**S11/L2**

**Relazione: Esplorazione di Processi, Thread, Handle e Registro di Windows**

Il laboratorio in questione ha l'obiettivo di approfondire l'analisi dei processi, dei thread, degli handle e del Registro di Windows utilizzando **Process Explorer** della suite SysInternals. Si articola in tre parti principali: esplorazione dei processi, dei thread e degli handle, e infine del Registro di Windows.

**Esplorazione dei Processi**

Nella prima fase, i partecipanti apprendono a gestire i processi, definiti come programmi o applicazioni in esecuzione. Dopo aver scaricato la suite SysInternals e avviato **Process Explorer**, viene illustrato come identificare i processi attivi, localizzarli tramite strumenti integrati (ad esempio, tramite l'icona "Find Window’s Process"), e come terminare un processo, con un esempio pratico basato su Microsoft Edge.

Un secondo esperimento mostra come avviare un nuovo processo, come nel caso del prompt dei comandi (cmd.exe) e il suo figlio conhost.exe. Durante l'analisi, è possibile verificare se un processo è potenzialmente malevolo utilizzando l'integrazione con **VirusTotal**, un servizio di analisi antivirus.

**Esplorazione di Thread e Handle**

Nella seconda parte, i partecipanti esplorano i **thread**, unità di esecuzione all'interno di un processo, e gli **handle**, riferimenti astratti a risorse gestite dal sistema operativo. Utilizzando il menu delle proprietà di Process Explorer, si accede a dettagli approfonditi dei thread, come variabili d'ambiente e informazioni di sicurezza. Gli handle vengono analizzati attraverso una visualizzazione specifica, evidenziando le risorse a cui fanno riferimento, come file o chiavi di registro.

**Esplorazione del Registro di Windows**

Infine, viene introdotta la struttura gerarchica del **Registro di Windows**, spiegando il ruolo delle cinque "hives" principali, che contengono configurazioni di sistema e utente. I partecipanti manipolano una chiave di registro (EulaAccepted) relativa a Process Explorer, osservando l’effetto di modificare il valore da 1 (indicante accettazione dell'EULA) a 0. Questo cambiamento forza la riapparizione della finestra di accettazione della licenza all'avvio del programma.