S11 - L1
Esplorazione di Processi, Thread, Handle e Registro di Windows

INTRODUZIONE:

Ho analizzato il **funzionamento dei processi Windows utilizzando Process Explorer della suite Sysinternals**. Ho osservato **relazioni tra processi, thread, handle e l'impatto delle modifiche al Registro di sistema** sul comportamento delle applicazioni.

Parte 1 — Esplorazione dei processi

Passo 1 — Scaricare Windows Sysinternals Suite

1. Apro il browser.
2. Vado alla pagina di download della Sysinternals Suite (Microsoft).
3. Scarico il pacchetto **SysinternalsSuite**.
4. Estraggo lo ZIP in una cartella (es. Desktop\SysinternalsSuite).
5. Lascio il browser aperto.

Passo 2 — Esplorare un processo attivo (browser)

1. Entro nella cartella **SysinternalsSuite** estratta.
2. Avvio **procexp.exe**.
3. Accetto l'EULA quando richiesto.
4. In Process Explorer clicco e trascino l'icona **Find Window's Process** sulla finestra del browser aperto: Process Explorer evidenzia il processo del browser.

Domanda: Cosa è successo alla finestra del browser quando il processo è stato terminato?

Risposta: la finestra del browser **si chiude immediatamente** (termina di colpo), perché il processo principale del browser viene ucciso.

Passo 3 — Avviare un altro processo (cmd.exe + ping + VirusTotal)

1. Apro **Prompt dei comandi** (Start → cerco "Prompt dei comandi" → apro).
2. In Process Explorer uso di nuovo **Find Window's Process** trascinandolo sulla finestra del Prompt: viene evidenziato **cmd.exe**.
3. Verifico le relazioni:
    - Processo: **cmd.exe**

- Parent process: **explorer.exe**
- Child process: **conhost.exe**

4. Torno nella finestra del Prompt e avvio un ping (esempio pratico):
   `ping 8.8.8.8` *(oppure un host raggiungibile)*
5. Osservo in Process Explorer cosa cambia sotto **cmd.exe**.

Domanda: Cosa è successo durante il processo ping?

Risposta: mentre il ping è in esecuzione, **cmd.exe rimane attivo** e si vede **attività/aggiornamenti in tempo reale** (variazioni di CPU/IO e/o incremento di eventi/attività del processo). Il comando produce output continuo finché non termina o lo interrompo (Ctrl+C).

6. (Verifica VirusTotal) In Process Explorer clicco destro su **conhost.exe → Check VirusTotal** → accetto Terms → OK.
7. Scorro a destra fino alla colonna **VirusTotal** e clicco sul link per aprire i risultati nel browser.
8. Clicco destro su **cmd.exe → Kill Process**.

Domanda: Cosa è successo al processo figlio conhost.exe?
Risposta: conhost.exe si chiude/termina insieme a cmd.exe, perché è un **processo figlio** legato alla console: quando termina il parent, normalmente viene chiuso anche il child associato.

Parte 2 — Esplorazione di Thread e Handle

Passo 1 — Esplorare i thread (conhost.exe)

1. Apro un Prompt dei comandi (così conhost.exe esiste sicuramente).
2. In Process Explorer clicco destro su **conhost.exe → Properties…**
3. Vado nella scheda **Threads** (se compare un warning, confermo con OK).
4. Esamino i dettagli mostrati.

Domanda: Che tipo di informazioni sono disponibili nella finestra Proprietà?

Risposta: nella finestra **Properties** sono disponibili informazioni tecniche del processo e dei thread, ad esempio:

- dettagli del processo (nome, percorso, command line/parametri, utente, PID/avvio),
- **lista dei thread** con **TID**, stato/attività,
- **start address** e moduli/DLL collegati al thread,
- utilizzo risorse (CPU time, contatori, ecc.), dipende dalla scheda visualizzata.

Passo 2 — Esplorare gli handle (Lower Pane)

1. In Process Explorer vado su **View → Lower Pane View → Handles**.

2. Seleziono **conhost.exe** e osservo nel riquadro inferiore l’elenco degli handle.

Domanda: A cosa puntano gli handle?

Risposta: gli handle puntano a **risorse/oggetti del sistema operativo** usati dal processo, tipicamente:

- file e cartelle,
- chiavi di registro,
- processi/thread,
- sezioni di memoria,
- named pipes,
- oggetti di sincronizzazione (eventi, mutex),
- token di sicurezza, ecc.

3. Chiudo Process Explorer.

Parte 3 — Esplorazione del Registro di Windows

Passo a — Aprire regedit e vedere gli hive

1. Start → cerco **regedit** → apro **Editor del Registro di sistema**.
2. Confermo **Sì** al controllo UAC.
3. Prendo visione dei 5 hive principali.

Passo b/c/d — Modificare EulaAccepted

1. Navigo nel percorso indicato:
   HKEY_CURRENT_USER → Software → Sysinternals → Process Explorer
2. Scorro e trovo la chiave/valore **EulaAccepted** (inizialmente vale 1).
3. Faccio doppio clic su **EulaAccepted**.
4. Cambio il **Value data** da **1** a **0** e confermo con OK.

Domanda: Qual è il valore per questa chiave nella colonna Dati (Data)?

Risposta: dopo la modifica, nella colonna **Data** risulta **0x00000000 (0)**.

Passo e — Riaprire Process Explorer

1. Torno nella cartella **SysinternalsSuite**.
2. Avvio **procexp.exe**.

Domanda: Quando apri Process Explorer, cosa vedi?
Risposta: compare di nuovo la richiesta/finestrella di **accettazione dell'EULA** (come se non fosse mai stata accettata), perché **EulaAccepted** è stato riportato a 0.

CONCLUSIONI FINALI:

L'attività ha confermato come **processi, thread e handle siano strettamente collegati alla gestione delle risorse di sistema.**

Inoltre, **la modifica della chiave di registro ha dimostrato in modo pratico come il Registry influenzi direttamente il comportamento dei programmi** in ambiente Windows.