ESERCIZIO: Esplorazione di Processi, Thread, Handle e Registro di Windows

Esplorare un processo attivo

- ***Cosa è successo alla finestra del browser web quando il processo è stato terminato?***

Facendo Kill Process alla finestra del browser web, essa viene chiusa in maniera forza.

Avviare un altro processo

- ***Cosa è successo durante il processo ping?***

Durante il ping nel prompt dei comandi su Process Explorer vedo che viene eseguito il processo Ping.exe, comando ping TCP/IP.

- ***Cosa è successo al processo figlio conhost.exe?***

Facendo clic con il pulsante destro sul processo cmd.exe e selezionando Kill Process il processo figlio conhost.exe viene chiuso insieme a cmd.exe

Esplorare i thread

- ***Che tipo di informazioni sono disponibili nella finestra Proprietà?***

Nella finestra Proprietà esaminando la scheda Threads si vedono i dettagli dei singoli thread per il processo conhost.exe.

Count: Indica che quanti thread attivi ha il processoi.
TID (Thread ID): è l'identificativo unico del thread.
CPU: indica l'utilizzo della CPU per il thread.
Cycles Delta: indica la differenza nei cicli di CPU dall'ultimo aggiornamento.
Suspend Count: Il numero di volte in cui il thread è stato sospeso.
Start Address: L'indirizzo di memoria da cui il thread ha iniziato l'esecuzione.

Il pannello inferiore fornisce dettagli molto più granulari del thread.
Thread ID: identificativo del thread.
Start Time: l'ora e la data esatta in cui il thread è stato avviato.
State: indica lo stato attuale del thread. "Wait:Executive" significa che il thread è in attesa di un oggetto kernel o di un'operazione del sistema operativo. Questo è uno stato comune per i thread che non stanno attualmente eseguendo codice e sono in attesa che qualcosa accada (ad esempio, input, un evento, I/O disco/rete, ecc.).
Kernel Time: il tempo totale che il thread ha trascorso in modalità kernel (eseguendo codice del sistema operativo).
User Time: il tempo totale che il thread ha trascorso in modalità utente (eseguendo codice dell'applicazione). Quando è zero, combinato con "Wait:Executive", suggerisce che il thread è inattivo o in attesa di un evento e non sta consumando CPU attivamente.
Context Switches: il numero di volte in cui il sistema operativo ha dovuto cambiare il contesto della CPU per eseguire un altro thread e poi tornare a questo.
Cycles: Il numero totale di cicli di CPU che questo thread ha consumato dalla sua creazione. Nonostante i tempi kernel/user siano zero, questo mostra i cicli cumulativi.
Base Priorityla priorità di base assegnata al thread.
Dynamic Priority: la priorità dinamica corrente, che può variare in base all'attività del thread e alle esigenze del sistema.
I/O Priority: Normal: la priorità delle operazioni di I/O del thread.

Memory Priority: la priorità della memoria del thread, che influenza come Windows gestisce la memoria per quel thread.
Ideal Processor: il processore (core CPU) ideale su cui il sistema preferirebbe eseguire questo thread, per ottimizzare le prestazioni della cache.

- ***A cosa puntano gli handle?***

Gli handle puntano alle risorse gestite dal kernel del sistema operativo.

Esplorazione del Registro di Windows

- ***Qual è il valore per questa chiave di registro nella colonna Dati Data)?***

Il valore per la chiave di registro nella colonna Dati (Data) è 0.

- ***Quando apri Process Explorer, cosa vedi?***

Dopo aver cambiato il valore 1 in 0 per il Value Data aprendo Process Explorer si apre la finestra che chiederà nuovamente l'accettazione dell'EULA.