S11L2

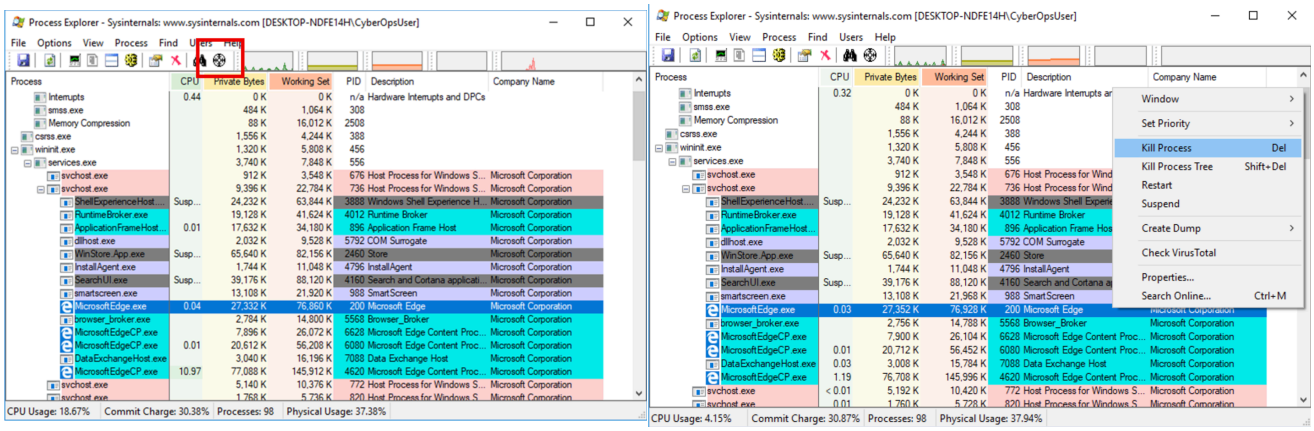
Cisco Cyber Ops giorno 1

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.

Esercizio Pratico

Per iniziare, scarica la suite SysInternals dal sito ufficiale Microsoft. Una volta completato il download, estrai il contenuto del file compresso in una cartella sul tuo computer. Mantieni aperto il browser web, poiché potrebbe essere utile nei passaggi successivi.

Apri la cartella dove hai estratto i file e avvia l'applicazione chiamata "procexp.exe". Quando viene richiesto, accetta il contratto di licenza di Process Explorer. A questo punto, vedrai una lista di processi attivi sul tuo sistema. Per identificare un processo specifico, ad esempio quello del tuo browser web, usa l'icona di ricerca di Process Explorer. Trascinala sopra la finestra del browser aperta. Una volta individuato il processo, puoi decidere di terminarlo facendo clic con il tasto destro del mouse, selezionando l'opzione "Kill Process" e confermando con "OK". Noterai che la finestra del browser si chiuderà.



Ora puoi avviare un altro processo. Apri il prompt dei comandi cercando "Command Prompt" nel menu Start e selezionalo. Utilizzando nuovamente l'icona di ricerca di Process Explorer, individua il processo associato al prompt dei comandi, chiamato "cmd.exe". Osserva che questo processo è figlio del processo "explorer.exe" e può a sua volta generare un processo figlio, come "conhost.exe". Nel prompt dei comandi, lancia un comando di ping e osserva le modifiche sotto il processo "cmd.exe" in Process Explorer. Noterai l'apparizione di un processo figlio chiamato "PING.EXE". Se necessario, verifica la sicurezza del processo "conhost.exe" cliccando con il tasto destro su di esso e selezionando "Check VirusTotal". Accetta i termini di servizio e consulta i risultati nel browser.

Per esplorare thread e handle, apri il prompt dei comandi e torna a Process Explorer. Clicca con il tasto destro su "conhost.exe", seleziona "Properties" e vai alla scheda

"Threads" per esaminare i thread attivi. Qui troverai informazioni sulle variabili di ambiente, sulla sicurezza e sulle prestazioni del thread. Successivamente, attiva la vista degli handle dal menu "View" selezionando "Lower Pane View > Handles". Osserva che gli handle possono puntare a file, chiavi di registro o thread.

Per esplorare il Registro di Windows, avvia l'Editor del Registro digitando "regedit" nella barra di ricerca e confermando l'accesso. Naviga attraverso la struttura gerarchica per trovare la chiave associata a Process Explorer. Vai in "HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer" e individua la chiave "EulaAccepted". Fai doppio clic su di essa per modificarne il valore. Se il valore è impostato su "1", significa che l'accordo di licenza è stato accettato. Cambialo in "0" per indicare che non è stato accettato. Conferma con "OK" e chiudi l'Editor del Registro.

Infine, riapri Process Explorer dalla cartella della suite SysInternals. Noterai che, a causa della modifica nel registro, l'applicazione mostrerà nuovamente la finestra di dialogo del contratto di licenza.