In questo laboratorio di Cyber Security & Ethical Hacking con Cisco CyberOps, l'obiettivo è esplorare i processi, i thread, gli handle e il Registro di Windows. Utilizzeremo Process Explorer dalla suite Sysinternals e il Registro di Windows per eseguire modifiche a livello di configurazione. Qui di seguito trovi una panoramica dei passaggi principali per completare il laboratorio:

1. Esplorazione dei Processi, Thread e Handle con Process Explorer

Process Explorer è uno strumento potente per monitorare e analizzare i processi in esecuzione sul sistema Windows. È una delle utilità incluse nella Sysinternals Suite di Microsoft. Ecco come utilizzarlo per esplorare processi, thread e handle:

Passi:
1. Scaricare Process Explorer:
   - Vai al sito ufficiale di Sysinternals:
https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer e scarica Process Explorer.
   - Estrai il contenuto in una cartella e avvia l'applicazione procexp.exe.

2. Esplorare i Processi:
   - Dopo aver avviato Process Explorer, vedrai un elenco di tutti i processi in esecuzione.
   - Puoi osservare le informazioni dettagliate su ciascun processo, come l'ID del processo (PID), la memoria utilizzata e altre statistiche.

3. Esplorare i Thread:
   - Seleziona un processo dalla lista e fai clic con il tasto destro su di esso. Scegli "Properties" per visualizzare i thread associati al processo.
   - Nella finestra Thread, vedrai l'elenco dei thread, incluso il loro stato e l'ID del thread (TID). Puoi anche vedere la percentuale di CPU utilizzata da ogni thread.

4. Esplorare gli Handle:
   - Sempre nella finestra delle proprietà di un processo, seleziona la scheda Handles.
   - Questa sezione mostrerà gli handle associati al processo, che rappresentano risorse come file, porte di rete o chiavi di registro che il processo sta utilizzando.
   - Puoi anche cercare specifici tipi di handle, come i file aperti o le porte di comunicazione.

5. Monitorare e Analizzare le Attività:
   - Usa le funzionalità avanzate di Process Explorer, come la ricerca e il filtro, per monitorare attività sospette, come un aumento improvviso dei thread o l’apertura di handle sospetti.

2. Utilizzo del Registro di Windows per Modificare un’Impostazione

Il Registro di Windows è una base di dati utilizzata dal sistema operativo per memorizzare le configurazioni di sistema e le impostazioni delle applicazioni. In questo laboratorio, esploreremo come modificare una chiave di registro.

Passi:
1. Accedere al Registro di Windows:
   - Premi Windows + R per aprire la finestra "Esegui".
   - Digita `regedit` e premi Invio per aprire l'Editor del Registro di Windows.

2. Navigare nel Registro:

- Nella finestra dell'Editor del Registro, puoi navigare tra le varie sezioni (chiavi di registro) sul lato sinistro della finestra.
- Le principali sezioni del registro includono:
  - HKEY_LOCAL_MACHINE: Contiene le configurazioni del sistema e delle applicazioni.
  - HKEY_CURRENT_USER: Contiene le configurazioni specifiche per l'utente corrente.
  - HKEY_CLASSES_ROOT: Gestisce i tipi di file e le associazioni.

3. Modificare una Chiave di Registro:
- Per esempio, puoi navigare in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` per vedere quali applicazioni vengono avviate automaticamente all'avvio del sistema.
- Se desideri disabilitare un'applicazione che si avvia automaticamente, puoi fare clic destro su una chiave di registro e selezionare Elimina.

4. Aggiungere una Nuova Chiave:
- Se vuoi aggiungere una nuova chiave di registro, fai clic destro sulla cartella in cui vuoi inserirla, scegli Nuovo > Valore Stringa (o un altro tipo di valore), e inserisci il nome e i dati desiderati.

5. Esportare e Importare Chiavi di Registro:
- Puoi anche esportare e importare chiavi di registro per creare backup delle tue modifiche. Fai clic destro sulla chiave di registro, seleziona Esporta per salvarla come file `.reg`, e successivamente puoi importarla su un altro sistema o ripristinarla in caso di problemi.

Attenzione:
- Modificare il Registro di Windows senza una buona conoscenza può danneggiare il sistema, quindi è importante eseguire sempre il backup prima di fare modifiche.
- Le modifiche al registro non diventano effettive fino a quando il sistema non viene riavviato in alcuni casi.

L'obiettivo di questo laboratorio è acquisire competenze pratiche nella gestione e analisi dei processi e nel monitoraggio delle risorse di sistema, così come nel manipolare il registro di Windows per configurazioni avanzate. Le informazioni raccolte da Process Explorer possono essere utilizzate per rilevare attività sospette o malware, mentre le modifiche al Registro di Windows possono migliorare o personalizzare l'ambiente operativo del sistema.