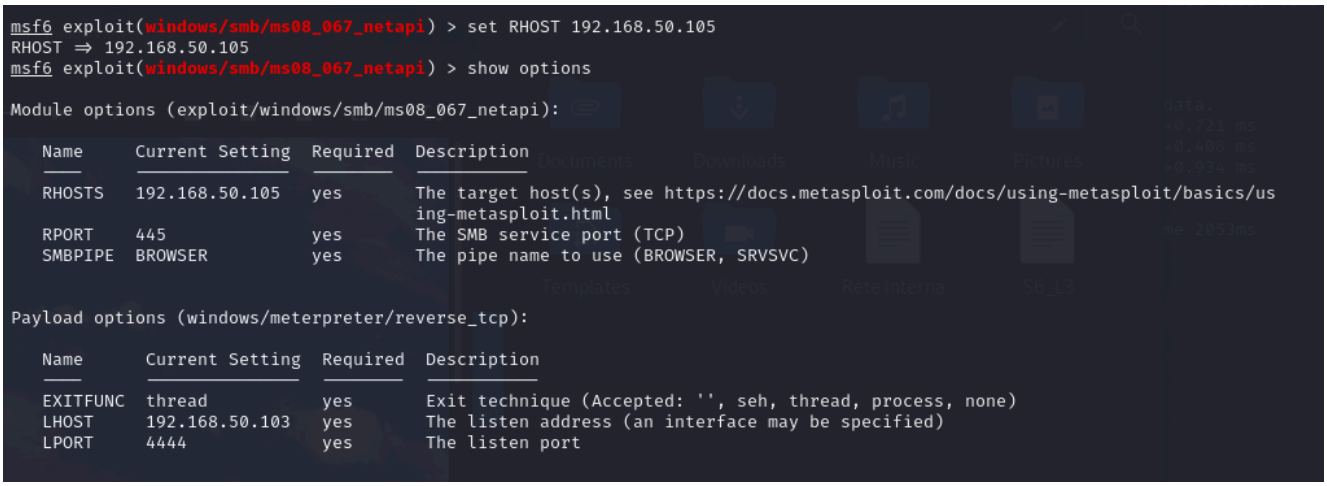
- Per selezionare il modulo abbiamo usato il comando “use 0”, che equivale a “use <nome dell’exploit>”



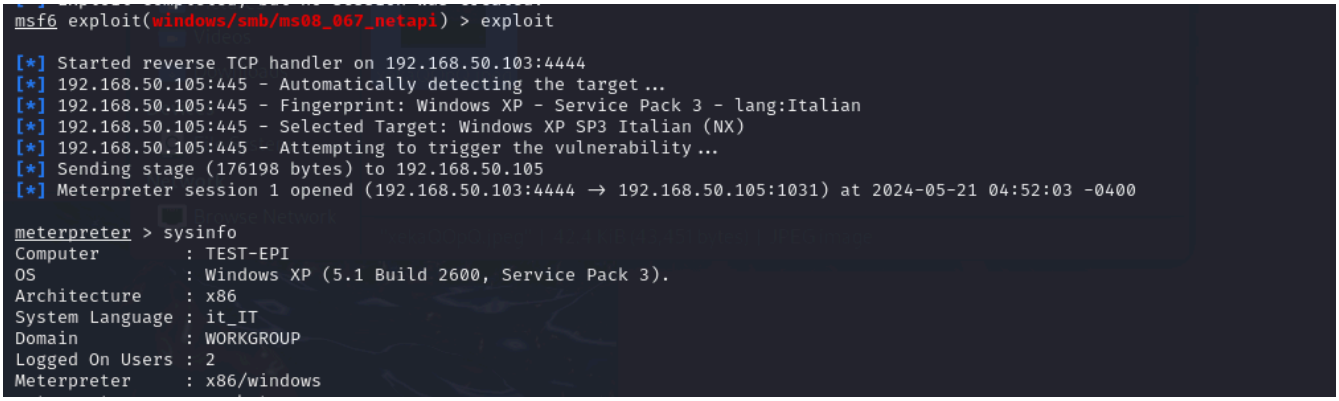
- Con il comando show options abbiamo potuto ottenere le informazioni sull’exploit MS08. In particolare abbiamo potuto osservare quali campi erano neccessari per la riuscita dell’exploit.



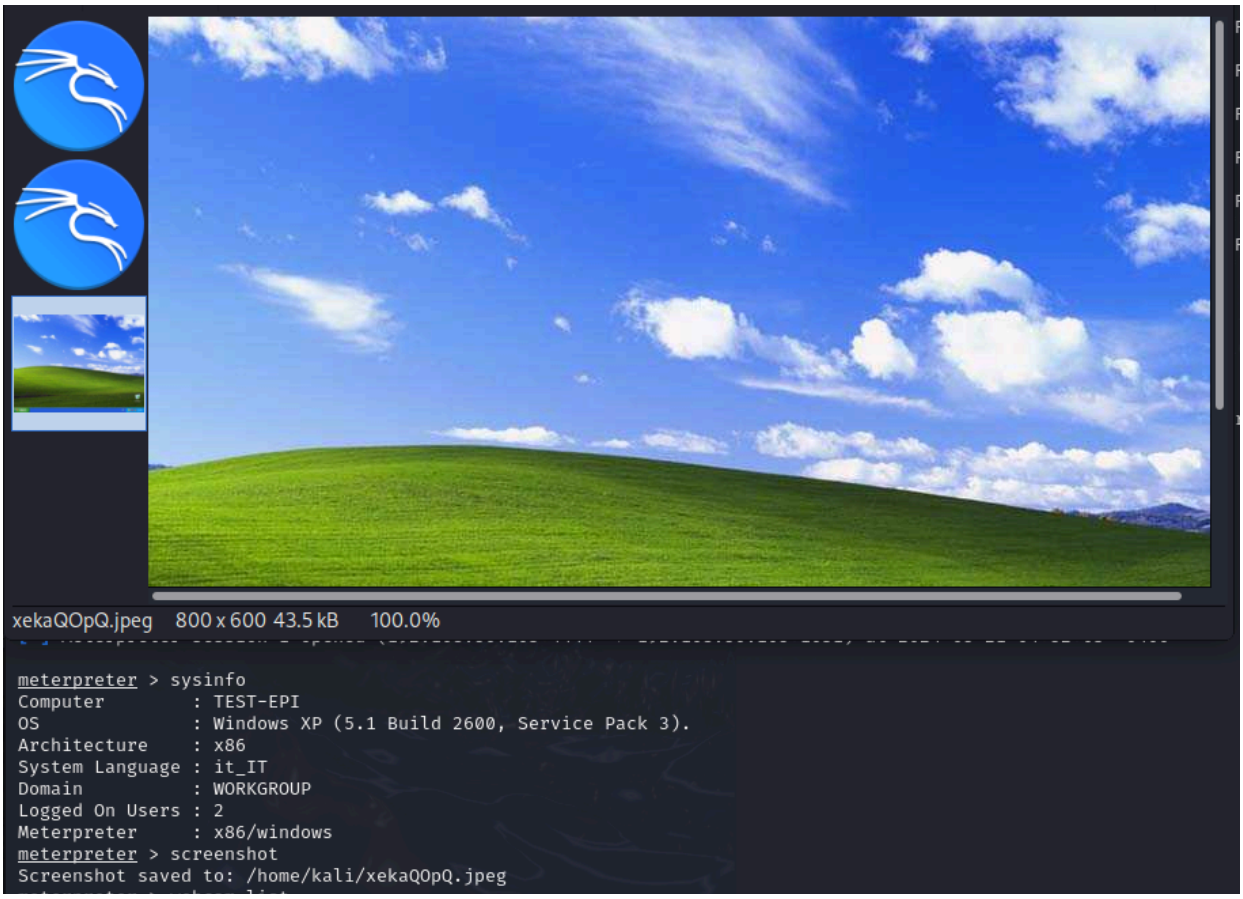
- Abbiamo settato l'indirizzo della nostra macchina target in questo caso "windows XP" con in seguente indirizzo IP "192.168.50.105"



- Dopo aver configurato i dati mancanti abbiamo lanciato l'attacco con il comando "exploit", che fa apparire il prompt "meterpreter" se andato a buon fine.



- Dopo aver confermato che l'attacco è andato a buon fine abbiamo chiesto di eseguire uno "screenshot" andato a buon fine.



- In seguito abbiamo provato con il comando “webcam_list” per controllare se ci fosse una webcam connessa, non è stata riscontrata la presenza di webcam

TEAM 2

Fabio Nobili - Noemi de Martino - Andrea di Benedetto - Mario Reitano - Danilo Malagoli - Samuele Aversa