Cisco cyberops

Introduzione

In questo laboratorio, sono stati esplorati concetti fondamentali del sistema operativo Windows, come i processi, i thread, gli handle e il registro di Windows. Questi concetti sono cruciali per comprendere il funzionamento interno di un sistema operativo e per monitorare e diagnosticare problemi legati a risorse di sistema. Gli strumenti utilizzati per questa esplorazione sono la **SysInternals Suite** e l'**Editor del Registro di sistema di Windows**.

Parte 1: Esplorazione dei Processi

Fase 1: Scaricare e Avviare Process Explorer

Il primo passo è stato scaricare la **Windows SysInternals Suite** dal sito ufficiale di Microsoft. Una volta estratti i file, è stato avviato il programma **Process Explorer**. Questo strumento consente di visualizzare in tempo reale tutti i processi attivi nel sistema.

Fase 2: Esplorazione di un Processo Attivo

Successivamente, è stato esaminato il processo di un browser web (in questo caso Microsoft Edge). Utilizzando la funzione "Trova" di Process Explorer, ho individuato il processo associato al browser web. Dopo averlo selezionato, è stato terminato facendo clic su "Kill Process". La finestra del browser si è chiusa immediatamente, confermando che la terminazione del processo ha avuto effetto sul programma che stava eseguendo.

Fase 3: Avvio di un Nuovo Processo

Per continuare l'esplorazione, è stato avviato il processo **cmd.exe** (Prompt dei comandi) dal menu Start. Questo processo è stato osservato in Process Explorer, dove è stato notato che **cmd.exe** aveva come processo padre **explorer.exe** e un processo figlio chiamato **conhost.exe**.

In seguito, è stato eseguito un comando di **ping** dal prompt dei comandi. Durante l'esecuzione, è stato visibile un nuovo processo figlio denominato **PING.EXE** sotto **cmd.exe**. Questo ha mostrato come i processi possano avviare altri processi, creando una gerarchia di esecuzione.

Inoltre, è stata fatta una verifica del processo **conhost.exe** per verificare se potesse essere dannoso, utilizzando il servizio **VirusTotal**. Dopo aver controllato, non sono emerse minacce, e il processo **cmd.exe** è stato terminato. Quando il processo padre è stato terminato, anche il processo figlio **conhost.exe** si è fermato, confermando la dipendenza tra processi padre e figlio.

Parte 2: Esplorazione di Thread e Handle

Fase 1: Esplorazione dei Thread

I thread sono le unità di esecuzione all'interno di un processo. Ogni processo può contenere uno o più thread. Ho selezionato il processo **conhost.exe** in Process Explorer e aperto la scheda "Thread" nelle proprietà del processo. Le informazioni visualizzate includevano dettagli sui thread attivi, come l'ID del thread e lo stato corrente di esecuzione. Questo ha permesso di osservare come i thread interagiscono all'interno di un processo.

Fase 2: Esplorazione degli Handle

Gli handle sono riferimenti a risorse del sistema, come file, chiavi di registro e thread, che vengono gestiti dal sistema operativo. In Process Explorer, ho selezionato l'opzione per visualizzare gli handle associati al processo **conhost.exe**. È stato osservato che gli handle puntano a vari oggetti, come file o chiavi di registro. Questo ha mostrato come i processi interagiscono con il sistema operativo e come le risorse siano accessibili tramite gli handle.

Parte 3: Esplorazione del Registro di Windows

Fase 1: Modifica di una Chiave di Registro

Il Registro di Windows è una parte fondamentale del sistema operativo che memorizza le configurazioni e le impostazioni di sistema. Per esplorare il registro, è stato utilizzato l'**Editor del Registro di sistema** (regedit). In particolare, è stata esaminata la chiave di registro relativa a **Process Explorer**.

Ho navigato nel percorso **HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer**, dove si trovava la chiave **EulaAccepted**. Inizialmente, il valore di questa chiave era **0x00000001(1)**, indicando che l'EULA era stato accettato. Successivamente, ho modificato il valore a **0**, per simulare il non accettamento dell'EULA. Dopo aver fatto ciò e riaperto **Process Explorer**, è comparso di nuovo il contratto di licenza, come previsto.

Conclusioni

In questo laboratorio, ho acquisito una comprensione più approfondita dei concetti di processi, thread, handle e registro di Windows. Ho imparato a utilizzare strumenti come **Process Explorer** per monitorare e gestire i processi attivi nel sistema, esplorare la struttura dei thread e degli handle, e anche come modificare il registro di Windows per cambiare alcune configurazioni di sistema. Questi strumenti e concetti sono essenziali per la gestione e la sicurezza dei sistemi operativi, in particolare per monitorare e diagnosticare comportamenti sospetti o anomali nei processi.