REPORT DI LABORATORIO: Cisco CyberOps - Day 1

Studente: Nicola Cassandra
Data: 16/02/2026
Oggetto: Analisi Dinamica dei Processi, Thread, Handle e Manipolazione del Registro di Windows
Strumenti Utilizzati: Windows Sysinternals Suite (Process Explorer), Prompt dei Comandi, Editor del Registro di Sistema (Regedit).

1. Obiettivi dell'Esercitazione

L'obiettivo del laboratorio è stato acquisire familiarità con il monitoraggio avanzato del sistema operativo Windows. Nello specifico, si è puntato a comprendere la gerarchia dei processi, la gestione delle risorse (Thread e Handle) e il meccanismo di persistenza delle configurazioni tramite il Registro di Sistema.

2. Analisi dei Processi (Process Explorer)

Metodologia

Utilizzando `procexp.exe`, abbiamo isolato e analizzato processi attivi, tra cui il browser web (Microsoft Edge) e la shell di comando (`cmd.exe`).

Osservazioni e Risultati

- **Terminazione Forzata:** L'azione di "Kill Process" sul processo padre di Microsoft Edge ha comportato la chiusura immediata dell'applicazione e di tutte le schede aperte. Questo dimostra che terminando il processo principale, il sistema operativo revoca immediatamente l'allocazione di memoria.
- **Gerarchia Padre-Figlio:** Analizzando il Prompt dei Comandi, è emersa una chiara catena gerarchica:
    - **Parent:** `explorer.exe` (la shell grafica di Windows) ha generato `cmd.exe`.
    - **Child:** `cmd.exe` ha generato `conhost.exe` (Console Window Host), necessario per gestire l'input/output della finestra.
- **Analisi di Sicurezza:** È stato verificato l'hash del processo `conhost.exe` tramite l'integrazione con **VirusTotal**, confermando che processi di sistema legittimi possono essere verificati in tempo reale per escludere iniezioni di codice malevolo.

3. Analisi delle Risorse: Thread e Handle

Definizioni Operative

- **Thread:** Unità di esecuzione all'interno di un processo.
- **Handle:** Riferimento astratto a risorse di sistema (file, chiavi di registro, ecc.).

Risultati dell'Indagine

Ispezionando le proprietà di `conhost.exe`, la scheda **Threads** ha mostrato l'attività della CPU per ogni singola unità di esecuzione, permettendo di identificare quali sottoprocessi stavano consumando risorse. Attraverso la vista "Lower Pane", sono stati enumerati gli **Handle**, rivelando che il processo manteneva puntatori attivi verso file di sistema e chiavi di registro essenziali per il suo funzionamento.

4. Manipolazione del Registro di Sistema

Metodologia

L'accesso al database di configurazione è avvenuto tramite `regedit`, navigando nell'hive `HKEY_CURRENT_USER`, che contiene le impostazioni specifiche per l'utente loggato.

Esperimento di Persistenza

1. È stata localizzata la chiave `EulaAccepted` relativa a Process Explorer all'interno del percorso `Software\Sysinternals\Process Explorer` .
2. Il valore originale `0x00000001` (Vero/Accettato) è stato modificato manualmente in `0`.
3. **Esito:** Al successivo avvio di Process Explorer, il software ha riproposto la finestra di accettazione della licenza.

Conclusioni sulla Parte 3

Questo esperimento dimostra come le applicazioni "ricordino" lo stato (come l'accettazione di una licenza o, nel caso di malware, l'istruzione di avviarsi all'accensione) scrivendo valori specifici nel Registro. La modifica di questi valori altera il comportamento del software senza toccare l'eseguibile stesso.

Conclusioni Generali

Il laboratorio ha evidenziato come strumenti nativi o della suite Sysinternals offrano una visibilità granulare rispetto al classico Task Manager. La comprensione della relazione Padre-Figlio e la capacità di manipolare il Registro sono competenze fondamentali per **Incident Response** (Identificare processi anomali o orfani) e **Malware Analysis** (Comprendere come il codice malevolo ottiene persistenza tramite Registro e come si nasconde tramite Thread Injection).