

REPORT S11/L1

Cisco CyberOps 1

Traccia

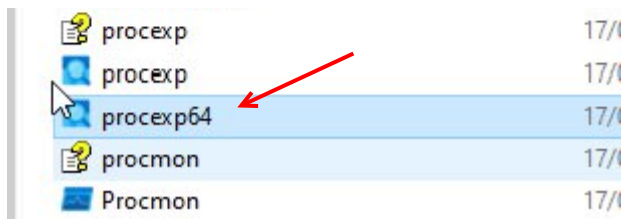
Esplorazione di Processi, Thread, Handle e Registro di Windows

In questo laboratorio, completerai i seguenti obiettivi:

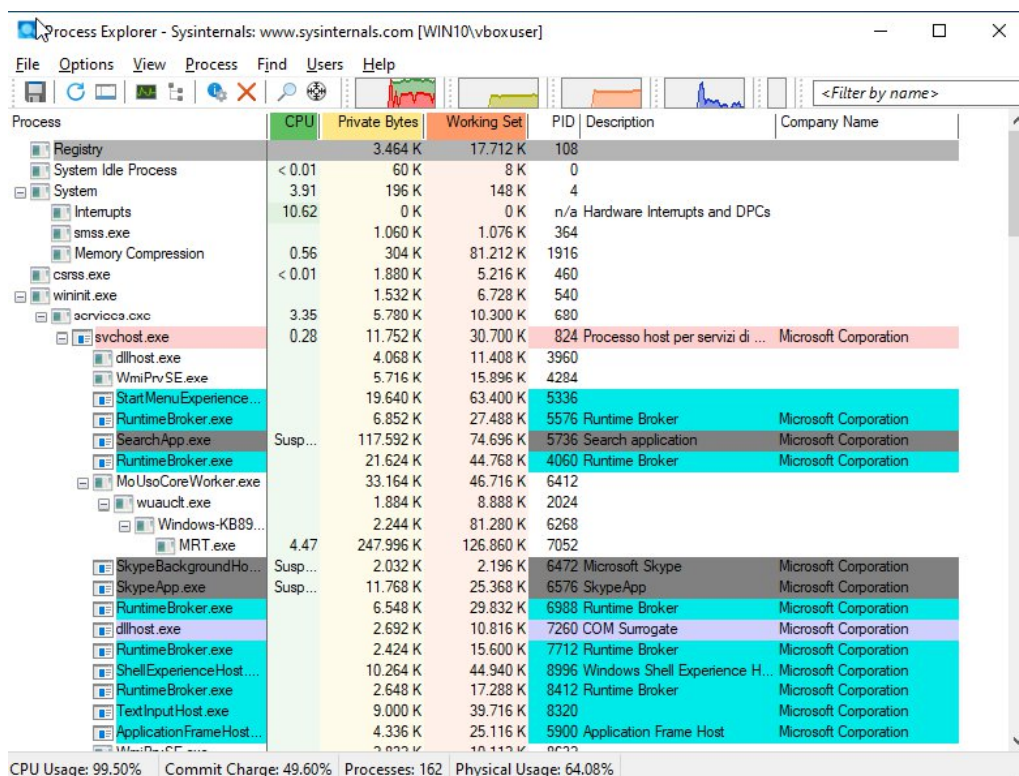
- Esplora i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite.
- Utilizza il Registro di Windows per modificare un'impostazione.

Svolgimento

Per svolgere l'esercizio odierno scarichiamo Sysinternals Suite sulla macchina virtuale di Windows 10 Home ed avviamo il programma **procexp.exe**

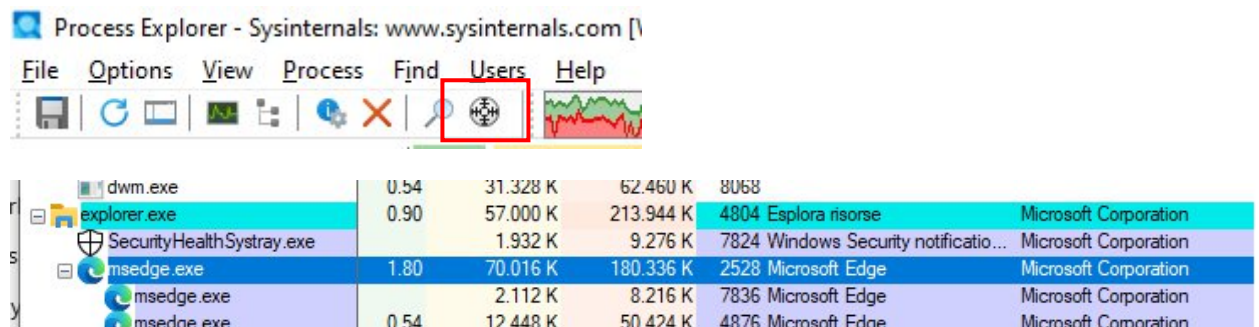


All'avvio vediamo:

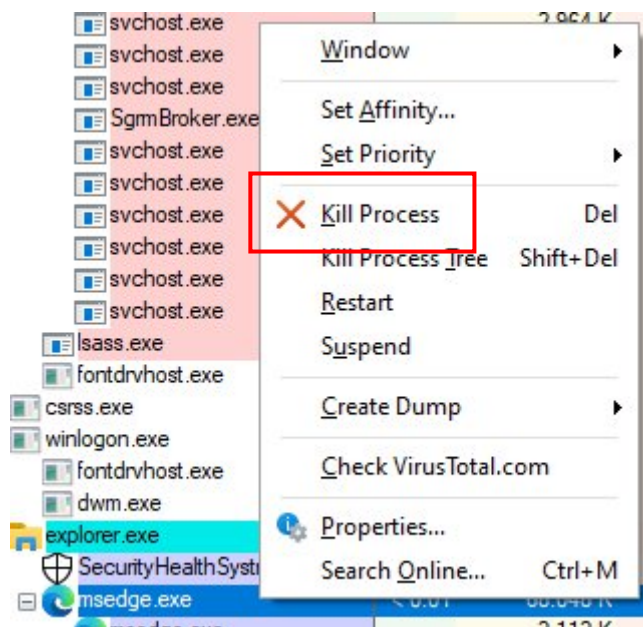


Process Explorer ci mostra la lista dei processi attualmente in esecuzione sulla VM.

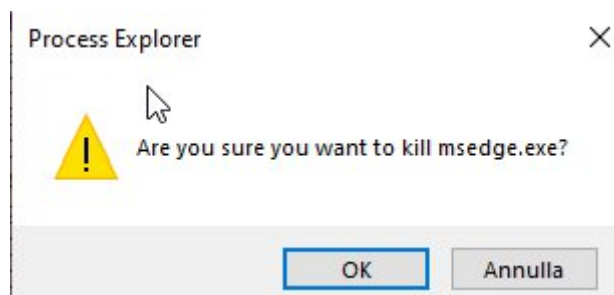
Cerchiamo il processo del browser cliccando sulla specifica icona del **Find Window's Process** e trasciniamola sulla finestra di Edge. In questo modo il digramma dei processi verrà espanso fino a mettere in evidenza il processo cercato.



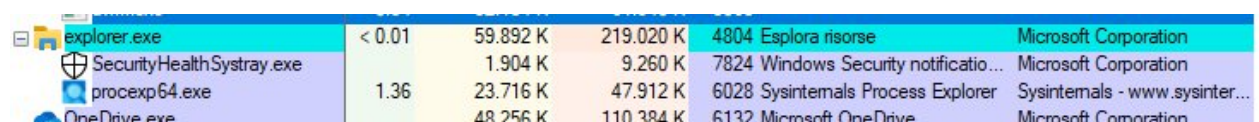
A questo punto possiamo terminare il processo cliccando con il tasto destro del mouse sul processo evidenziato e scegliendo **Kill Process**:



Ci apparirà una finestra di conferma, diamo OK

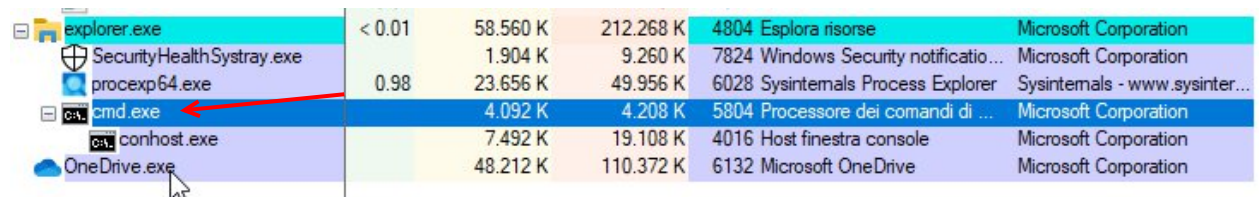


Edge verrà chiuso e il processo scomparirà dalla lista



Proviamo adesso ad avviare un nuovo processo e ad analizzare cosa succede.

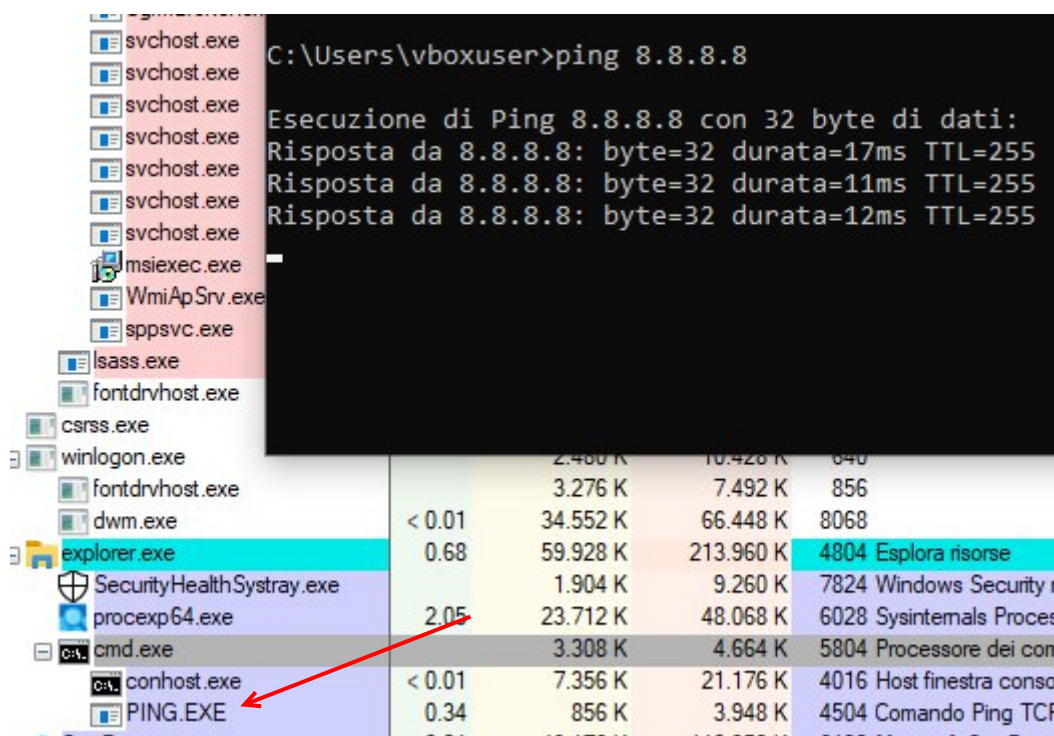
Avviamo un nuovo prompt e come prima usiamo il tasto **Find Window's Process** per localizzarlo nell'elenco dei processi.



Process Name	Private Bytes	Working Set	Virtual Bytes	Process ID	Description	Company Name
explorer.exe	< 0.01	58.560 K	212.268 K	4804	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		1.904 K	9.260 K	7824	Windows Security notificatio...	Microsoft Corporation
procexp64.exe	0.98	23.656 K	49.956 K	6028	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		4.092 K	4.208 K	5804	Processore dei comandi di ...	Microsoft Corporation
conhost.exe		7.492 K	19.108 K	4016	Host finestra console	Microsoft Corporation
OneDrive.exe		48.212 K	110.372 K	6132	Microsoft OneDrive	Microsoft Corporation

Vediamo che il processo **cmd.exe** ha un “processo padre” che è *explorer.exe*, e a sua volta ha un “processo figlio” nominato *conhost.exe*

Dando il comando ping vediamo comparire un nuovo processo figlio per cmd.exe, ovvero **PING.EXE**



Process Name	Private Bytes	Working Set	Virtual Bytes	Process ID	Description	Company Name
svchost.exe		2.480 K	10.428 K	840		
svchost.exe		3.276 K	7.492 K	856		
svchost.exe		34.552 K	66.448 K	8068		
svchost.exe		59.928 K	213.960 K	4804	Esplora risorse	
svchost.exe		1.904 K	9.260 K	7824	Windows Security n	
svchost.exe		23.712 K	48.068 K	6028	Sysinternals Proces	
svchost.exe		3.308 K	4.664 K	5804	Processore dei com	
msiexec.exe		7.356 K	21.176 K	4016	Host finestra consol	
WmiApSrv.exe		856 K	3.948 K	4504	Comando Ping TCP	
sppsvc.exe						
lsass.exe						
fontdrvhost.exe						
csrss.exe						
winlogon.exe						
fontdrvhost.exe						
dwm.exe						
explorer.exe	0.68	59.928 K	213.960 K	4804	Esplora risorse	
SecurityHealthSystray.exe		1.904 K	9.260 K	7824	Windows Security n	
procexp64.exe	2.05	23.712 K	48.068 K	6028	Sysinternals Proces	
cmd.exe		3.308 K	4.664 K	5804	Processore dei com	
conhost.exe	< 0.01	7.356 K	21.176 K	4016	Host finestra consol	
PING.EXE	0.34	856 K	3.948 K	4504	Comando Ping TCP	

```
C:\Users\vboxuser>ping 8.8.8.8

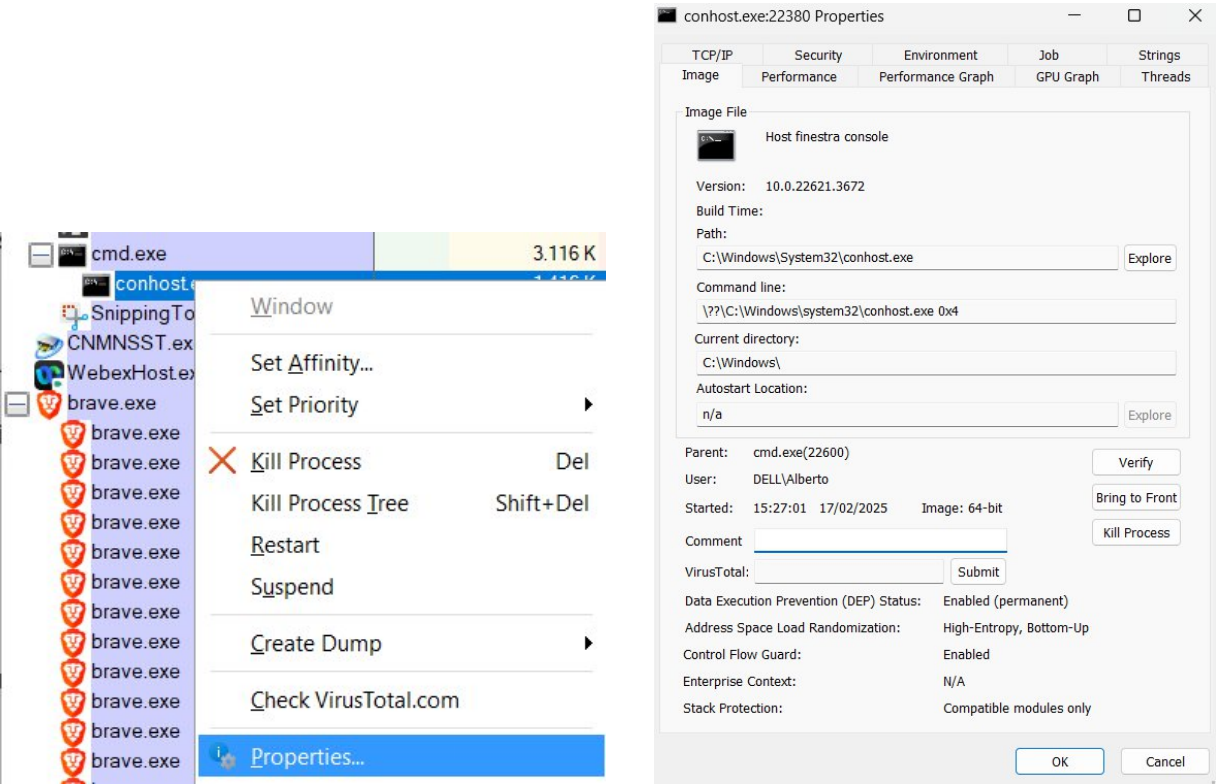
Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=17ms TTL=255
Risposta da 8.8.8.8: byte=32 durata=11ms TTL=255
Risposta da 8.8.8.8: byte=32 durata=12ms TTL=255
```

Questo significa che per eseguire il comando il prompt si appoggia ad un processo secondario, che viene avviato quando confermiamo il comando e automaticamente killato al termine della sua esecuzione.

Esploriamo ora i thread e gli handle. I processi hanno uno o più thread, che è un'unità di esecuzione in un processo. Un handle, invece, è un riferimento astratto a blocchi di memoria o oggetti gestiti da un sistema operativo.

THREAD

Facciamo clic con il pulsante destro del mouse su conhost.exe e selezioniamo Proprietà.



Scegliamo la scheda *Threads* per visualizzare quelli attivi per il processo conhost.exe.

Count: 4

TID	CPU	Cycles Delta	Suspend Count	Start Address
16080				conhost.exe+0x9290
2308				conhost.exe+0x96b70
4476				ntdll.dll!RtlClearThread...
14792				ntdll.dll!RtlClearThread...

Thread ID: 16080 Stack Module

Start Time: 15:27:01 17/02/2025

State: Wait:UserRequest Base Priority: 8

Kernel Time: 0:00:00.000 Dynamic Priority: 9

User Time: 0:00:00.000 I/O Priority: Normal

Context Switches: 51 Memory Priority: 5

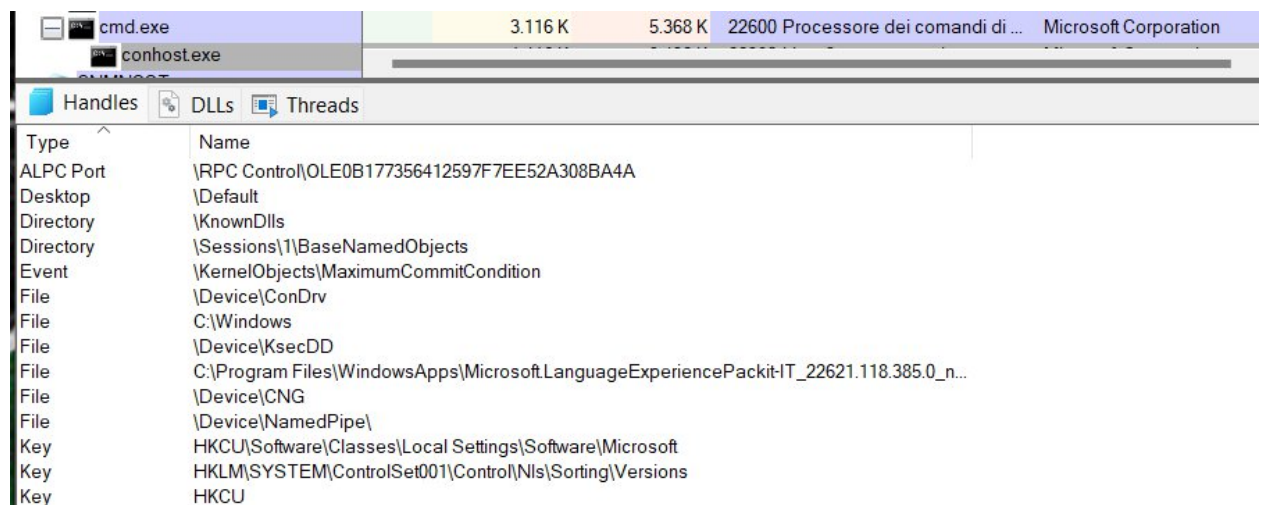
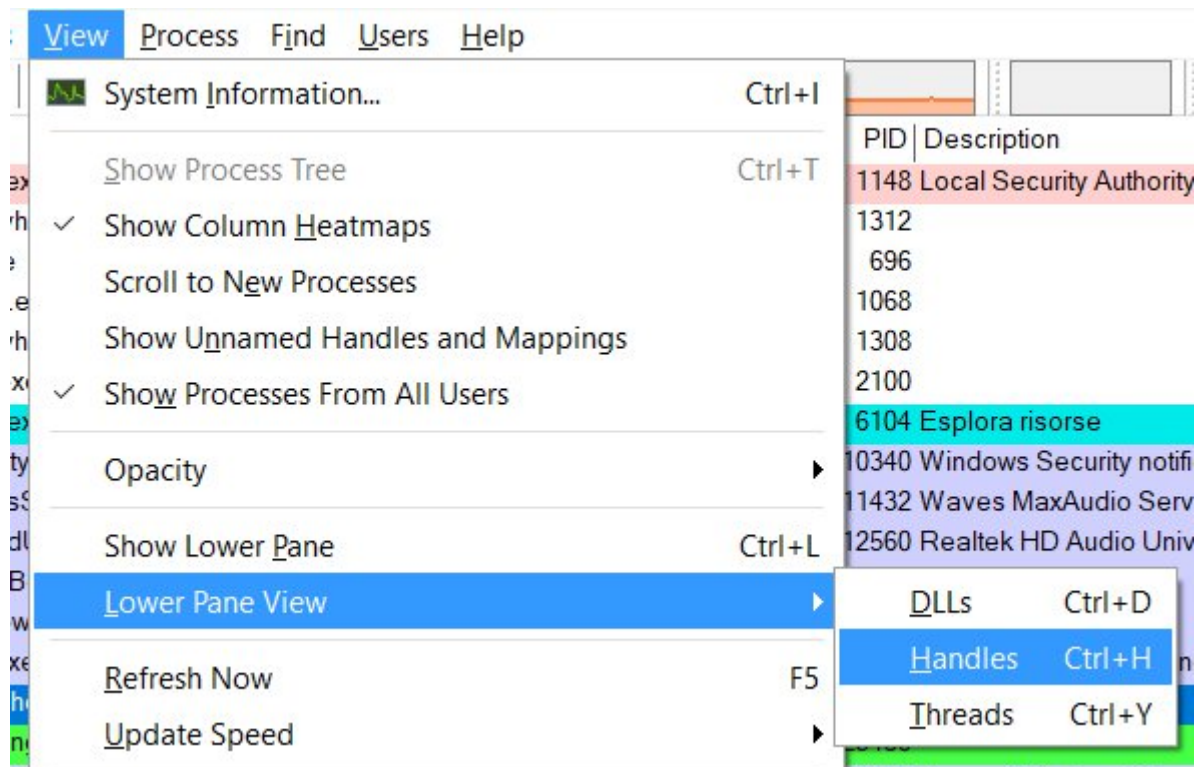
Cycles: 52.558.366 Ideal Processor: 7

Permissions Kill Suspend

Esaminando i dettagli del thread vediamo le informazioni disponibili che includono variabili d'ambiente, informazioni sulla sicurezza, informazioni sulle prestazioni e stringhe stampabili.

HANDLES

In Esplora processi, andiamo su Visualizza, poi Vista riquadro inferiore e infine Handles per visualizzare le handle associate al processo conhost.exe.



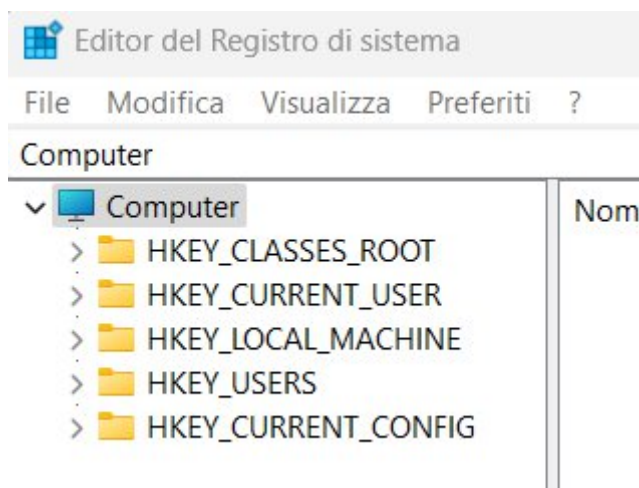
Esaminando gli handles vediamo che puntano a file, chiavi di registro e thread, quindi ci facilitano l'individuazione di questi oggetti nel caso in cui stiamo analizzando un processo malevole.

Per l'ultima parte dell'esercizio esploriamo il registro di sistema e modifichiamo un'impostazione.

Apriamo la finestra *Esegui* con la shortcut Win+R, scriviamo regedit e diamo invia. Ci si aprirà il registro di sistema, che è un database gerarchico che memorizza la maggior parte delle impostazioni di configurazione del sistema operativo e dei programmi installati in esso.

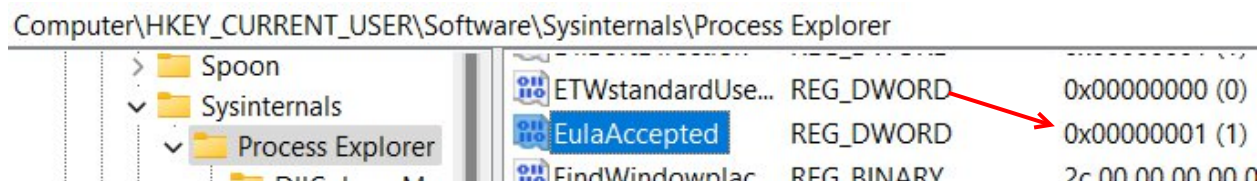
Ricordiamo che l'Editor del Registro ha cinque macrogruppi in cui vengono salvate e classificate le varie *chiavi*.

1. **HKEY_CLASSES_ROOT** che memorizza le informazioni utilizzate dalle applicazioni registrate come l'associazione di estensione dei file, nonché i dati identificativi programmatici (ProgID), ID classe (CLSID) e ID interfaccia (IID).
2. **HKEY_CURRENT_USER** contiene le impostazioni e le configurazioni per gli utenti che sono attualmente connessi.
3. **HKEY_LOCAL_MACHINE** memorizza informazioni di configurazione specifiche per il computer locale.
4. **HKEY_USERS** contiene le impostazioni e le configurazioni per tutti gli utenti sul computer locale.
5. **HKEY_CURRENT_CONFIG** memorizza le informazioni hardware utilizzate all'avvio dal computer locale.



Ricordiamo che all'avvio di *Process Explorer* abbiamo accettato un EULA, pertanto possiamo rintracciare questa nostra "scelta" nel registro di sistema.

Seguiamo il percorso HKEY_CURRENT_USER > Software > Sisinterni > Process Explorer. Scorriamo verso il basso per individuare la chiave EulaAccepted. Attualmente, il valore per la chiave di registro EulaAccepted è 0x00000001 (1).



Per cambiare il valore da 1 a 0 facciamo doppio click sulla chiave e scriviamo 0 nel campo *Dati valore*, poi premiamo ok. Vediamo cosa succede quando andiamo a riaprire *Process Explorer*.

Modifica valore DWORD (32 bit) ✕

Nome valore:
EulaAccepted

Dati valore:
0

Base
☒ Esadecimale
☐ Decimale

OK Annulla

Come previsto al riavvio del programma ci ricompare la finestra per l'accettazione degli EULA.

Process Explorer License Agreement ✕

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Print Agree Decline