EPICODE

Esercizio S7 – L3

TRACCIA

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).

SOLUZIONE

Si apre Metasploit e si ricerca la vulnerabilità da utilizzare. Una volta identificata la si richiama (use 0).

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Segue

Si verificano e si settano le informazioni mancanti per effettuare l’exploit. In questo caso si è settato l’ip della macchina vittima (Windows XP).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

A questo punto si fa partire l’exploit. Una volta ottenuta la sessione Meterpreter si usa il comando “ps” per visualizzare i processi in esecuzione sulla macchina vittima. Da qui è possibile identificare il processo di cui si vuole effettuare lo screenshot.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Si è scelto di simulare una situazione di utilizzo delle mail da parte della vittima. Identificato il processo Outlook con il pid 1212 si è effettuata la migrazione sul processo. Si è quindi utilizzata un’estensione di Meterpreter (Espia) per poter effettuare lo screenshot con il comando “screengrab”.  
Si è inoltre verificata la non presenza di webcam sulla macchina vittima tramite il comando “webcam\_list”.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Nell’immagine è riportato lo screenshot effettuato. Si è notato che lo screenshot è stato salvato all’interno di Kali Linux nella directory da cui si è aperto Metasploit e da cui si è lanciato l’attacco.

Immagine che contiene testo, software, schermata, Icona del computer

Descrizione generata automaticamente