# S11L2 Luca Calvigioni

# Esplorazione processi, Threads, Handles, e Registri Windows

**Riferimento alla guida:**
https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html

## Esplorazione dei Processi

**Cosa sono i processi?**

Un processo rappresenta un programma in esecuzione sul sistema operativo. Ogni processo ha una serie di attributi come ID, memoria utilizzata, priorità e stato (esecuzione, attesa, sospeso, ecc.). Esplorare i processi ti consente di capire come le applicazioni interagiscono con il sistema e identificare eventuali comportamenti anomali o sospetti.

**Passaggio 1: Scaricare Windows SysInternals Suite**

La suite SysInternals è un insieme di strumenti avanzati sviluppati da Microsoft per analizzare e diagnosticare i sistemi Windows.
**Perché usarla?**

- **Process Explorer** offre una vista dettagliata sui processi attivi e le loro relazioni.
- Può essere utilizzata per identificare processi sospetti, gestire le risorse di sistema e analizzare le dipendenze tra processi.

**Passaggio 2: Esplorare un processo attivo**

Quando apri **Process Explorer**, ottieni una rappresentazione gerarchica dei processi attivi sul sistema. La struttura ad albero mostra:

- **Processi genitori**: quelli che avviano altri processi.
- **Processi figli**: quelli avviati da un processo genitore.

Trascinando l'icona **Find Window's Process** su una finestra del browser, puoi identificare il processo che la controlla.Termina il processo del browser per osservare come il sistema reagisce. Questo è utile per chiudere applicazioni che non rispondono o sono sospette.

**Passaggio 3: Avviare un altro processo**

Ogni volta che esegui un comando nel Prompt dei comandi (cmd.exe), un processo figlio viene generato.

- I processi interagiscono tra loro (genitori e figli).
- Ad esempio, un comando ping genera un processo figlio chiamato **PING.EXE**, visibile sotto il processo genitore **cmd.exe**.
- Con Process Explorer, puoi monitorare in tempo reale queste interazioni.

**Check VirusTotal**

Questa funzione consente di verificare se un processo è sospetto confrontandolo con un database di hash di file noto. Questo è particolarmente utile per analizzare malware o applicazioni non sicure.

---

## Esplorazione dei Thread e degli Handle

**Cosa sono i thread?**

Un thread è la più piccola unità di esecuzione all'interno di un processo. Ogni processo può avere uno o più thread, che condividono la stessa memoria e risorse del processo principale.

- **Esempio**: Un browser web può avere thread separati per caricare pagine, gestire la UI e controllare gli script.

**Analisi pratica con Process Explorer**

- La scheda **Threads** mostra informazioni su ID, stato e utilizzo delle risorse per ciascun thread.
- Esaminando un thread puoi identificare eventuali blocchi o comportamenti anomali.

**Cosa sono gli handle?**

Un handle è un riferimento utilizzato dal sistema operativo per accedere a risorse come:

- File
- Chiavi di registro
- Oggetti di memoria

**Analisi degli handle in Process Explorer**

- Visualizzando gli handle associati a un processo, puoi capire quali risorse sta utilizzando.
- **Esempio**: Se un processo sospetto ha handle che puntano a file sconosciuti, potresti essere di fronte a un malware.

---

## Registro di Sistema

**Cos'è il Registro di Sistema?**

Il Registro di Sistema è il cuore della configurazione di Windows. Contiene informazioni su hardware, software, utenti e preferenze di sistema.

**Struttura del Registro di Sistema**

1. **HKEY_CLASSES_ROOT**
    - Memorizza informazioni sulle associazioni di file e identificatori dei programmi (ProgID).
2. **HKEY_CURRENT_USER**
    - Contiene le impostazioni dell'utente attualmente connesso, come preferenze di desktop e applicazioni.
3. **HKEY_LOCAL_MACHINE**
    - Memorizza configurazioni specifiche del computer (es. driver e servizi).
4. **HKEY_USERS**
    - Contiene le impostazioni per tutti gli utenti del sistema.
5. **HKEY_CURRENT_CONFIG**
    - Memorizza le configurazioni hardware in uso durante l'avvio.

---

## Conclusioni

1. **Gestione avanzata del sistema**
    - Conoscere i processi e i thread aiuta a identificare anomalie, ottimizzare le risorse e diagnosticare problemi.
2. **Sicurezza informatica**
    - Esplorando gli handle e utilizzando VirusTotal, puoi individuare potenziali malware.
3. **Modifica del Registro**
    - Comprendere la struttura del Registro di Sistema consente di personalizzare configurazioni avanzate, risolvere problemi e imparare a lavorare con gli script di registro.