Cisco CyberOps

PREPARAZIONE

La parte pratica si basa su due VM, disponibili a questi link:

- https://drive.google.com/file/d/1wMeMzdRPvz5pwLJgJnLwMsw8-g98b22Q/view?usp=sharing
- https://drive.google.com/file/d/1dB1nxaJFF0V805LnNxUzOrKHUlrs2hx1/view?usp=sharing Guida
- https://itexamanswers.net/115-lab-installing-the-virtual-machines-answers.html

Laboratorio:

Esplorazione di Processi, Thread, Handle e Registro di Windows

- In questo laboratorio, completerai i seguenti obiettivi:
    - Esplora i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite.
    - Utilizza il Registro di Windows per modificare un'impostazione.

- https://itexamanswers.net/3211-lab-exploring-processes-threads-handles-and-windows-regi stry-answers.html

Relazione

Per eseguire il compito, ho avviato la vm di Windows 10, ho scaricato SysinternalsSuite all'interno della vm, ho aperto la cartella ed ho avviando il file procexp.exe.
Mi sono recato su HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer, dove ho individuato la chiave EulaAccepted.
Questa era inizialmente impostata su 0x00000001 (1), valore che indica l'accettazione del contratto di licenza.
Dopo aver aperto la chiave con un doppio clic, ho modificato il valore dei dati da 1 a 0, il che rappresenta il mancato accettamento dell'EULA.
Dopo la modifica, ho verificato che la colonna "Dati" mostrasse il nuovo valore 0x00000000 (0).
Infine, ho riaperto Process Explorer dalla cartella SysinternalsSuite, avviando il file procexp.exe. Come previsto, si è aperta la finestra di dialogo del contratto di licenza (EULA), confermando che il programma aveva riconosciuto la modifica effettuata nel registro.
Questo passaggio è stato utile per comprendere come il sistema risponda ai cambiamenti apportati alle sue impostazioni.
Questo laboratorio mi ha permesso di acquisire maggiore dimestichezza con l'analisi dei processi e la manipolazione del Registro di Windows. L'intero processo è stato utile per migliorare la mia comprensione pratica degli strumenti e delle tecniche utilizzate per monitorare e configurare il sistema operativo.

Daniel_Gabriel_Costeanu