AMATO SARA

S11 L2

### **Esplorazione di Processi, Thread, Handle e Registro di Windows**

**Obiettivo:**Questa esercitazione permette di esplorare i processi, i thread e gli handle utilizzando **Process Explorer**, uno strumento della suite SysInternals di Windows. Inoltre, consente di modificare una configurazione nel Registro di sistema di Windows.

### **Parte 1: Esplorazione dei processi**

**Definizione:**Un processo è un programma o un'applicazione in esecuzione. Attraverso **Process Explorer**, è possibile visualizzare, analizzare e gestire i processi attivi.

#### **Fase 1: Download della suite SysInternals**

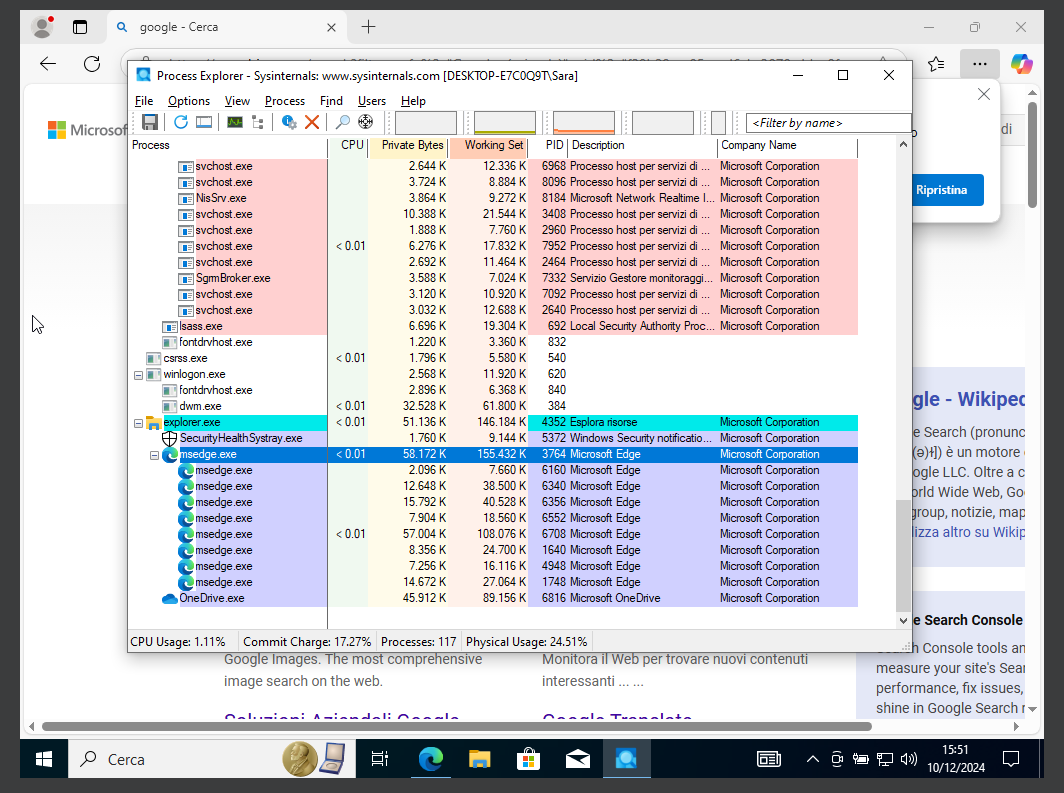
1. Scaricare la suite SysInternals dal link fornito.

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

1. Estrarre i file dalla cartella e mantenere il browser aperto per i passaggi successivi.

#### **Fase 2: Analisi di un processo attivo**

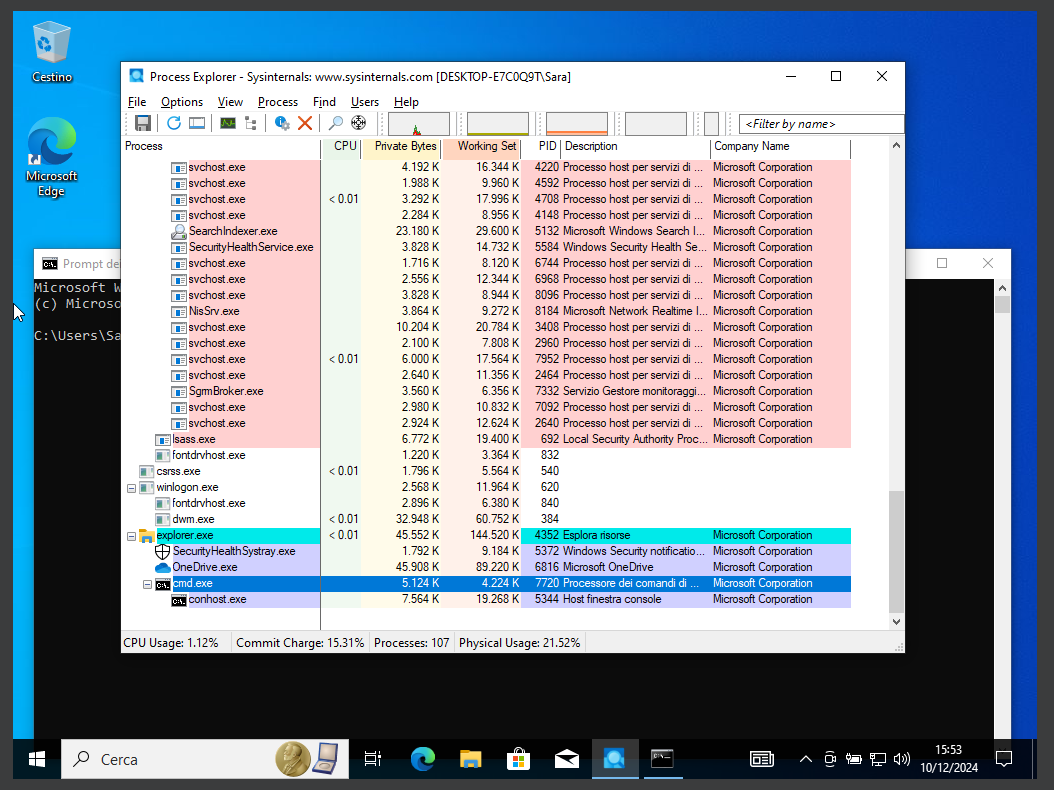
1. Aprire il file **procexp.exe** nella cartella estratta.
2. Accettare il contratto di licenza (EULA) di Process Explorer.
3. Visualizzare l’elenco dei processi attivi.
   * Trascinare l'icona **Find Window’s Process** nella finestra del browser (ad esempio Microsoft Edge).
   * Identificare il processo del browser e terminarlo tramite l’opzione **Kill Process**.

****

**Risultato:** La finestra del browser si chiude al termine del processo.

#### **Fase 3: Avvio di un nuovo processo**

1. Aprire un Prompt dei comandi (*cmd.exe*).
2. Usare l'icona **Find Window’s Process** per individuare il processo del Prompt dei comandi.
   * Il processo padre è **explorer.exe**, mentre il processo figlio è **conhost.exe**.
3. Eseguire un comando *ping* e osservare i cambiamenti:
   * Durante il ping, si crea un processo figlio denominato **PING.EXE** sotto il **cmd.exe**.

****

**Verifica di contenuti sospetti:**

* Identificare **conhost.exe** come sospetto e utilizzare l'opzione **Check VirusTotal**.
* Visualizzare i risultati tramite la colonna **VirusTotal**.

**Termine dei processi:**

* Terminare il processo **cmd.exe**.
* **Effetto:** Il processo figlio **conhost.exe** viene interrotto automaticamente poiché dipende dal processo padre.

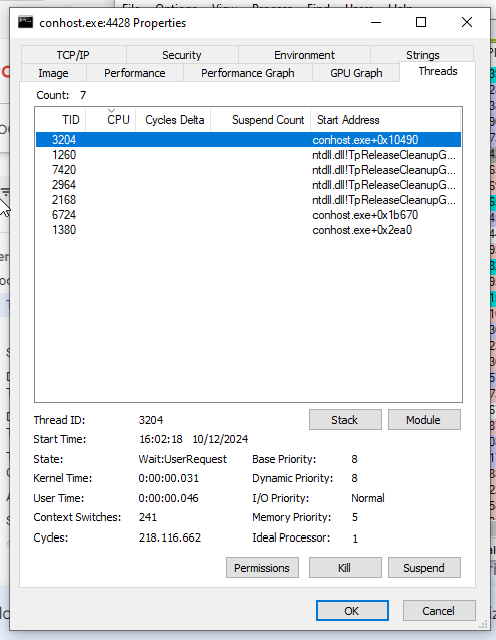
### **Parte 2: Esplorazione di Thread e Handle**

**Definizione:**

* **Thread:** Un'unità di esecuzione all'interno di un processo.
* **Handle:** Un riferimento astratto a risorse di sistema (es. file, chiavi di registro, memoria).

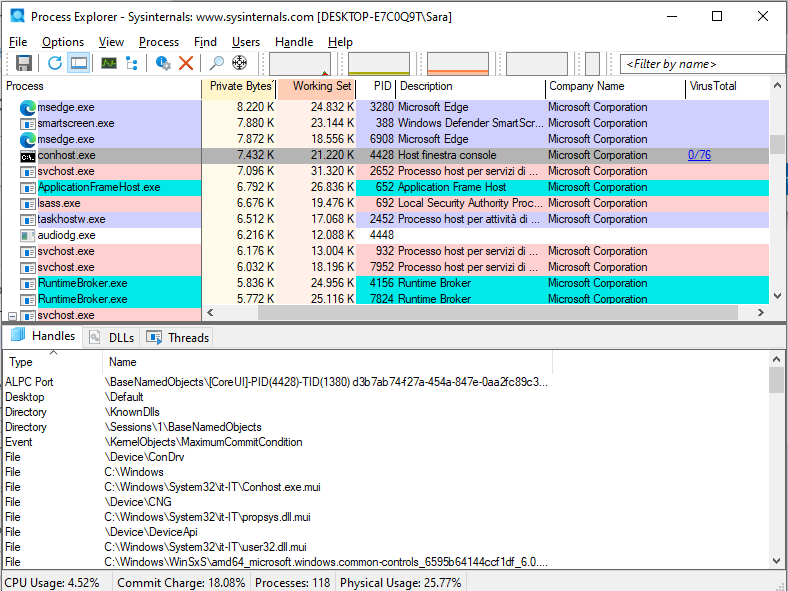
#### **Fase 1: Esplorazione dei thread**

1. Aprire il Prompt dei comandi.
2. In Process Explorer, fare clic destro su **conhost.exe** e selezionare **Properties**.
3. Accedere alla scheda **Threads** per visualizzare i thread attivi.

**Informazioni disponibili:**Variabili d’ambiente, informazioni di sicurezza, prestazioni e stringhe stampabili.

#### **Fase 2: Esplorazione degli handle**

1. In Process Explorer, selezionare **View > Lower Pane View > Handles**.
2. Analizzare gli handle associati a **conhost.exe**.

****

**Risultato:**Gli handle fanno riferimento a file, chiavi di registro e thread.

### **Parte 3: Esplorazione del Registro di sistema**

**Definizione:**Il Registro di sistema è un database gerarchico che memorizza configurazioni del sistema operativo e dell'ambiente desktop.

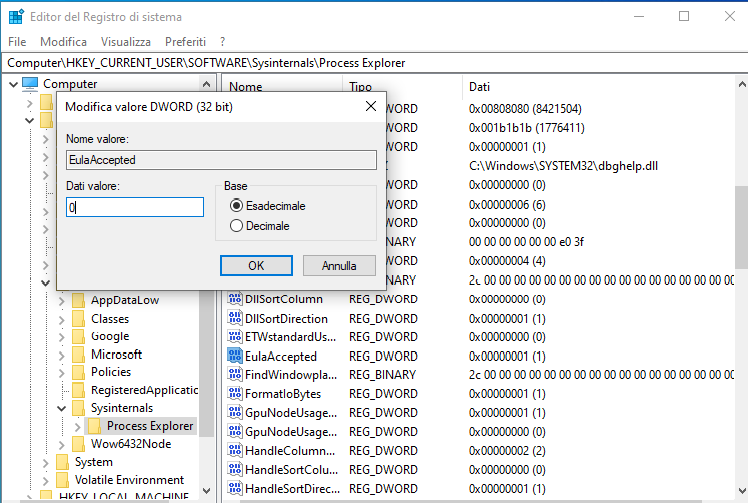
#### **Fase 1: Accesso al Registro di sistema**

1. Aprire il **Registry Editor** (*regedit*).
2. Navigare attraverso le cinque principali sezioni (hive):
   * **HKEY\_CLASSES\_ROOT**: Associazioni di file ed estensioni.
   * **HKEY\_CURRENT\_USER**: Configurazioni dell’utente corrente.
   * **HKEY\_LOCAL\_MACHINE**: Configurazioni specifiche del computer.
   * **HKEY\_USERS**: Configurazioni di tutti gli utenti.
   * **HKEY\_CURRENT\_CONFIG**: Informazioni hardware utilizzate durante l'avvio.

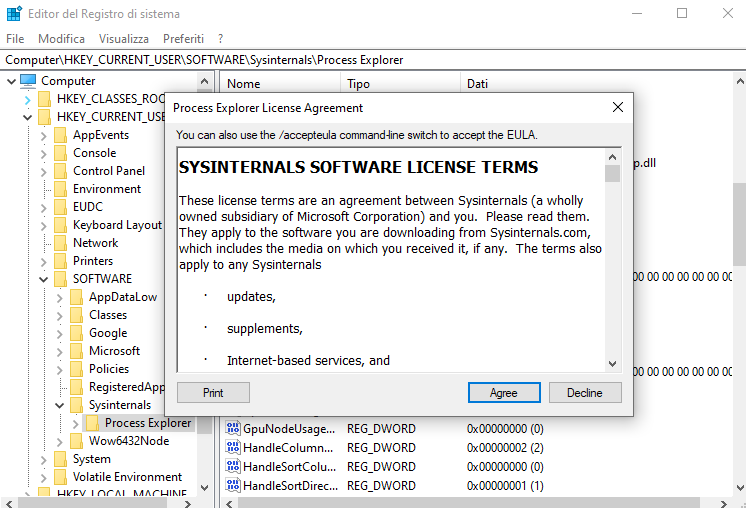
#### 

#### **Fase 2: Modifica di una chiave di registro**

1. Navigare alla chiave **EulaAccepted** per Process Explorer:
   * **HKEY\_CURRENT\_USER > Software > Sysinternals > Process Explorer**.
   * Il valore predefinito è **0x00000001(1)**, che indica che l'EULA è stata accettata.
2. Modificare il valore a **0** per simulare il rifiuto dell'EULA.

****

**Effetto:**All’apertura di Process Explorer, viene visualizzato nuovamente il contratto di licenza.



### 

### 

### 

### **Conclusioni**

Questa esercitazione ha dimostrato come:

* Esplorare processi attivi e gestirli tramite **Process Explorer**.
* Analizzare i thread e gli handle di un processo per comprendere l'allocazione delle risorse.
* Modificare impostazioni specifiche nel Registro di sistema per configurare il comportamento delle applicazioni.

L'uso di strumenti avanzati come Process Explorer e il Registry Editor è fondamentale per il monitoraggio e la gestione delle risorse del sistema, nonché per l’individuazione di potenziali attività sospette.