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).

Possiamo attivare l’interfaccia di Metasploit attraverso il comando MSFCONSOLE.

Per prima cosa attiviamo un NMAP -sV seguito dall’IP della nostra macchina vittima (windowsXP), questo ci darà una scansione dei servizi per rilevare le versioni dei servizi aperti.

L’esercizio richiede di sfruttare la vulnerabilità MS08-067.

Dopo di che, sempre su terminale kali andiamo ad inserire la keywords “search” seguita dal nome della vulnerabilità, da qui otteniamo un elenco di moduli e exploit che sono correlati al servizio.

Per prassi dovremmo testare tutti gli exploit ed una volta individuato quello più idoneo lo utilizziamo con il comando “use” + il suo relativo path; in questo caso ne abbiamo solo 1, corrispondente allo zero. Vediamo quali parametri sono richiesti per lanciare l’attacco, attraverso il comando “show options”. Andiamo a settare l’input richiesto (required) RHOSTS con l’IP della nostra macchina vittima, e attiviamo l’exploit con il suo relativo comando “exploit”.

Da qui per prima cosa con il comando webcam\_list vediamo che non ha trovato nessuna webcam attiva su WindowsXP. Mentre con il comando screenshot andiamo a fare uno screen al desktop della nostra macchina vittima.



Su kali vediamo dove ha salvato lo screenshot e ci comparirà la seguente immagine:

