Esplorazione di Processi, Thread, Handle e Registro di Windows

profilo studente

- **Gabriel Giustinelli**
- **Epicode Cyber Security**
- **classe** CS0525
- **data** 12/02/2026

1. Cosa è successo alla finestra del browser web quando il processo è stato terminato?

Quando si termina un processo (Kill Process) di un'applicazione, il sistema operativo interrompe immediatamente l'esecuzione del codice, quindi la finestra grafica scompare istantaneamente.

2. Cosa è successo durante il processo ping?

Mentre il comando ping è in esecuzione nel terminale, appare un processo figlio sotto cmd.exe, ovvero: PING.EXE e una volta terminato il comando il processo figlio sparisce.

3. Cosa è successo al processo figlio conhost.exe?

Quando il processo genitore cmd.exe viene terminato, il sistema operativo chiude anche i suoi processi figli associati.

4. Che tipo di informazioni sono disponibili nella finestra Proprietà?

La finestra delle proprietà dei thread è composta da più thread, sono presenti diverse informazioni come: l'ID del thread, lo stato(wait), il tempo di quando è stato creato (user time), e l'indirizzo di inizio del codice (start address).

5. Esaminare gli handle. A cosa puntano gli handle?

Puntano ai file, chiavi di registro e alle porte di comunicazione necessari per far funzionare il processo.

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

Dopo aver modificato il valore di `EulaAccepted` da 1 a 0 nell'editor del registro, la colonna Dati mostra `0x00000000 (0)`.quindi il registro memorizza le configurazioni software in formato esadecimale e decimale.

Quando apri Process Explorer, cosa vedi?

il programma si comporta come se fosse la prima volta che lo avvio, mostrandomi nuovamente la finestra del contratto di licenza (EULA) da accettare.