

# Report Esercizio 17/02/2025

## CyberOps Esercizio 1 Leonardo Catalano

“La traccia di oggi ci chiede di effettuare l’esercizio di Cisco CyberOps 3.2.11 Lab – Exploring Processes, Threads, Handles, and Windows Registry, seguendo il seguente link: <https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html> ”

Le fasi da effettuare saranno le seguenti:

1. Exploring Processes :
2. Exploring Threads and Handles :
3. Exploring Windows Registry :

### -PART 1: Exploring Processes

“In this, you will explore processes. Processes are programs or applications in execution. You will explore the processes using Process Explorer in the Windows SysInternals Suite. You will also start and observe a new process”.

Come 1\* Step andremo a scaricare la Windows SysInternals Suite:

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

Come 2\* Step andremo ad esplorare i processi attivi:

Nei programmi SysinternalsSuite andremo ad aprire **procexp.exe**, questo tool ci andrà a visualizzare i processi attualmente attivi nel pc.

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-U8C0OMG7\leolo]

File Options View Process Find Users Help

<Filter by name>

| Process                     | CPU     | Private Bytes | Working Set | PID   | Description                      | Company Name          |
|-----------------------------|---------|---------------|-------------|-------|----------------------------------|-----------------------|
| Secure System               |         | 172 K         | 64.732 K    | 236   |                                  |                       |
| Registry                    |         | 10.376 K      | 44.568 K    | 276   |                                  |                       |
| System Idle Process         | 90.02   | 60 K          | 8 K         | 0     |                                  |                       |
| System                      | 0.83    | 52 K          | 4.300 K     | 4     |                                  |                       |
| Interrupts                  | 0.19    | 0 K           | 0 K         | n/a   | Hardware Interrupts and DPCs     |                       |
| smss.exe                    |         | 1.144 K       | 636 K       | 856   |                                  |                       |
| Memory Compression          | < 0.01  | 3.008 K       | 696.720 K   | 3904  |                                  |                       |
| csrss.exe                   | < 0.01  | 2.716 K       | 3.444 K     | 1268  |                                  |                       |
| wininit.exe                 |         | 1.588 K       | 3.824 K     | 1416  |                                  |                       |
| services.exe                | 0.09    | 6.680 K       | 9.944 K     | 1544  |                                  |                       |
| svchost.exe                 | < 0.01  | 15.956 K      | 30.284 K    | 1744  | Processo host per servizi di ... | Microsoft Corporation |
| unsecapp.exe                | < 0.01  | 3.844 K       | 4.560 K     | 6624  |                                  |                       |
| WmiPrvSE.exe                |         | 6.976 K       | 11.416 K    | 1896  |                                  |                       |
| unsecapp.exe                |         | 1.704 K       | 9.592 K     | 14472 |                                  |                       |
| SearchHost.exe              | Susp... | 209.676 K     | 139.312 K   | 13468 |                                  | Microsoft Corporation |
| StartMenuExperienceHost.exe | < 0.01  | 52.084 K      | 99.912 K    | 3732  | Windows Start Experience H...    | Microsoft Corporation |
| WidgetBoard.exe             | < 0.01  | 32.276 K      | 76.728 K    | 12884 |                                  | Microsoft Corporation |
| msedgewebview2.exe          |         | 54.092 K      | 115.132 K   | 19216 | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 2.284 K       | 8.868 K     | 1432  | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 221.464 K     | 120.952 K   | 14352 | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 13.892 K      | 38.836 K    | 4176  | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 10.684 K      | 20.748 K    | 3872  | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 17.912 K      | 37.680 K    | 7136  | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          | < 0.01  | 242.144 K     | 241.768 K   | 6980  | Microsoft Edge WebView2          | Microsoft Corporation |
| msedgewebview2.exe          |         | 7.876 K       | 20.444 K    | 21000 | Microsoft Edge WebView2          | Microsoft Corporation |
| RuntimeBroker.exe           |         | 15.080 K      | 68.252 K    | 4784  | Runtime Broker                   | Microsoft Corporation |
| RuntimeBroker.exe           |         | 7.100 K       | 34.740 K    | 3640  | Runtime Broker                   | Microsoft Corporation |
| dllhost.exe                 |         | 6.772 K       | 19.332 K    | 7884  | COM Surrogate                    | Microsoft Corporation |
| LockApp.exe                 | Susp... | 16.768 K      | 58.344 K    | 12416 | LockApp.exe                      | Microsoft Corporation |
| RuntimeBroker.exe           |         | 10.188 K      | 45.288 K    | 12812 | Runtime Broker                   | Microsoft Corporation |

CPU Usage: 8.97% Commit Charge: 57.33% Processes: 269 Physical Usage: 75.95%

Per localizzare il web browser, si clicca l'icona specifica (sottolineata nello screen) e ci apparirà nello specifico il processo del browser web (nel mio caso è Brave).

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-U8C0OMG7\leolo]

File Options View Process Find Users Help

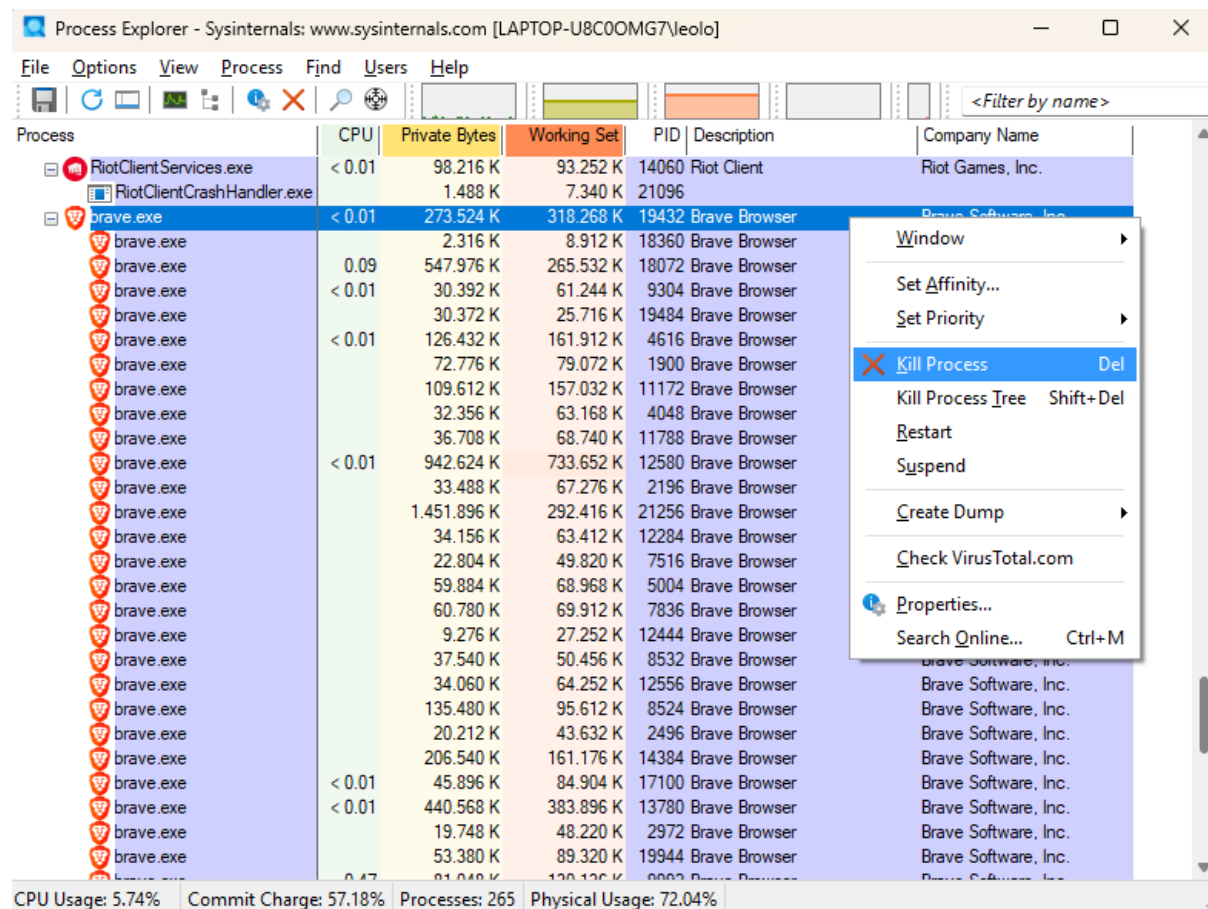
<Filter by name>

| Process                    | CPU    | Private Bytes | Working Set | PID   | Description   | Company Name         |
|----------------------------|--------|---------------|-------------|-------|---------------|----------------------|
| RiotClientServices.exe     | < 0.01 | 97.672 K      | 92.408 K    | 14060 | Riot Client   | Riot Games, Inc.     |
| RiotClientCrashHandler.exe |        | 1.520 K       | 7.356 K     | 21096 |               |                      |
| brave.exe                  | < 0.01 | 273.132 K     | 326.884 K   | 19432 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 2.360 K       | 8.932 K     | 18360 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 536.956 K     | 267.904 K   | 18072 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 30.748 K      | 61.312 K    | 9304  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 30.216 K      | 25.472 K    | 19484 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 133.148 K     | 167.848 K   | 4616  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 72.372 K      | 76.024 K    | 1900  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 109.712 K     | 77.828 K    | 11172 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 32.368 K      | 63.132 K    | 4048  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 36.728 K      | 68.672 K    | 11788 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 924.372 K     | 704.324 K   | 12580 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 33.480 K      | 67.108 K    | 2196  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 1.458.708 K   | 298.128 K   | 21256 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 34.148 K      | 63.304 K    | 12284 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 22.836 K      | 51.540 K    | 7516  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 59.712 K      | 68.552 K    | 5004  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 60.428 K      | 69.288 K    | 7836  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 9.464 K       | 27.528 K    | 12444 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 37.632 K      | 50.476 K    | 8532  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 34.092 K      | 64.448 K    | 12556 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 135.512 K     | 96.428 K    | 8524  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 20.244 K      | 43.652 K    | 2496  | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 206.160 K     | 85.096 K    | 14384 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 44.900 K      | 83.592 K    | 17100 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 441.004 K     | 381.264 K   | 13780 | Brave Browser | Brave Software, Inc. |
| brave.exe                  |        | 19.660 K      | 47.160 K    | 2972  | Brave Browser | Brave Software, Inc. |
| brave.exe                  | < 0.01 | 59.480 K      | 93.116 K    | 19944 | Brave Browser | Brave Software, Inc. |
| brave.exe                  | 0.37   | 83.434 K      | 133.188 K   | 8888  | Brave Browser | Brave Software, Inc. |

CPU Usage: 3.83% Commit Charge: 56.94% Processes: 273 Physical Usage: 69.73%

Per Terminare il processo possiamo killare il processo padre e tutte le finestre del

browser saranno chiuse.



Come 3\* step andiamo a startare un nuovo processo:

Aprendo il cmd, andiamo a cercare il processo da Process Explorer:



Possiamo vedere che il processo cmd.exe ha come padre il processo explorer.exe, e ha un processo figlio conhost.exe .

Ora se facciamo un test di un ping, vedremo che ci saranno dei cambiamenti sotto il processo cmd.exe:

| Process           | CPU    | Private Bytes | Working Set | PID   | Description                   | Company Name                   |
|-------------------|--------|---------------|-------------|-------|-------------------------------|--------------------------------|
| brave.exe         |        | 133.968 K     | 152.540 K   | 8524  | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 20.212 K      | 24.456 K    | 2496  | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 206.932 K     | 140.944 K   | 14384 | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 50.388 K      | 94.084 K    | 17100 | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         | < 0.01 | 443.488 K     | 361.460 K   | 13780 | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         | < 0.01 | 19.756 K      | 28.200 K    | 2972  | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 50.948 K      | 103.196 K   | 19944 | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         | 0.28   | 82.236 K      | 132.772 K   | 9992  | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 41.764 K      | 89.120 K    | 17036 | Brave Browser                 | Brave Software, Inc.           |
| brave.exe         |        | 16.368 K      | 34.692 K    | 22132 | Brave Browser                 | Brave Software, Inc.           |
| SnippingTool.exe  |        | 147.944 K     | 148.568 K   | 22332 |                               |                                |
| procexp.exe       |        | 4.712 K       | 8.592 K     | 7024  | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| procexp64.exe     | 0.65   | 44.756 K      | 47.020 K    | 21888 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| Spotify.exe       | 0.37   | 159.768 K     | 203.852 K   | 22340 | Spotify                       | Spotify Ltd                    |
| Spotify.exe       |        | 15.452 K      | 20.740 K    | 12400 | Spotify                       | Spotify Ltd                    |
| Spotify.exe       |        | 369.144 K     | 308.860 K   | 19204 | Spotify                       | Spotify Ltd                    |
| Spotify.exe       |        | 25.204 K      | 44.448 K    | 23540 | Spotify                       | Spotify Ltd                    |
| Spotify.exe       |        | 16.944 K      | 24.216 K    | 17404 | Spotify                       | Spotify Ltd                    |
| Spotify.exe       | 0.09   | 190.316 K     | 224.672 K   | 23992 | Spotify                       | Spotify Ltd                    |
| cmd.exe           | < 0.01 | 2.168 K       | 5.172 K     | 19044 | Processore dei comandi di ... | Microsoft Corporation          |
| conhost.exe       | < 0.01 | 1.456 K       | 9.092 K     | 1848  | Host finestra console         | Microsoft Corporation          |
| PING.EXE          | < 0.01 | 912 K         | 5.460 K     | 5696  | Comando Ping TCP/IP           | Microsoft Corporation          |
| urban-vpn-app.exe | 0.09   | 79.024 K      | 30.644 K    | 6684  |                               |                                |
| Discord.exe       | 0.18   | 115.748 K     | 122.864 K   | 6920  | Discord                       | Discord Inc.                   |
| Discord.exe       |        | 11.320 K      | 18.084 K    | 7344  | Discord                       | Discord Inc.                   |
| Discord.exe       | < 0.01 | 234.292 K     | 183.360 K   | 20616 | Discord                       | Discord Inc.                   |
| Discord.exe       | < 0.01 | 16.888 K      | 56.060 K    | 8756  | Discord                       | Discord Inc.                   |
| Discord.exe       | 0.65   | 470.416 K     | 450.616 K   | 12188 | Discord                       | Discord Inc.                   |
| Discord.exe       |        | 12.516 K      | 79.012 K    | 9080  | Discord                       | Discord Inc.                   |

CPU Usage: 6.64%   Commit Charge: 54.92%   Processes: 266   Physical Usage: 72.42%

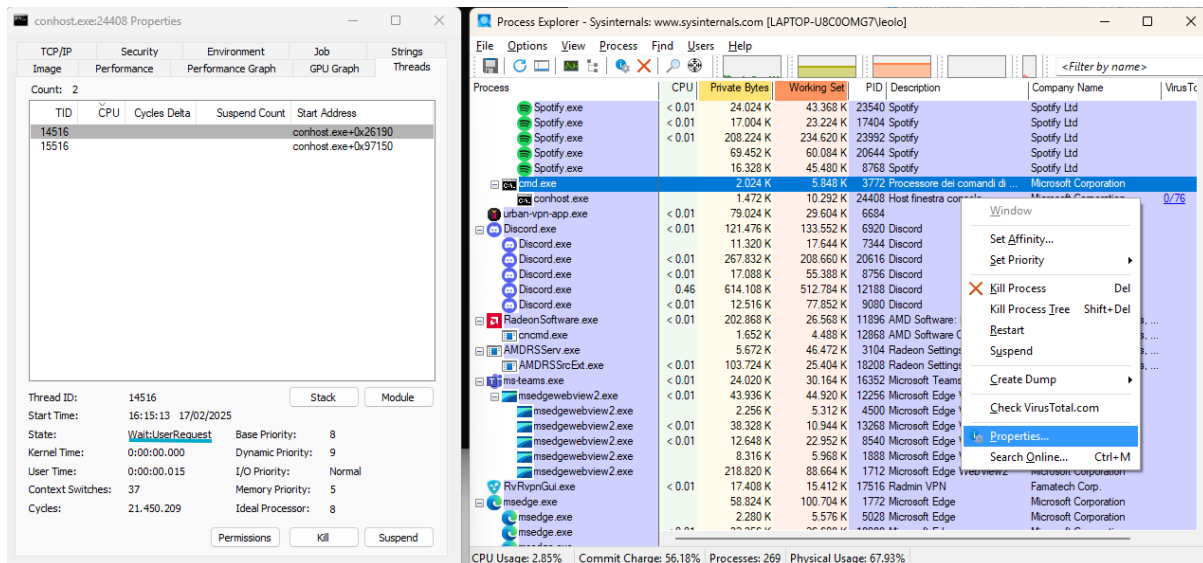
Un processo figlio PING.EXE sarà elencato sotto cmd.exe durante il processo di ping.

## -PART 2: Exploring Threads and Handles :

In this part, you will explore threads and handles. Processes have one or more threads. A thread is a unit of execution in a process. A handle is an abstract reference to memory blocks or objects managed by an operating system. You will use Process Explorer (procexp.exe) in Windows SysInternals Suite to explore the threads and handles.

Per far ciò andando su proprietà sul processo conhost.exe e andando nella sezione Threads vediamo che ci sono 2 thread uno che aspetta la richiesta dell'utente , e uno che aspetta l'esecuzione della richiesta.





### -PART 3: Exploring Windows Registry :

The Windows Registry is a hierarchical database that stores most of the operating systems and desktop environment configuration settings.

a. To access the Windows Registry, click **Start** > Search for **regedit** and select **Registry Editor**. Click **Yes** when asked to allow this app to make changes.

The Registry Editor has five hives. These hives are at the top level of the registry.

- **HKEY\_CLASSES\_ROOT** is actually the Classes subkey of **\*\*HKEY\_LOCAL\_MACHINE\Software\*\***. It stores information used by registered applications like file extension association, as well as a programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data.
- **HKEY\_CURRENT\_USER** contains the settings and configurations for the users who are currently logged in.
- **HKEY\_LOCAL\_MACHINE** stores configuration information specific to the local computer.
- **HKEY\_USERS** contains the settings and configurations for all the users on the local computer. **HKEY\_CURRENT\_USER** is a subkey of **HKEY\_USERS**.
- **HKEY\_CURRENT\_CONFIG** stores the hardware information that is used at bootup by the local computer.

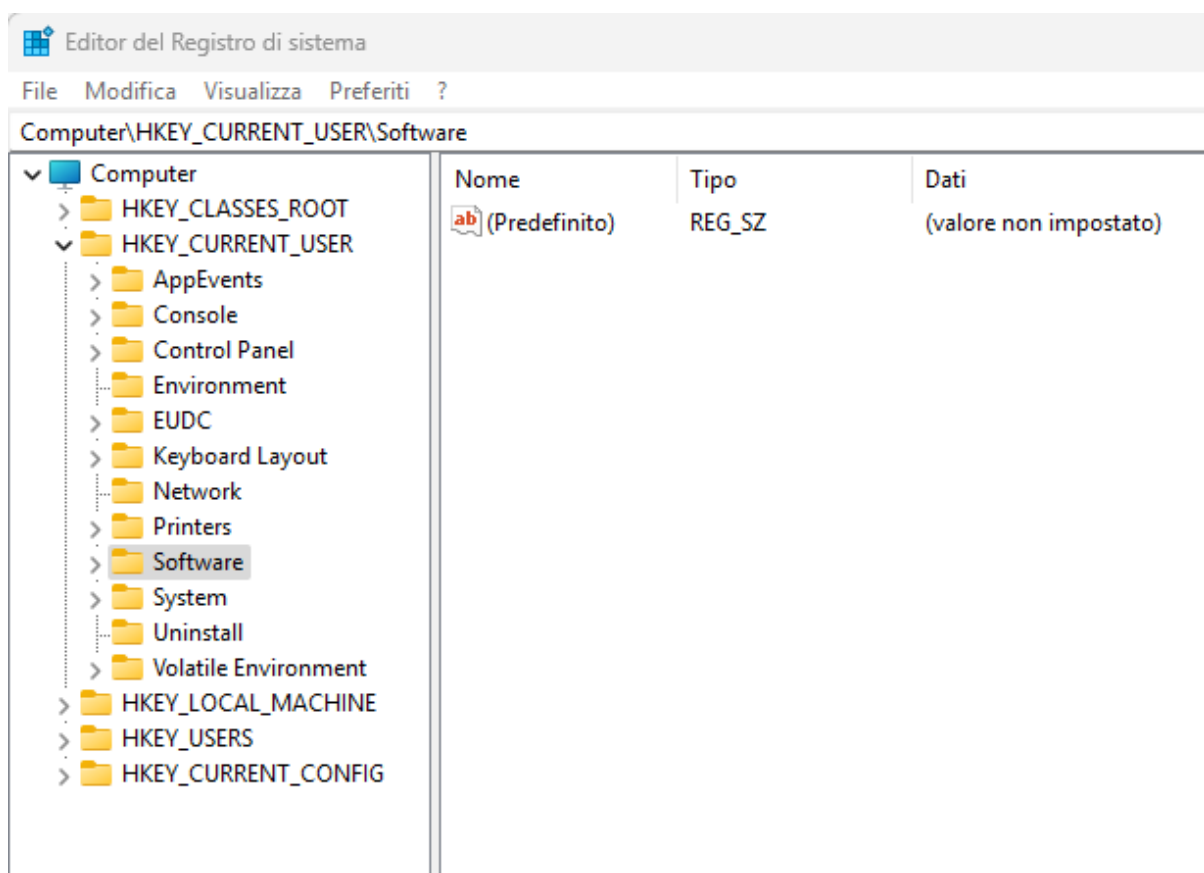
b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the *EulaAccepted* registry key for Process Explorer.

Click to select *Process Explorer* in **HKEY\_CURRENT\_USER > Software > Sysinternals > Process Explorer**. Scroll down to locate the key *EulaAccepted*. Currently, the value for the registry key *EulaAccepted* is **0x00000001(1)**.

c. Double-click **EulaAccepted** registry key. Currently, the value data is set to **1**. The value of **1** indicates that the EULA has been accepted by the user.

d. Change the **1** to **0** for Value data. The value of **0** indicates that the EULA was not accepted. Click **OK** to continue.

Iniziamo con aprire l'Editor del registro di sistema windows:



Nello specifico dovremmo andare nel seguente path " HKEY\_CURRENT\_USER -> Software -> Sysinternals -> Process Explorer.



| Editor del Registro di sistema                                    |            |  |  |
|---|------------|--|--|
| File Modifica Visualizza Preferiti ?                              |            |  |  |
| Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer |            |  |  |
| Nome  | Tipo       | Dati   |  |
| (Predefinito)   | REG_SZ     | (valore non impostato)                             |  |
| AlwaysOntop   | REG_DWORD  | 0x00000000 (0)                                     |  |
| ColorDelProc  | REG_DWORD  | 0x004646ff (4605695)                               |  |
| ColorDelProcDark  | REG_DWORD  | 0x00000046 (70)                                    |  |
| ColorGraphBk  | REG_DWORD  | 0x00f0f0f0 (15790320)                              |  |
| ColorGraphBkD...  | REG_DWORD  | 0x00343434 (3421236)                               |  |
| ColorImmersive  | REG_DWORD  | 0x00eaea00 (15395328)                              |  |
| ColorImmersive...   | REG_DWORD  | 0x00333300 (3355392)                               |  |
| ColorJobs   | REG_DWORD  | 0x00006cd0 (27856)                                 |  |
| ColorJobsDark   | REG_DWORD  | 0x0000172d (5933)                                  |  |
| ColorNet  | REG_DWORD  | 0x00a0ffff (10551295)                              |  |
| ColorNetDark  | REG_DWORD  | 0x00005959 (22873)                                 |  |
| ColorNewProc  | REG_DWORD  | 0x0046ff46 (4652870)                               |  |
| ColorNewProcD...  | REG_DWORD  | 0x00004600 (17920)                                 |  |
| ColorOwn  | REG_DWORD  | 0x00ffd0d0 (16765136)                              |  |
| ColorOwnDark  | REG_DWORD  | 0x00640000 (6553600)                               |  |
| ColorPacked   | REG_DWORD  | 0x00ff0080 (16711808)                              |  |
| ColorPackedDark   | REG_DWORD  | 0x0037001c (3604508)                               |  |
| ColorProtected  | REG_DWORD  | 0x008000ff (8388663)                               |  |
| ColorProtected...   | REG_DWORD  | 0x001c0037 (1835063)                               |  |
| ColorRelocated...   | REG_DWORD  | 0x00a0ffff (10551295)                              |  |
| ColorRelocated...   | REG_DWORD  | 0x00005959 (22873)                                 |  |
| ColorServices   | REG_DWORD  | 0x00d0d0ff (13684991)                              |  |
| ColorServicesDark   | REG_DWORD  | 0x00000064 (100)                                   |  |
| ColorSuspend  | REG_DWORD  | 0x00808080 (8421504)                               |  |
| ColorSuspendD...  | REG_DWORD  | 0x001b1b1b (1776411)                               |  |
| ConfirmKill   | REG_DWORD  | 0x00000001 (1)                                     |  |
| DbgHelpPath   | REG_SZ     | C:\Windows\SYSTEM32\dbghelp.dll                    |  |
| DefaultDllProp...   | REG_DWORD  | 0x00000000 (0)                                     |  |
| DefaultProcProp...  | REG_DWORD  | 0x00000006 (6)                                     |  |
| DefaultSysInfoP...  | REG_DWORD  | 0x00000000 (0)                                     |  |
| Divider   | REG_BINARY | 00 00 00 00 00 00 e0 3f                            |  |
| DllColumnCount  | REG_DWORD  | 0x00000004 (4)                                     |  |
| DllPropWindow...  | REG_BINARY | 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |  |
| DllSortColumn   | REG_DWORD  | 0x00000000 (0)                                     |  |
| DllSortDirection  | REG_DWORD  | 0x00000001 (1)                                     |  |
| ETWStandardUs...  | REG_DWORD  | 0x00000000 (0)                                     |  |
| EulaAccepted  | REG_DWORD  | 0x00000001 (1)                                     |  |
| FindWindowpla...  | REG_BINARY | 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |  |
| FormatIoBytes   | REG_DWORD  | 0x00000001 (1)                                     |  |
| GpuNodeUsage...   | REG_DWORD  | 0x00000001 (1)                                     |  |
| GpuNodeUsage...   | REG_DWORD  | 0x00000000 (0)                                     |  |
| HandleColumn...   | REG_DWORD  | 0x00000002 (2)                                     |  |
| HandleSortColu...   | REG_DWORD  | 0x00000000 (0)                                     |  |
| HandleSortDirec...  | REG_DWORD  | 0x00000001 (1)                                     |  |
| HideWhenMini...   | REG_DWORD  | 0x00000000 (0)                                     |  |
| HighlightDelProc  | REG_DWORD  | 0x00000001 (1)                                     |  |
| HighlightDuration   | REG_DWORD  | 0x000003e8 (1000)                                  |  |

Di base il valore è a 0x00000001, il valore 1 indica che l'EULA è stato accettato dall'utente.

Andiamo a cambiare il valore da 1 a 0 così che L'EULA non sarà più accettata.

Modifica valore DWORD (32 bit)

Nome valore:

EulaAccepted

Dati valore:

0

Base

☒ Esadecimale
 ☐ Decimale

OK

Annulla

Andando a riaprire il tool procexp.exe da SysInternalsSuite ci richiederà di accettare l'EULA (Explorer License Agreement).

