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 :

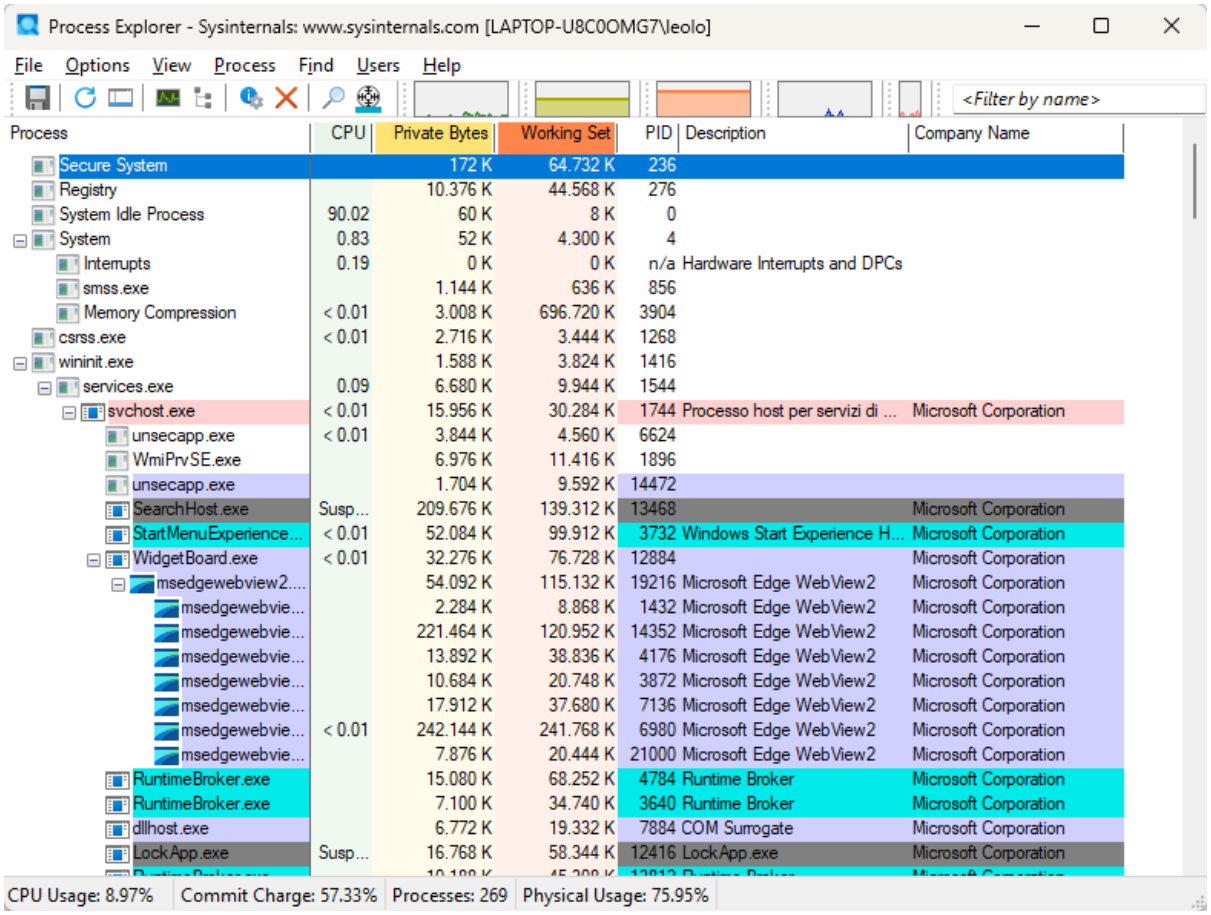
2. Exploring Threads and Handles :

3. Exploring Windows Registry :

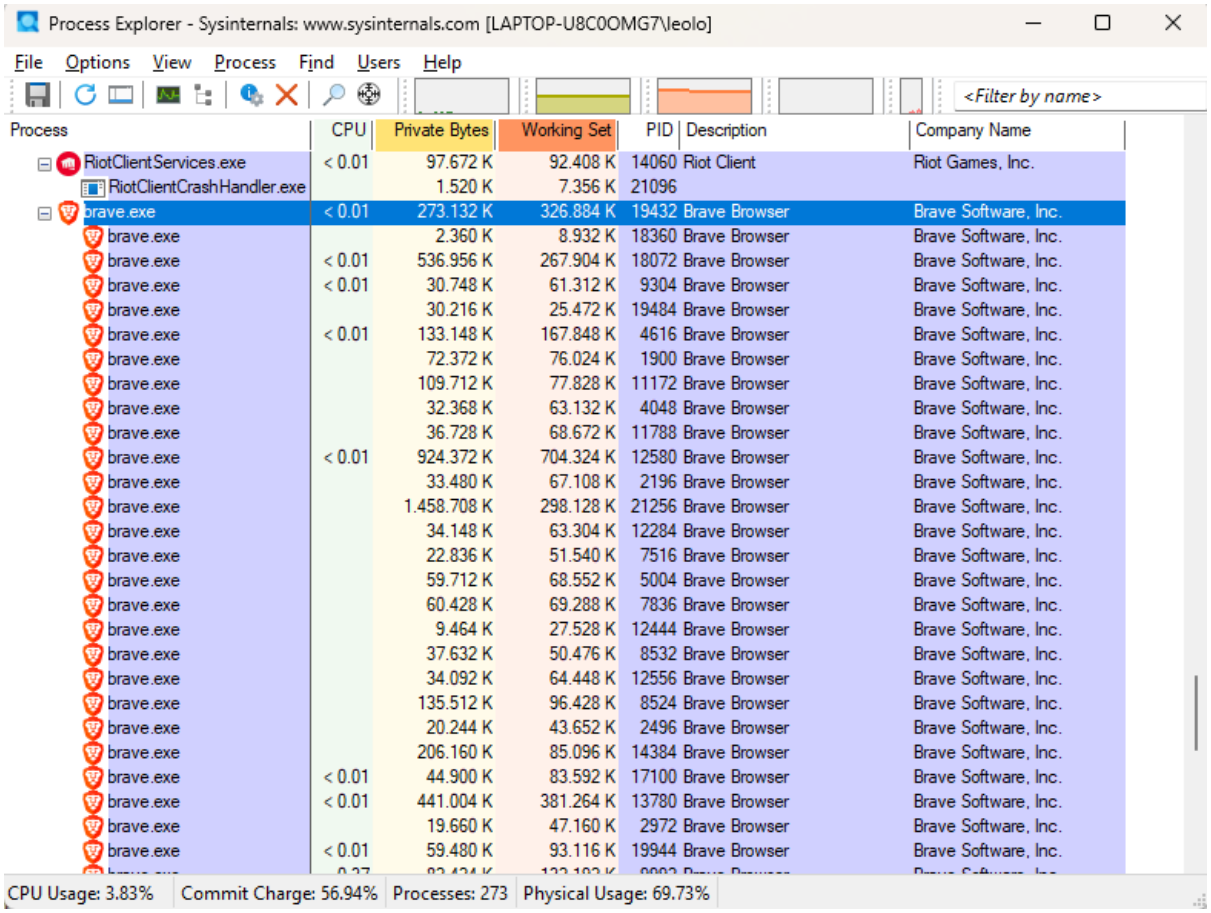
-PART 1: Exploring Processes
“In this, you will explore processes. Processes are programs or applications in execution. You will explore the processes using Process Explorer in the Windows SysInternals Suite. You will also start and observe a new process”.

Come 1* Step andremo a scaricare la Windows SysInernals 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.

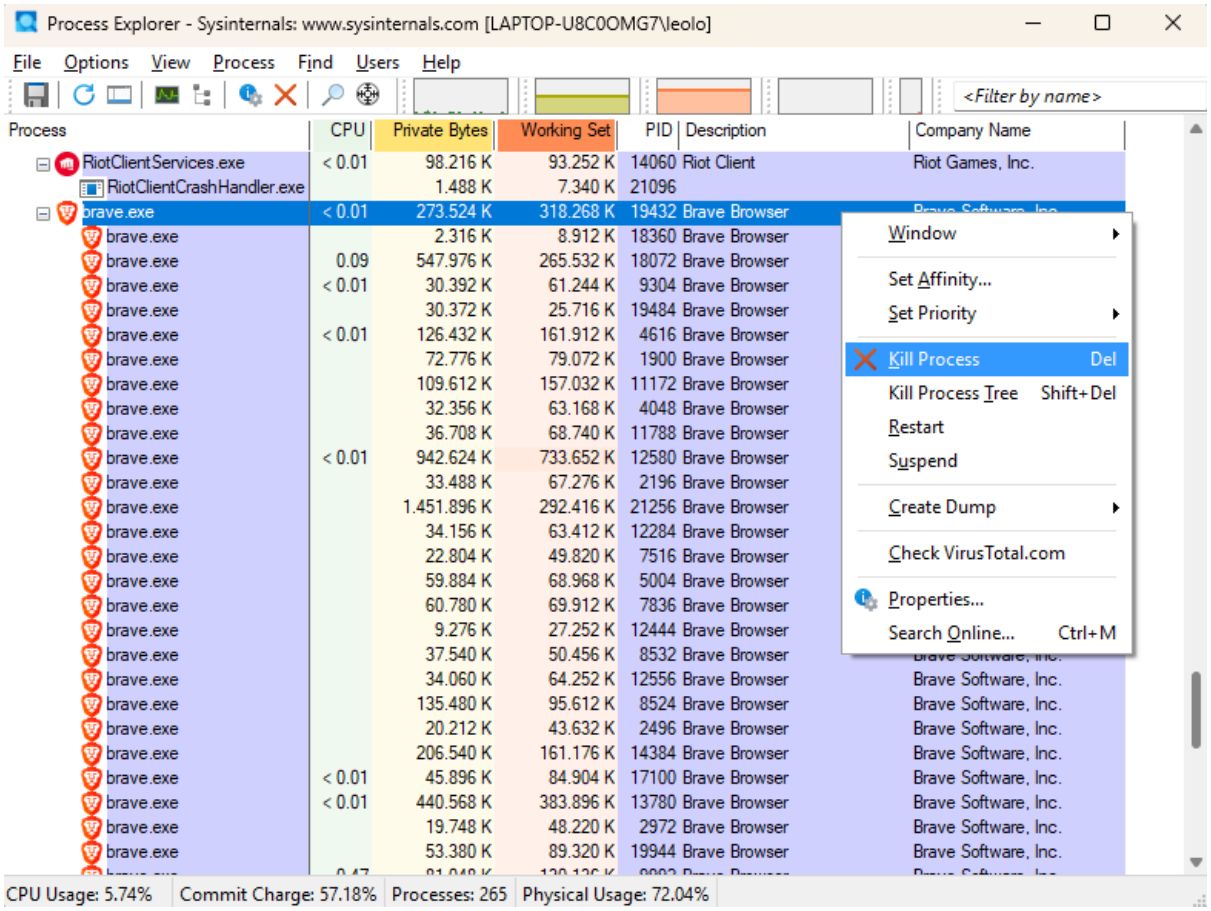


Per localizzare il web browser, si clicca l'icona specifica (sottolineata nello screen) e ci apparirà nello specifico il processo del browser web (nel mio caso è Brave).



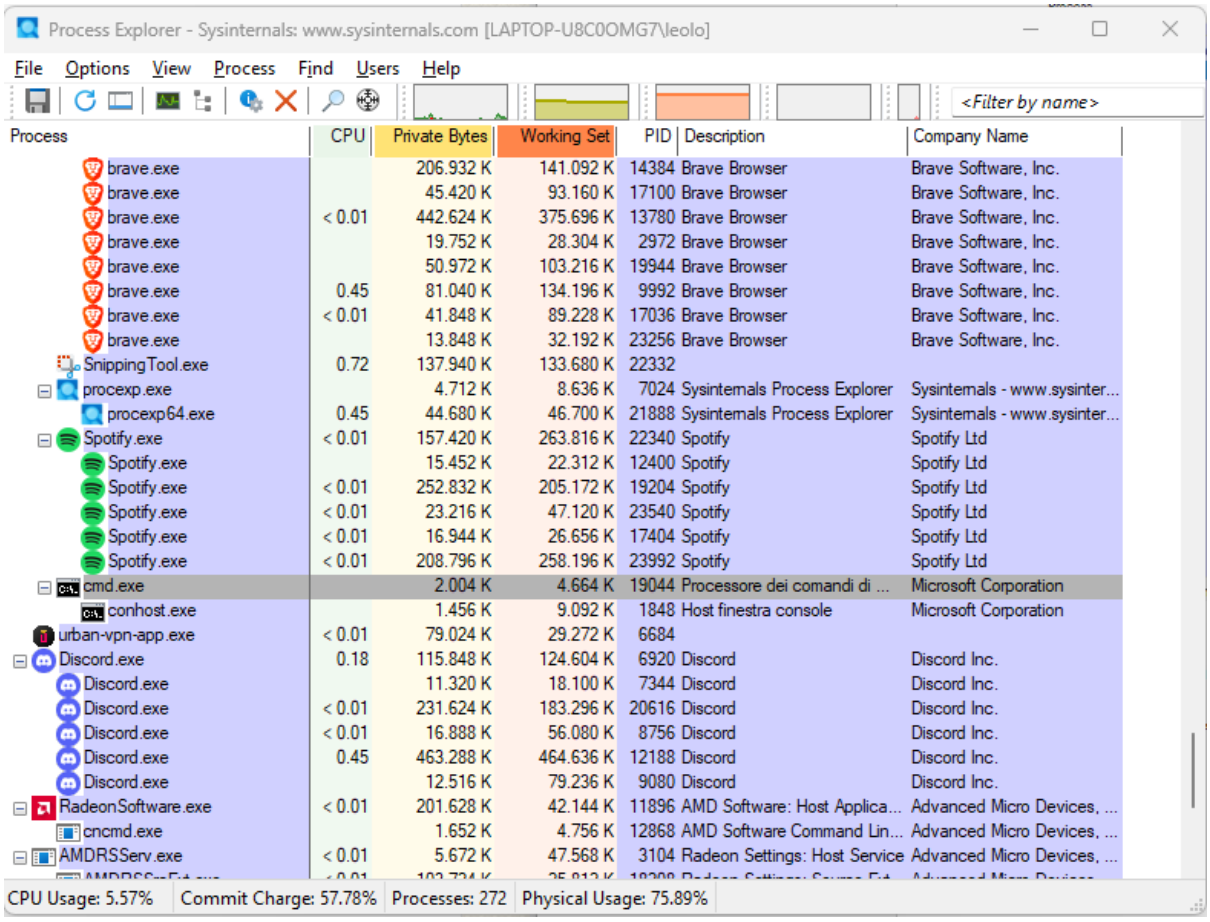
Per Terminare il processo possiamo killare il processo padre e tutte le finestre del

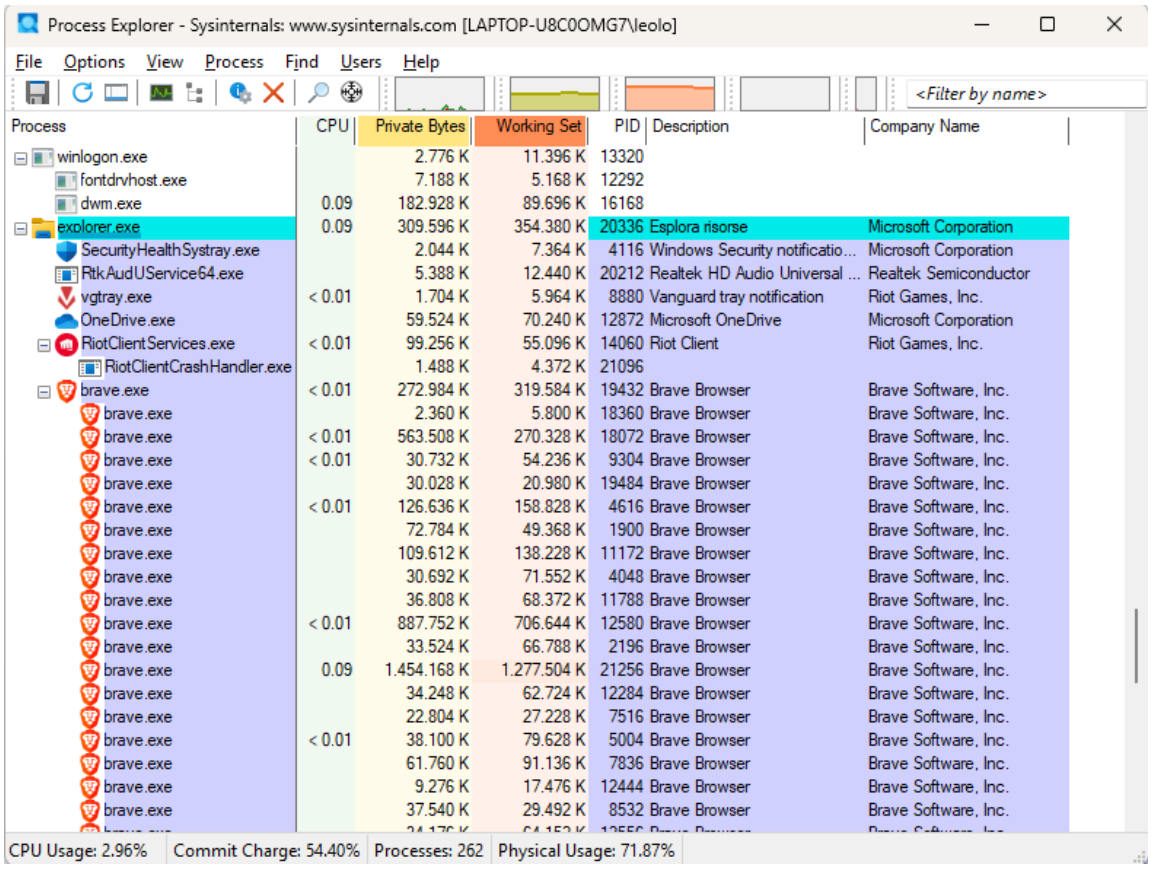
browser saranno chiuse.



Come 3* step andiamo a startare un nuovo processo:

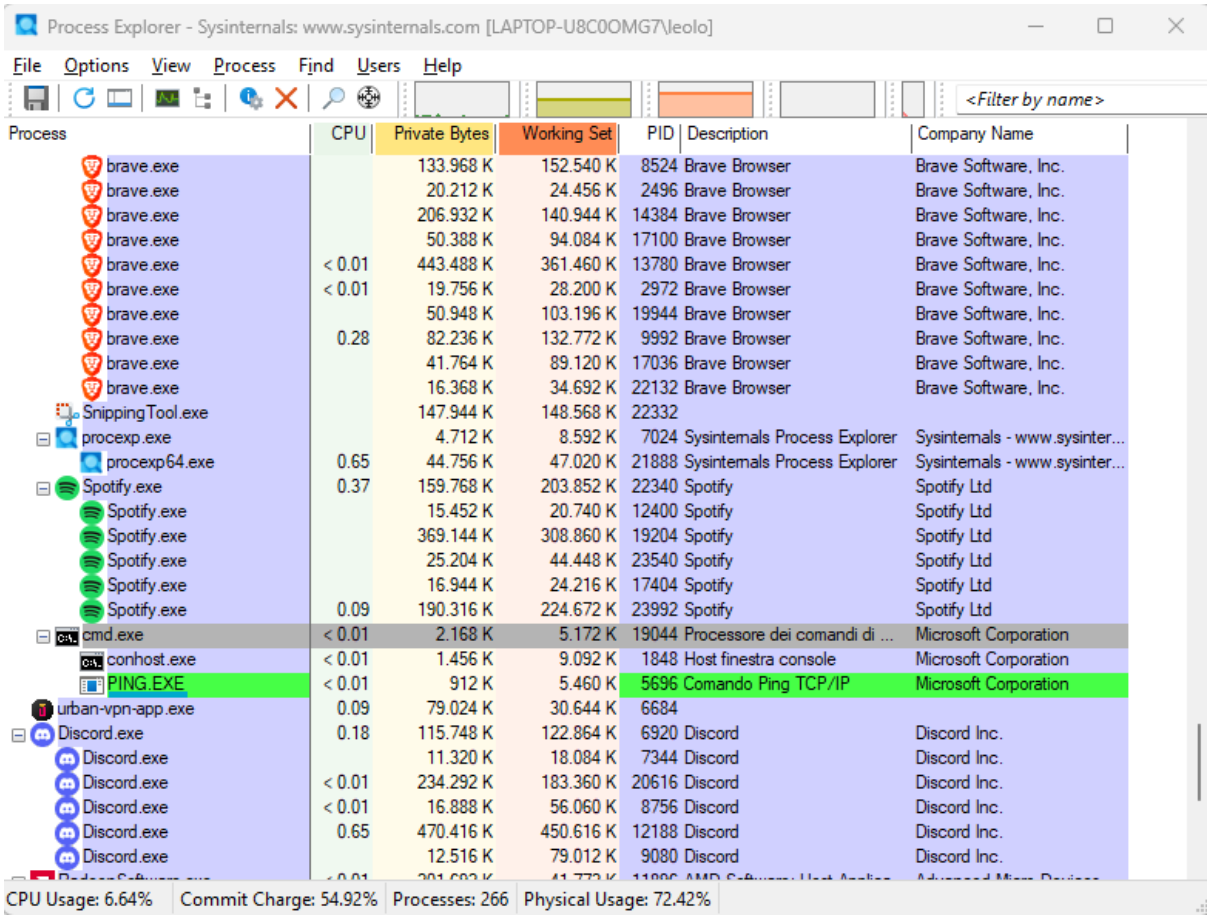
Aprendo il cmd, andiamo a cercare il processo da Process Explorer:


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
brave.exe 206.932 K 141.092 K 14384 Brave Browser Brave Software, Inc.
brave.exe 45.420 K 93.160 K 17100 Brave Browser Brave Software, Inc.
brave.exe < 0.01 442.624 K 375.696 K 13780 Brave Browser Brave Software, Inc.
brave.exe 19.752 K 28.304 K 2972 Brave Browser Brave Software, Inc.
brave.exe 50.972 K 103.216 K 19944 Brave Browser Brave Software, Inc.
brave.exe 0.45 81.040 K 134.196 K 9992 Brave Browser Brave Software, Inc.
brave.exe < 0.01 41.848 K 89.228 K 17036 Brave Browser Brave Software, Inc.
brave.exe 13.848 K 32.192 K 23256 Brave Browser Brave Software, Inc.
SnippingTool.exe 0.72 137.940 K 133.680 K 22332
procexp.exe 4.712 K 8.636 K 7024 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe 0.45 44.680 K 46.700 K 21888 Sysinternals Process Explorer Sysinternals - www.sysinter...
Spotify.exe < 0.01 157.420 K 263.816 K 22340 Spotify Spotify Ltd
Spotify.exe 15.452 K 22.312 K 12400 Spotify Spotify Ltd
Spotify.exe < 0.01 252.832 K 205.172 K 19204 Spotify Spotify Ltd
Spotify.exe < 0.01 23.216 K 47.120 K 23540 Spotify Spotify Ltd
Spotify.exe < 0.01 16.944 K 26.656 K 17404 Spotify Spotify Ltd
Spotify.exe < 0.01 208.796 K 258.196 K 23992 Spotify Spotify Ltd
cmd.exe 2.004 K 4.664 K 19044 Processore dei comandi di ... Microsoft Corporation
conhost.exe 1.456 K 9.092 K 1848 Host finestra console Microsoft Corporation
urban-vpn-app.exe < 0.01 79.024 K 29.272 K 6684
Discord.exe 0.18 115.848 K 124.604 K 6920 Discord Discord Inc.
Discord.exe 11.320 K 18.100 K 7344 Discord Discord Inc.
Discord.exe < 0.01 231.624 K 183.296 K 20616 Discord Discord Inc.
Discord.exe < 0.01 16.888 K 56.080 K 8756 Discord Discord Inc.
Discord.exe 0.45 463.288 K 464.636 K 12188 Discord Discord Inc.
Discord.exe 12.516 K 79.236 K 9080 Discord Discord Inc.
RadeonSoftware.exe < 0.01 201.628 K 42.144 K 11896 AMD Software: Host Applica... Advanced Micro Devices, ...
cncmd.exe 1.652 K 4.756 K 12868 AMD Software Command Lin... Advanced Micro Devices, ...
AMDRSServ.exe < 0.01 5.672 K 47.568 K 3104 Radeon Settings: Host Service Advanced Micro Devices, ...
CPU Usage: 5.57% Commit Charge: 57.78% Processes: 272 Physical Usage: 75.89%


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
winlogon.exe 2.776 K 11.396 K 13320
fontdrvhost.exe 7.188 K 5.168 K 12292
dwm.exe 0.09 182.928 K 89.696 K 16168
explorer.exe 0.09 309.596 K 354.380 K 20336 Esplora risorse Microsoft Corporation
SecurityHealthSystray.exe 2.044 K 7.364 K 4116 Windows Security notificatio... Microsoft Corporation
RtkAudUService64.exe 5.388 K 12.440 K 20212 Realtek HD Audio Universal ... Realtek Semiconductor
vgtray.exe < 0.01 1.704 K 5.964 K 8880 Vanguard tray notification Riot Games, Inc.
OneDrive.exe 59.524 K 70.240 K 12872 Microsoft OneDrive Microsoft Corporation
RiotClientServices.exe < 0.01 99.256 K 55.096 K 14060 Riot Client Riot Games, Inc.
RiotClientCrashHandler.exe 1.488 K 4.372 K 21096
brave.exe < 0.01 272.984 K 319.584 K 19432 Brave Browser Brave Software, Inc.
brave.exe 2.360 K 5.800 K 18360 Brave Browser Brave Software, Inc.
brave.exe < 0.01 563.508 K 270.328 K 18072 Brave Browser Brave Software, Inc.
brave.exe < 0.01 30.732 K 54.236 K 9304 Brave Browser Brave Software, Inc.
brave.exe 30.028 K 20.980 K 19484 Brave Browser Brave Software, Inc.
brave.exe < 0.01 126.636 K 158.828 K 4616 Brave Browser Brave Software, Inc.
brave.exe 72.784 K 49.368 K 1900 Brave Browser Brave Software, Inc.
brave.exe 109.612 K 138.228 K 11172 Brave Browser Brave Software, Inc.
brave.exe 30.692 K 71.552 K 4048 Brave Browser Brave Software, Inc.
brave.exe 36.808 K 68.372 K 11788 Brave Browser Brave Software, Inc.
brave.exe < 0.01 887.752 K 706.644 K 12580 Brave Browser Brave Software, Inc.
brave.exe 33.524 K 66.788 K 2196 Brave Browser Brave Software, Inc.
brave.exe 0.09 1.454.168 K 1.277.504 K 21256 Brave Browser Brave Software, Inc.
brave.exe 34.248 K 62.724 K 12284 Brave Browser Brave Software, Inc.
brave.exe 22.804 K 27.228 K 7516 Brave Browser Brave Software, Inc.
brave.exe < 0.01 38.100 K 79.628 K 5004 Brave Browser Brave Software, Inc.
brave.exe 61.760 K 91.136 K 7836 Brave Browser Brave Software, Inc.
brave.exe 9.276 K 17.476 K 12444 Brave Browser Brave Software, Inc.
brave.exe 37.540 K 29.492 K 8532 Brave Browser Brave Software, Inc.
CPU Usage: 2.96% Commit Charge: 54.40% Processes: 262 Physical Usage: 71.87%

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:

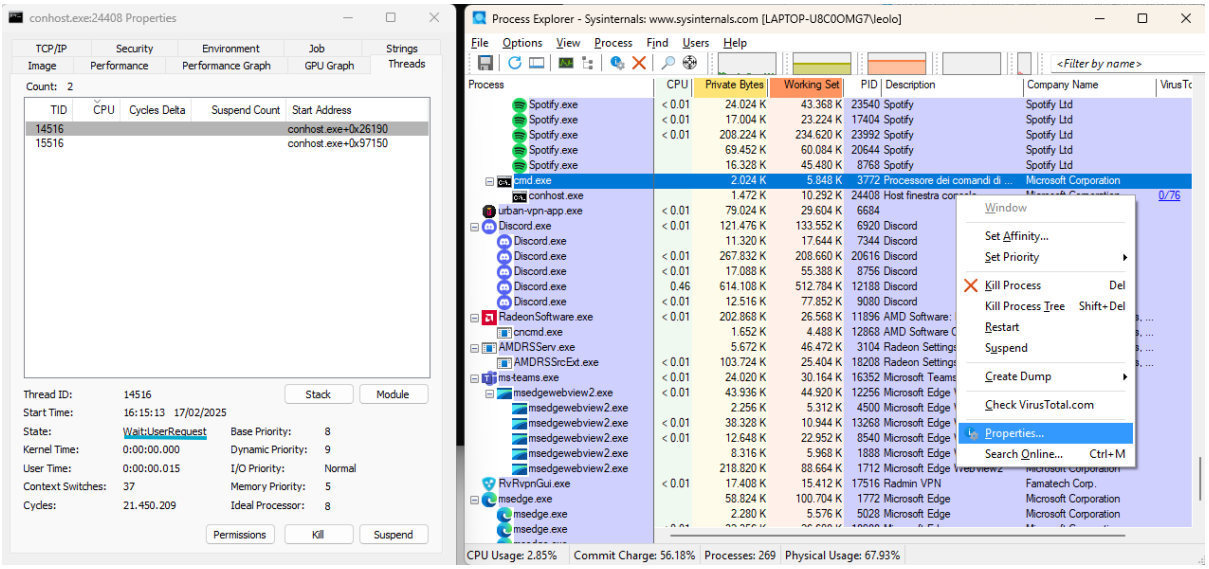


Un processo figlio PING.EXE sarà elencato sotto cmd.exe durante il processo di ping.

-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.

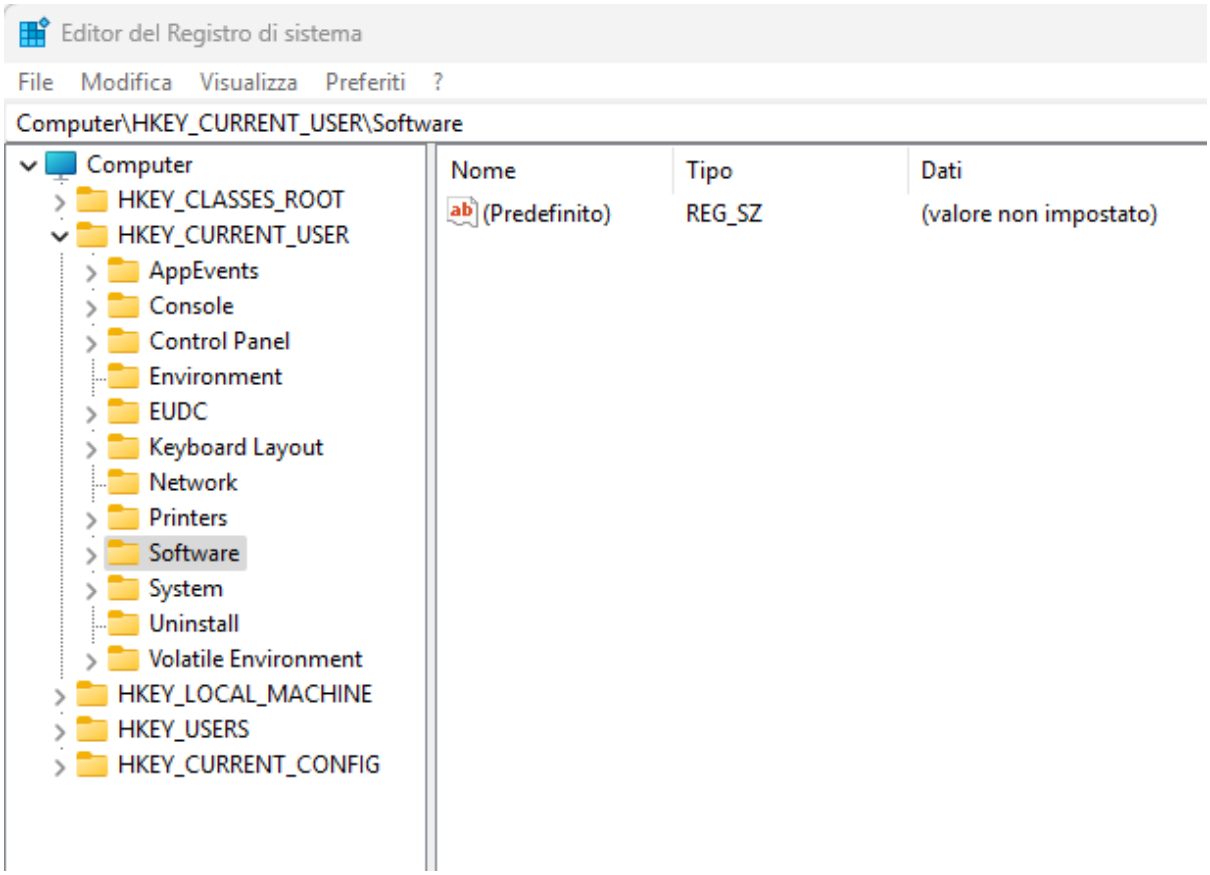
b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the *EulaAccepted* registry key for Process Explorer.

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)**.

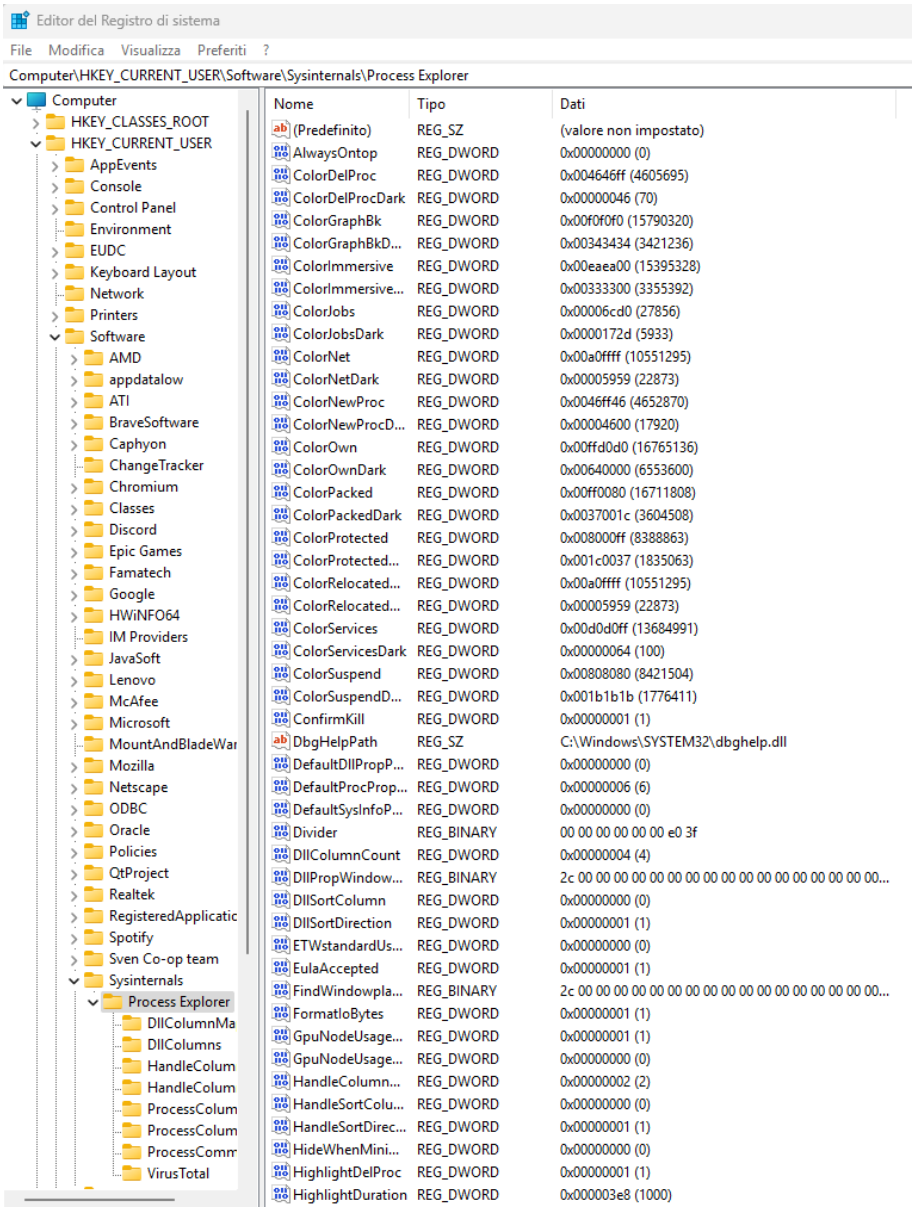
c. Double-click **EulaAccepted** registry key. Currently, the value data is set to **1**. The value of **1** indicates that the EULA has been accepted by the user.

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:

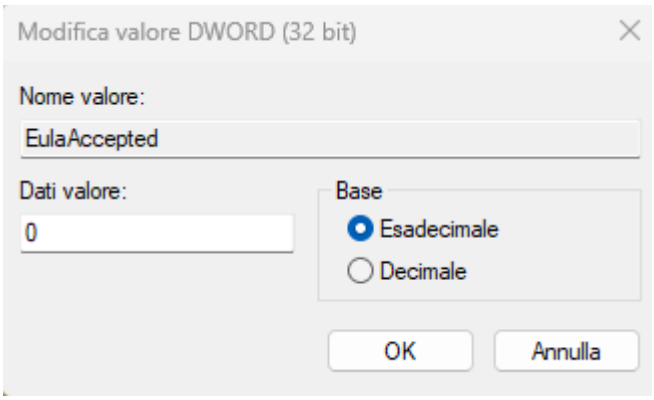


Nello specifico dovremmo andare nel seguente path " HKEY_CURRENT_USER -> Software -> Sysinternals -> Process Explorer.



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 cosi' che L'EULA non sarà più accettata.



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