















CYBER OPS PRACTICE 1

1. Scarica SysInternals Suite

▼ All'inizio dell'anno

 Sysmon	23/07/2024 14:08	Applicazione	8.282 KB
 Sysmon64	23/07/2024 14:08	Applicazione	4.457 KB
 Eula	23/07/2024 14:08	File TXT	8 KB
 Procmon	20/06/2024 21:55	Applicazione	4.029 KB
 Procmon64	20/06/2024 21:55	Applicazione	2.093 KB
 procxp	28/05/2024 16:11	Applicazione	4.425 KB
 procxp64	28/05/2024 16:11	Applicazione	2.326 KB
 ZoomIt	07/02/2024 16:27	Applicazione	1.616 KB
 ZoomIt64	07/02/2024 16:27	Applicazione	863 KB
 autoruns	06/02/2024 18:49	File della Guida H...	25 KB
 Autoruns	06/02/2024 18:49	Applicazione	1.718 KB
 Autoruns64	06/02/2024 18:49	Applicazione	1.910 KB
 autorunc	06/02/2024 18:49	Applicazione	702 KB
 autorunc64	06/02/2024 18:49	Applicazione	786 KB

2. Esplora un processo attivo

Come richiesto dalla traccia, dopo aver effettuato il download della **Sys Internal Suite**, procedo a lanciare **procexp**.

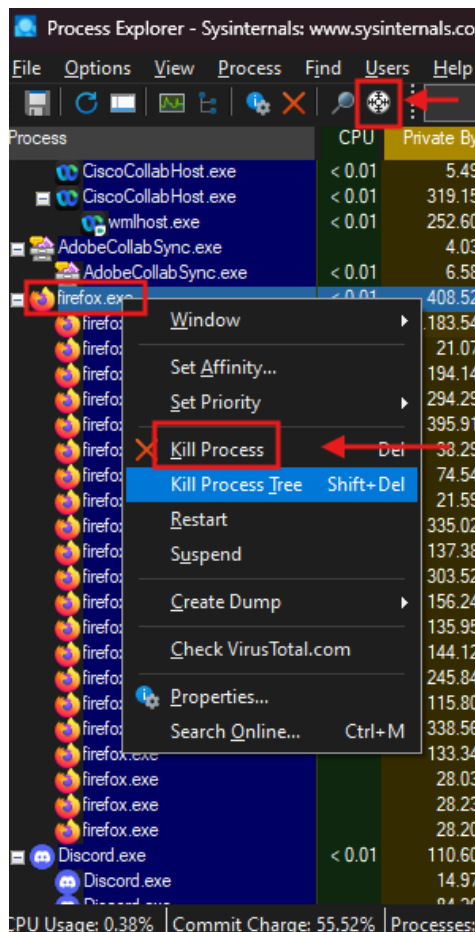
The screenshot shows the Windows Task Manager application window titled "Process Explorer - Sysinternals: www.sysinternals.com [IBN5100\il_giangi_meneghetti]". The menu bar includes File, Options, View, Process, Find, Users, and Help. Below the menu is a toolbar with various icons for task management. A search filter box at the top right contains the text "<Filter by name>".

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		188 K	46.196 K	140		
Registry		7.332 K	42.960 K	180		
System Idle Process	100.00	60 K	8 K	0		
System	< 0.01	64 K	10.876 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1.084 K	1.100 K	652		
Memory Compression		1.612 K	655.148 K	2720		
csrss.exe		2.056 K	5.048 K	852		
wininit.exe		1.448 K	6.180 K	944		
services.exe		5.236 K	9.748 K	1020		
svchost.exe		9.712 K	27.968 K	1104	Processo host per servizi di ...	Microsoft Corporation
SearchHost.exe	Susp...	250.232 K	308.120 K	8024		Microsoft Corporation
StartMenuExperienceHost.exe		84.164 K	111.196 K	8048	Windows Start Experience Host	Microsoft Corporation
Widgets.exe		12.280 K	53.628 K	6964		Microsoft Corporation
msedgewebview2.exe		35.560 K	11.728 K	4672	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2.092 K	7.368 K	3724	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		94.216 K	5.724 K	10436	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		11.368 K	6.396 K	10940	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		7.860 K	392 K	12944	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		129.456 K	504 K	2360	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		7.100 K	3.044 K	14080	Microsoft Edge WebView2	Microsoft Corporation
RuntimeBroker.exe		6.592 K	27.460 K	7536	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		13.288 K	48.932 K	8312	Runtime Broker	Microsoft Corporation
WidgetService.exe		4.404 K	20.460 K	8512	WidgetService.exe	Microsoft Corporation
dllhost.exe		6.372 K	16.868 K	7904	COM Surrogate	Microsoft Corporation
PhoneExperienceHost.exe		92.284 K	170.852 K	10728	Microsoft Phone Link	Microsoft Corporation
ShellExperienceHost.exe	Susp...	65.452 K	105.436 K	11636	Windows Shell Experience Host	Microsoft Corporation
RuntimeBroker.exe		6.972 K	28.544 K	11700	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		4.652 K	22.332 K	11876	System Settings Broker	Microsoft Corporation
ApplicationFrameHost.exe		12.416 K	22.748 K	12316	Application Frame Host	Microsoft Corporation

At the bottom of the window, there are three status bars:

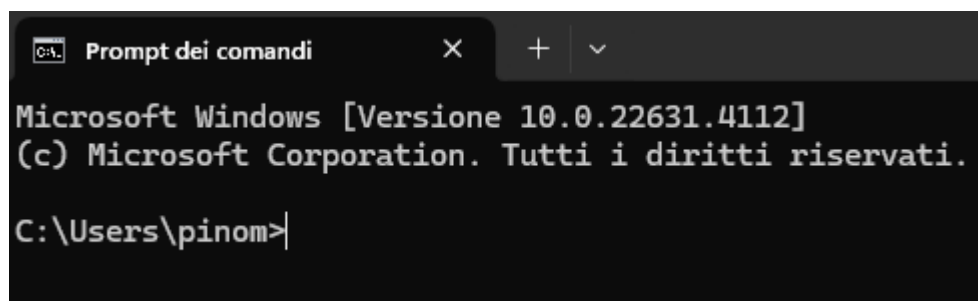
- CPU Usage: 0.00%
- Commit Charge: 55.42%
- Physical Usage: 49.29%

Successivamente chiede di trascinare l'icona **Find Windows Process** (evidenziata dal rettangolo rosso) sulla finestra del browser in esecuzione per poi killare il processo. Per farlo, dopo che **procexp** avrà evidenziato automaticamente la riga del processo corrispondente, serve fare click destro e scegliere **kill process**.



3. Avvia un altro processo

Per prima cosa chiede di avviare il prompt dei comandi.



Successivamente chiede di spostare l'icona **Find Windows Process** sulla finestra del prompt dei comandi, così da evidenziare il processo nella finestra di **procexp**.



Viene visualizzato anche il processo figlio, ovvero **conhost.exe**, proprio sotto al processo **cmd.exe**.

Dopo aver avviato un **ping** sul prompt si vedrà apparire nella finestra il processo **PING.EXE**.

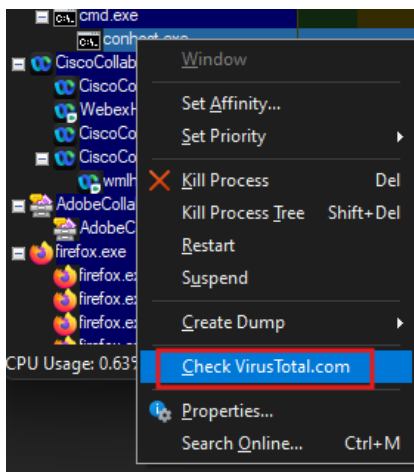
```
Microsoft Windows [Versione 10.0.22631.4112]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\pinom>ping www.google.it

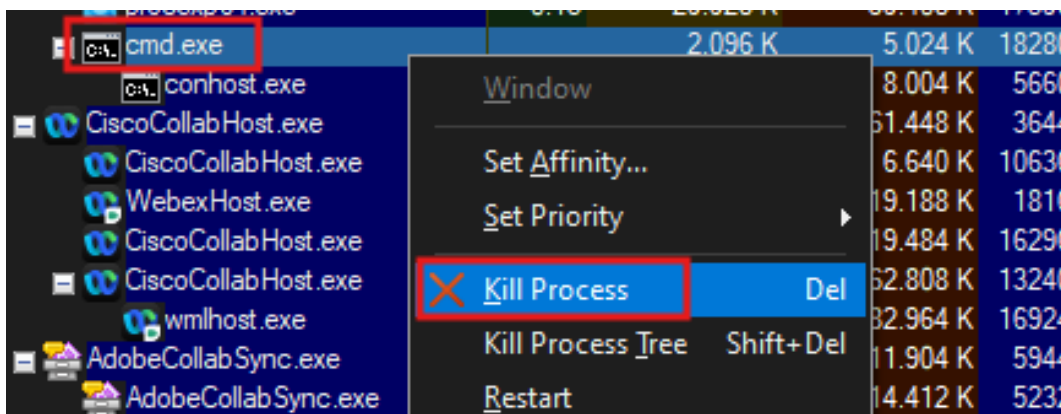
Esecuzione di Ping www.google.it [216.58.204.227] con 32 byte di dati:
Risposta da 216.58.204.227: byte=32 durata=68ms TTL=31
Risposta da 216.58.204.227: byte=32 durata=60ms TTL=31
```

cmd.exe	2.252 K
conhost.exe	1.336 K
PING.EXE	< 0.01
SpinningTool.exe	0.12

Viene poi richiesto di effettuare la scansione con **VirusTotal** del processo **conhost.exe**, cliccando col destro.

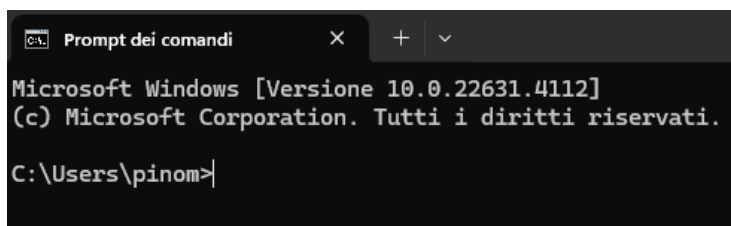


Poi chiede di effettuare il **kill** del processo **cmd.exe**. Di conseguenza viene effettuato il **kill** anche del processo figlio, ovvero **conhost.exe**.

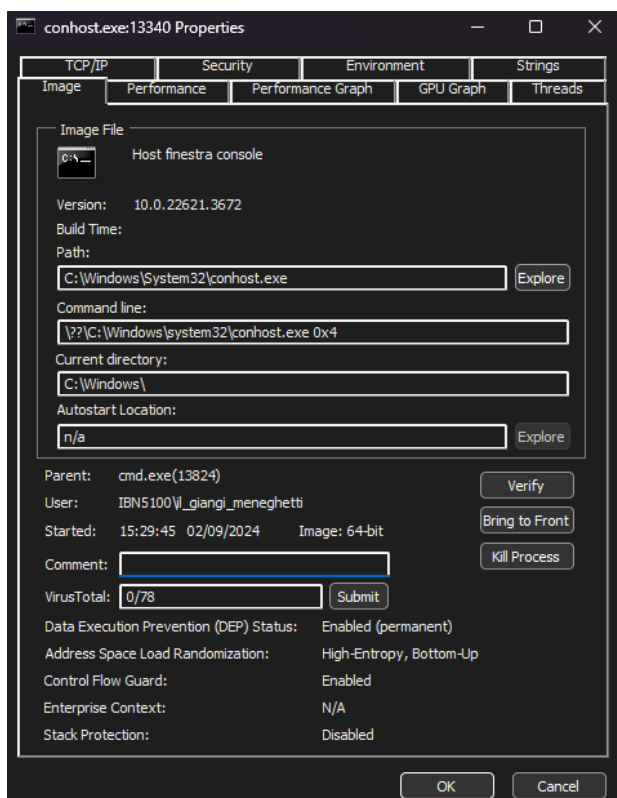
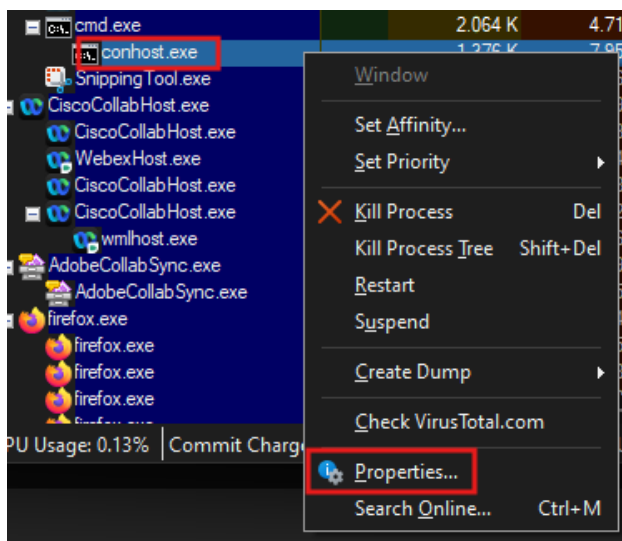


4. Esplorare Threads e Handles

Adesso chiede di avviare il **command prompt** nuovamente.



Successivamente chiede di fare click destro su **conhost.exe** ed aprire la scheda **properties**.



Si può accedere così a varie informazioni su quel processo attraverso tutte le schede disponibili poste in alto nella finestra.

conhost.exe:13340 Properties

TCP/IP Security Environment Strings

Image Performance Performance Graph GPU Graph Threads

CPU

Priority	8
Kernel Time	0:00:00.000
User Time	0:00:00.000
Total Time	0:00:00.000
Cycles	38.971.622

Virtual Memory

Private Bytes	1.316 K
Peak Private Bytes	1.432 K
Virtual Size	2.151.764.368 K
Page Faults	2.080
Page Fault Delta	0

Physical Memory

Memory Priority	5
Working Set	7.920 K
WS Private	920 K
WS Shareable	6.964 K
WS Shared	6.964 K
Peak Working Set	7.988 K

I/O

I/O Priority	Normal
Reads	4
Read Delta	0
Read Bytes Delta	0
Writes	0
Write Delta	0
Write Bytes Delta	0
Other	48
Other Delta	0
Other Bytes Delta	0

Handles

Handles	140
Peak Handles	140
GDI Handles	0
USER Handles	2

conhost.exe:13340 Properties

TCP/IP Security Environment Strings

Image Performance Performance Graph GPU Graph Threads

Count: 2

TID	CPU	Cycles Delta	Suspend Count	Start Address
15712				conhost.exe+0x9280
14196				conhost.exe+0x98670

Thread ID: 15712

Start Time: 15:29:45 02/09/2024

State: WaitUserRequest

Kernel Time: 0:00:00.000

User Time: 0:00:00.000

Context Switches: 33

Cycles: 18.117.450

Base Priority: 8

Dynamic Priority: 9

I/O Priority: Normal

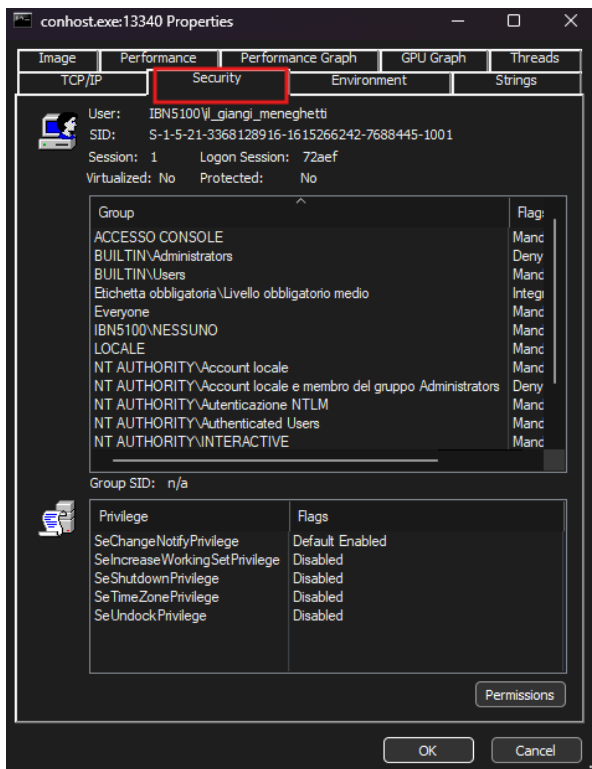
Memory Priority: 5

Ideal Processor: 3

Stack Module

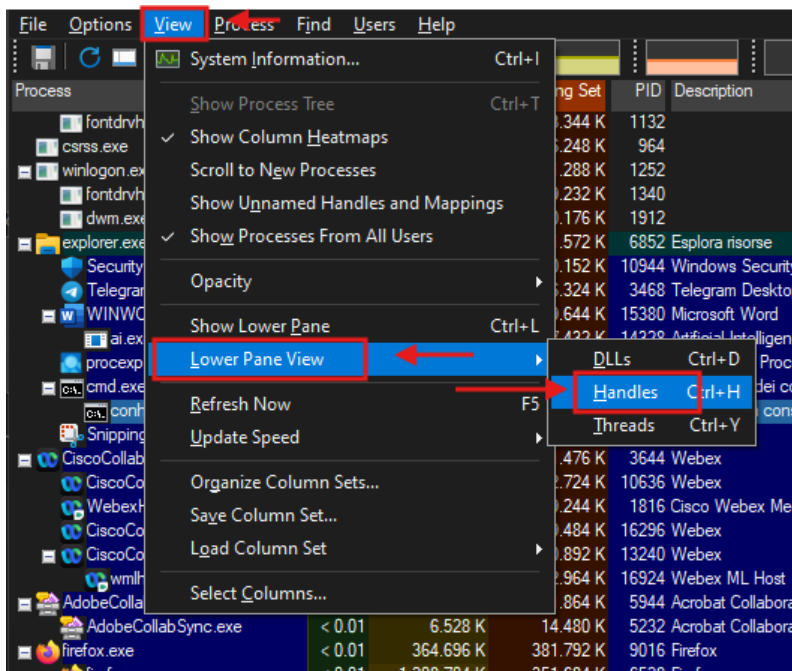
Permissions Kill Suspend

OK Cancel



5. Esplorazione Handles

In questo passaggio chiede di aprire il manu relativo agli **handles**.



Ci mostra come ogni **handle** punti a qualcosa di diverso: registri, file, oppure **threads**.

File Options View Process Find Users Handle Help	
Process	
fontdrvhost.exe	
Handles DLLs Threads	
Type	Name
ALPC Port	\RPC Control\OLEA28DF566C9365B4A5E4A786D789A
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\KsecDD
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackIt-IT_22621.74.291.0_...
File	\Device\CNG
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\TreatAsClassIndex
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom
Key	HKCU\Software\Classes\PackagedCom\Package
Key	HKCR\PackagedCom\Package
Key	HKCU\Software\Classes

CPU Usage: 0.36% | Commit Charge: 57.06% | Processes: 192 | Physical Usage: 48.22%

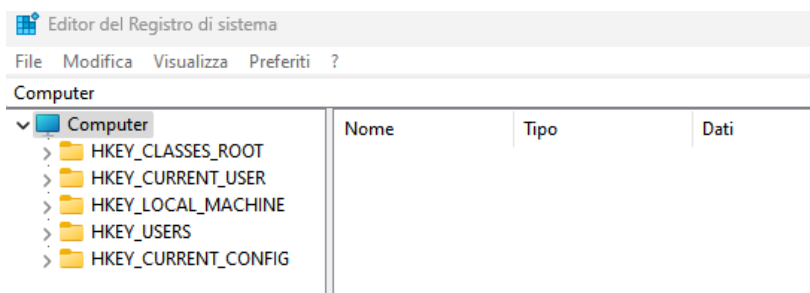
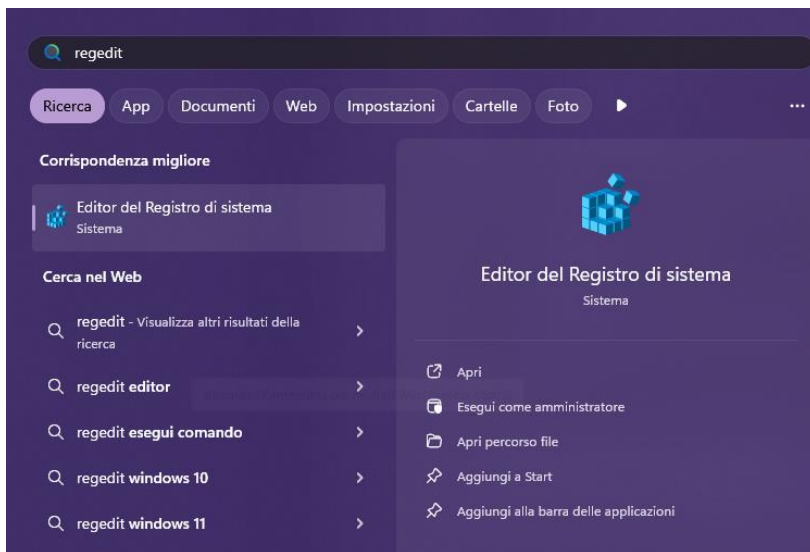
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom\InterfaceIndex
Mutant	\Sessions\1\BaseNamedObjects\SM0:13340:304:WilStaging_02
Mutant	\Sessions\1\BaseNamedObjects\SM0:13340:120:WilError_03
Section	\BaseNamedObjects__ComCatalogCache__
Section	\BaseNamedObjects__ComCatalogCache__
Semaphore	\Sessions\1\BaseNamedObjects\SM0:13340:304:WilStaging_02_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:13340:304:WilStaging_02_p0h
Semaphore	\Sessions\1\BaseNamedObjects\SM0:13340:120:WilError_03_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:13340:120:WilError_03_p0h
Thread	conhost.exe(13340): 14196
Thread	conhost.exe(13340): 15712
Thread	conhost.exe(13340): 15712
Window Station	\Sessions\1\Windows\WindowStations\WinSta0
Window Station	\Sessions\1\Windows\WindowStations\WinSta0

CPU Usage: 0.00% | Commit Charge: 56.74% | Processes: 192 | Physical Usage: 47.84%

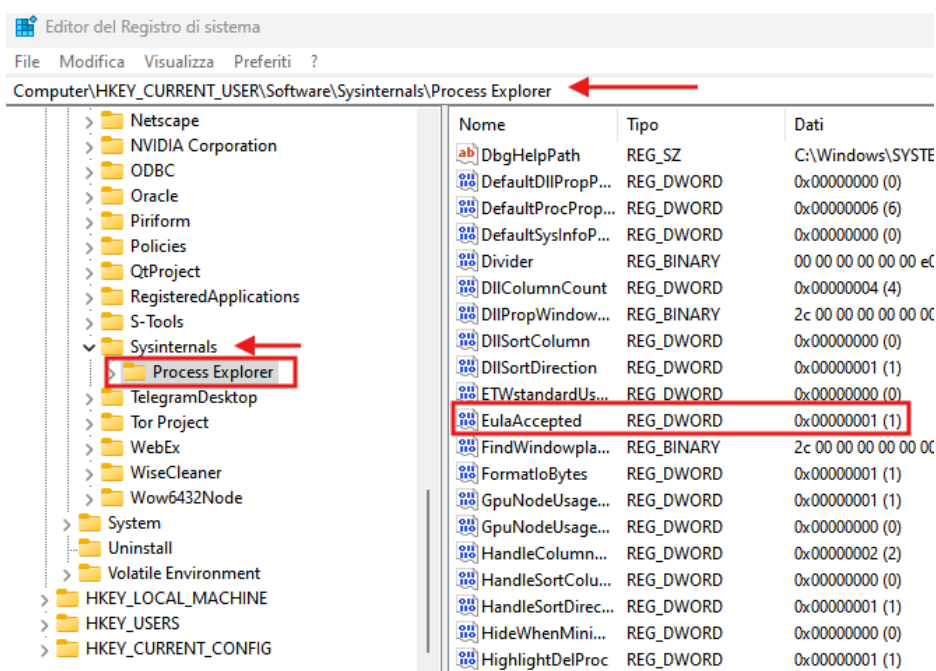
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\KsecDD
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackIt-IT_22621.74.291.0_...
File	\Device\CNG
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM

6. Esplorare il registro di Windows

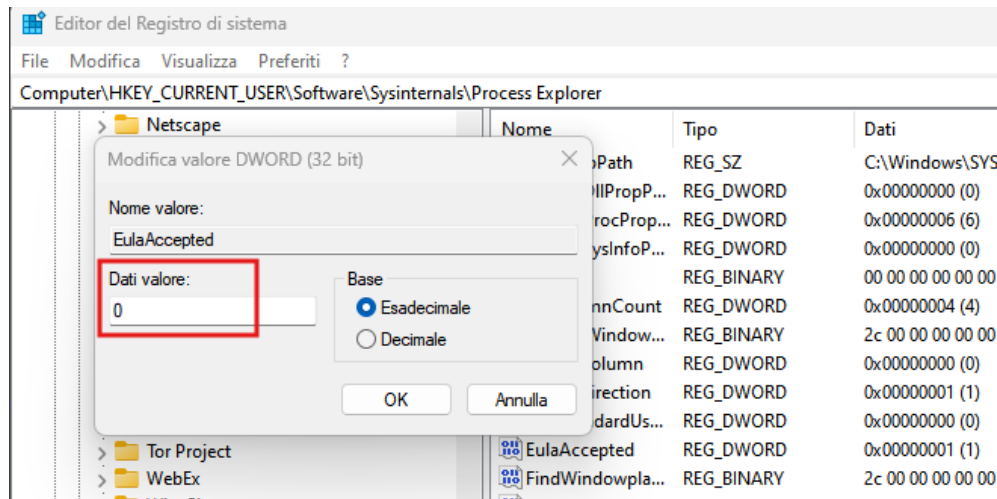
Qui ci viene chiesto di avviare **regedit** dal menu **Start**.



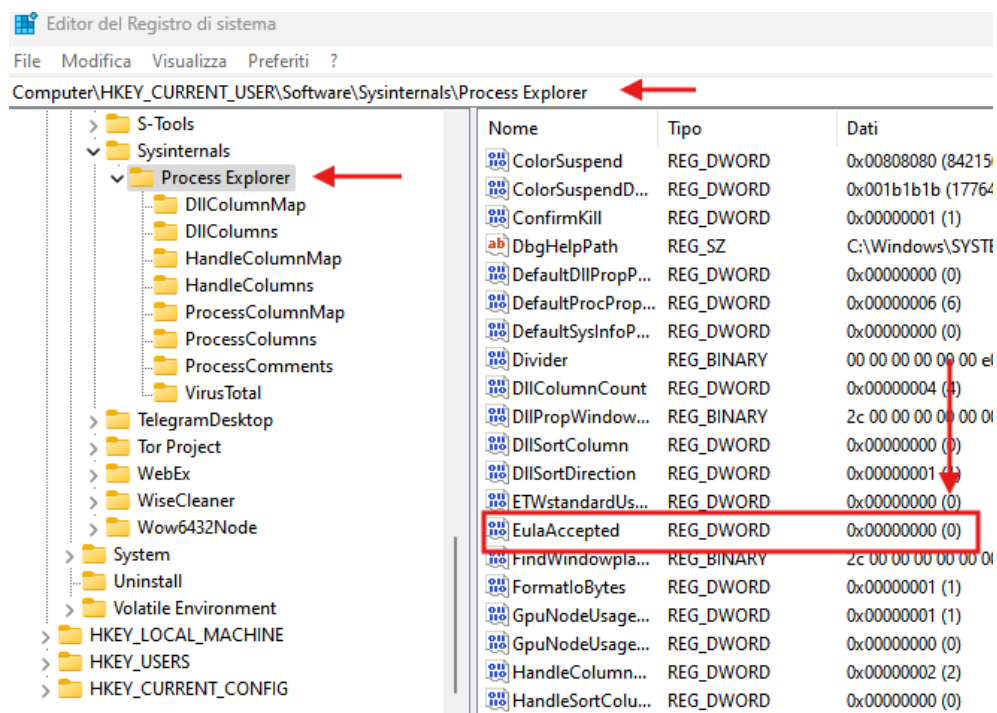
Adesso ci viene chiesto di ricercare all'interno del registro la sottochiave **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer**, relativa a **procexp**.



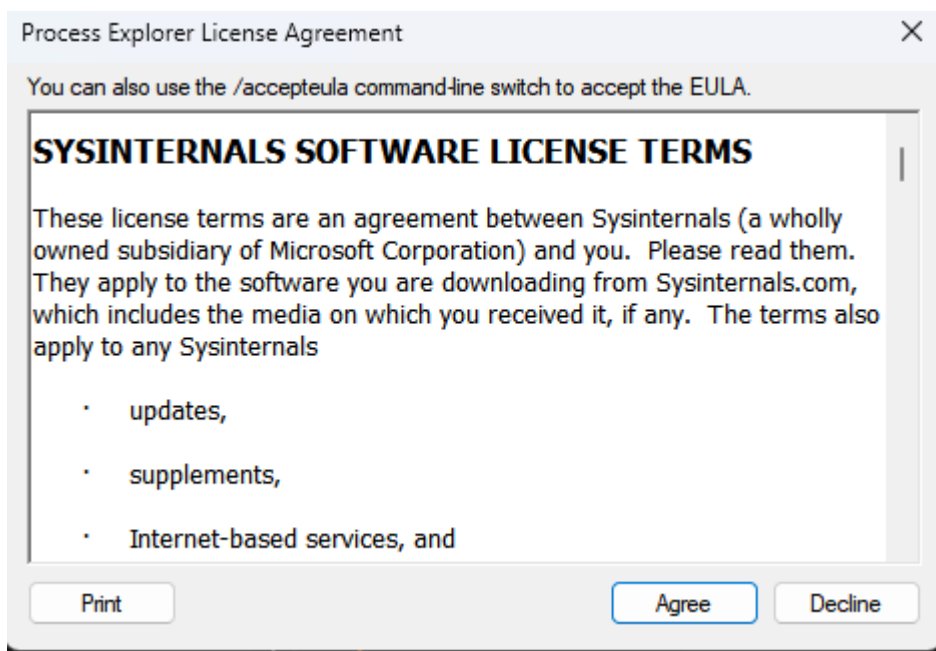
Ci viene poi chiesto di aprire la **entry EulaAccepted** e di settare il valore a **0**, quando invece era già stato settato a **1** nel momento in cui precedentemente avevamo accettato il contratto Eula all'avvio di **procexp**.



Adesso la **entry** del registro **EulaAccepted** avrà come valore **0**.



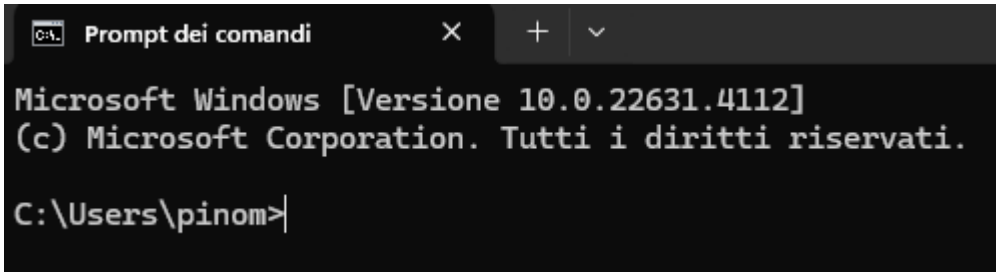
Adesso, infatti, all'avvio di **procexp** ci domanderà nuovamente di accettare il contratto Eula.



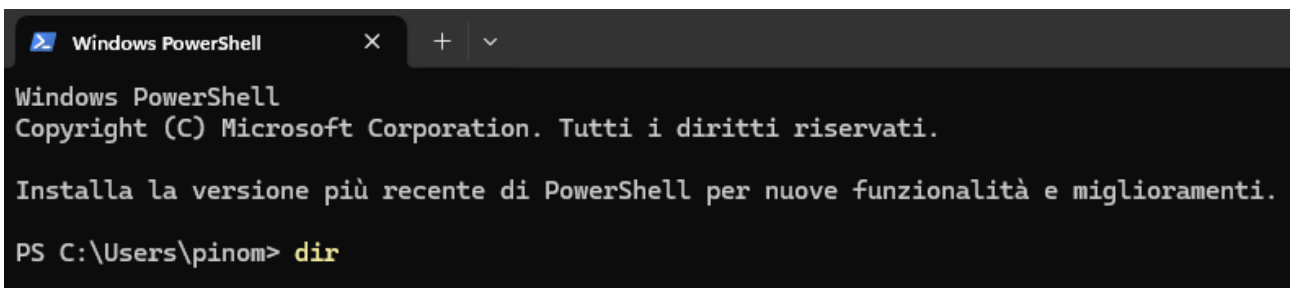
CYBER OPS PRACTICE 2

1. PowerShell

Il primo punto ci chiede di avviare la **PowerShell** e il **prompt dei comandi**.



A screenshot of the Windows Command Prompt window. The title bar reads 'C:\> Prompt dei comandi'. The window content shows the Microsoft Windows version (10.0.22631.4112) and copyright information for Microsoft Corporation. The current directory is C:\Users\pinom, and the prompt is C:\Users\pinom>.

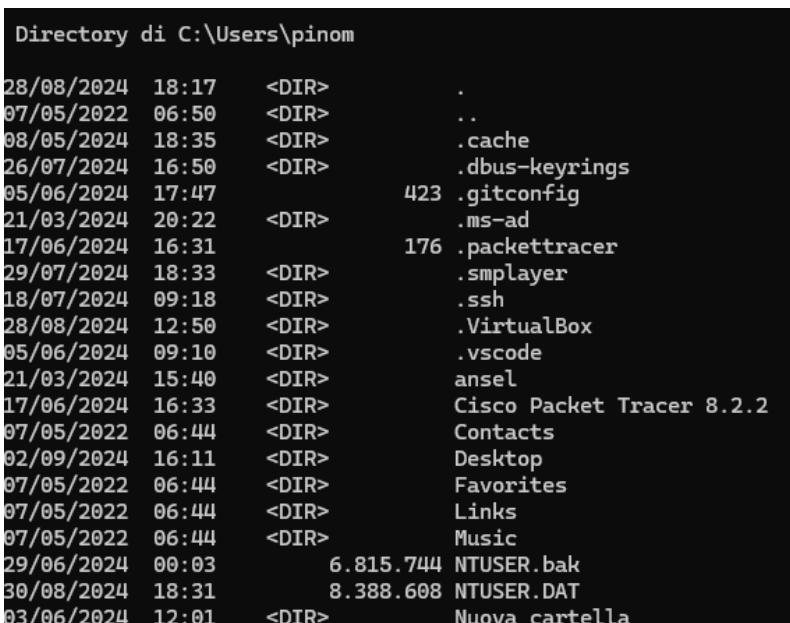


A screenshot of the Windows PowerShell window. The title bar reads 'Windows PowerShell'. The window content shows the Windows PowerShell version and copyright information for Microsoft Corporation. It also includes a message about installing the latest version of PowerShell. The current directory is C:\Users\pinom, and the prompt is PS C:\Users\pinom> dir.

2. Comandi della PowerShell e del Command Prompt

Qui ci viene chiesto di usare il comando **dir** per visualizzare le cartelle del percorso corrente. Ci fa notare che la differenza tra i due tipi di shell è che nella **PowerShell** vengono mostrati gli attributi dei file e delle cartelle, nella colonna prima di quella dedicata alla data di ultima modifica dei file.

COMMAND PROMPT



A screenshot of the Windows Command Prompt showing the output of the 'dir' command. The title bar reads 'Directory di C:\Users\pinom'. The output is a list of files and directories with their attributes, dates, times, and names.

Attributi	Data	Ora	Nome
<DIR>	28/08/2024	18:17	.
<DIR>	07/05/2022	06:50	..
<DIR>	08/05/2024	18:35	.cache
<DIR>	26/07/2024	16:50	.dbus-keyrings
423	05/06/2024	17:47	.gitconfig
<DIR>	21/03/2024	20:22	.ms-ad
176	17/06/2024	16:31	.packettracer
<DIR>	29/07/2024	18:33	.smplayer
<DIR>	18/07/2024	09:18	.ssh
<DIR>	28/08/2024	12:50	.VirtualBox
<DIR>	05/06/2024	09:10	.vscode
<DIR>	21/03/2024	15:40	ansel
<DIR>	17/06/2024	16:33	Cisco Packet Tracer 8.2.2
<DIR>	07/05/2022	06:44	Contacts
<DIR>	02/09/2024	16:11	Desktop
<DIR>	07/05/2022	06:44	Favorites
<DIR>	07/05/2022	06:44	Links
<DIR>	07/05/2022	06:44	Music
6.815.744	29/06/2024	00:03	NTUSER.bak
8.388.608	30/08/2024	18:31	NTUSER.DAT
<DIR>	03/06/2024	12:01	Nuova cartella

POWERSHELL

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e migra

PS C:\Users\pinom> dir

Directory: C:\Users\pinom

Mode                LastWriteTime         Length Name
----                -
d-----          08/05/2024      18:35             .cache
d-----          26/07/2024      16:50          .dbus-keyrings
d-----          21/03/2024      19:22             .ms-ad
d-----          29/07/2024      18:33          .smplayer
d-----          18/07/2024       09:18             .ssh
d-----          02/09/2024      17:21          .VirtualBox
d-----          05/06/2024       09:10          .vscode
d-----          21/03/2024      14:40          ansel
d-----          17/06/2024      16:33 Cisco Packet Tracer 8.2.2
d-r---          07/05/2022       06:44      Contacts
d-r---          02/09/2024      17:21      Desktop
d-r---          07/05/2022       06:44     Favorites
d-r---          07/05/2022       06:44       Links
d-r---          07/05/2022       06:44       Music
d-----          03/06/2024      12:01     Nuova cartella
dar--l          21/03/2024      19:37      OneDrive
d-r---          07/05/2022       06:44     Saved Games
```

Poi ci fa testare i comandi **ping**, **cd**, **ipconfig**.

PING (Command Prompt)

```
Microsoft Windows [Versione 10.0.22631.4112]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\pinom>ping www.google.it

Esecuzione di Ping www.google.it [216.58.204.227] con 32 byte di dati:
Risposta da 216.58.204.227: byte=32 durata=68ms TTL=31
Risposta da 216.58.204.227: byte=32 durata=60ms TTL=31
```

CD (Command Prompt)

```
C:\Users\pinom>cd Desktop

C:\Users\pinom\Desktop>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 789C-3650

Directory di C:\Users\pinom\Desktop

02/09/2024  16:11    <DIR>          .
28/08/2024  18:17    <DIR>          ..
02/09/2024  16:11      1.242.765  CYBER OPS PRACTICE 1.docx
18/07/2024  16:47    <DIR>          Derp
30/08/2024  18:12    <DIR>          EPICODE VARIE
21/03/2024  17:42           354  Fortnite.url
25/06/2024  19:48    <DIR>          GitRepoEpicode
07/05/2024  09:04      9.141.216  HwiNFO64.exe
22/08/2024  13:13           36  HwiNFO64.INI
27/05/2024  14:42    <DIR>          Metasploitable2-Linux
02/09/2024  14:48      45.576  Screenshot 2024-09-02 144757.png
02/09/2024  15:06      12.180  Screenshot 2024-09-02 150601.png
02/09/2024  15:08       5.292  Screenshot 2024-09-02 150746.png
02/09/2024  15:19       4.690  Screenshot 2024-09-02 151851.png
02/09/2024  15:21      19.445  Screenshot 2024-09-02 152051.png
```

IPCONFIG (Command Prompt)

```
C:\Users\pinom\Desktop>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fd00::8d53:187:9c60:eb76
    Indirizzo IPv6 temporaneo. . . . . : fd00::714c:229e:a97b:ed60
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::5a47:adf1:c61a:bcfa%10
    Indirizzo IPv4. . . . . : 192.168.1.140
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2e91:fbf9:8bc8:f05%6
    Indirizzo IPv4 configurazione automatica : 169.254.84.157
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :
```

PING (PowerShell)

```
PS C:\Users\pinom> ping www.google.it

Esecuzione di Ping www.google.it [216.58.204.227] con 32 byte di dati:
Risposta da 216.58.204.227: byte=32 durata=56ms TTL=31
Risposta da 216.58.204.227: byte=32 durata=61ms TTL=31
Risposta da 216.58.204.227: byte=32 durata=59ms TTL=31
Risposta da 216.58.204.227: byte=32 durata=68ms TTL=31

Statistiche Ping per 216.58.204.227:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 56ms, Massimo = 68ms, Medio = 61ms
PS C:\Users\pinom> |
```

CD (PowerShell)

```
PS C:\Users\pinom> cd Desktop
PS C:\Users\pinom\Desktop> ls

Directory: C:\Users\pinom\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----            18/07/2024         16:47      Derp
d-----            30/08/2024         18:12      EPICODE VARIE
d-----            25/06/2024         19:48      GitRepoEpicode
d-----            27/05/2024         14:42      Metasploitable2-Linux
d-----            02/09/2024         17:25      ops
-a-----            02/09/2024         17:28      1466635 CYBER OPS PRACTICE 1.docx
-a-----            21/03/2024          16:42          354 Fortnite.url
-a-----            07/05/2024         09:04      9141216 HwINFO64.exe
-a-----            22/08/2024         13:13          36 HwINFO64.INI
```

IPCONFIG (PowerShell)

```
PS C:\Users\pinom\Desktop> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fd00::8d53:187:9c60:eb76
    Indirizzo IPv6 temporaneo. . . . . : fd00::714c:229e:a97b:ed60
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::5a47:adf1:c61a:bcfa%10
    Indirizzo IPv4. . . . . : 192.168.1.140
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::2e91:fbf9:8bc8:f05%6
    Indirizzo IPv4 configurazione automatica : 169.254.84.157
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :
```

3. Cmdlets

In questo passaggio ci fa inserire il **cmdlet** “**Get-Alias dir**” sulla **PowerShell**.

```
PS C:\Users\pinom\Desktop> Get-Alias dir
```

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

In output, ci darà il comando equivalente a **dir** sulla **PowerShell**, ovvero il **cmdlet** “**Get-ChildItem**”.

Per una visione completa dei **cmdlets** ci consiglia di ricercare online.

The screenshot shows the Microsoft Learn website's PowerShell section. The main heading is "Cmdlet Overview", dated 09/18/2021, with 1 contributor. A sidebar on the left lists various PowerShell topics, with "Cmdlet Overview" selected. The main content area explains that a cmdlet is a lightweight command used in the PowerShell environment, invoked by the runtime within automation scripts or programmatically through APIs. It also provides a list of related articles: "Cmdlets", "Cmdlet Terms", "How Cmdlets Differ from Commands", and "Cmdlet Base Classes".

Learn / PowerShell /

Cmdlet Overview

Article • 09/18/2021 • 1 contributor

[Feedback](#)

In this article

- [Cmdlets](#)
- [Cmdlet Terms](#)
- [How Cmdlets Differ from Commands](#)
- [Cmdlet Base Classes](#)

[Show 4 more](#)

A cmdlet is a lightweight command that is used in the PowerShell environment. The PowerShell runtime invokes these cmdlets within the context of automation scripts that are provided at the command line. The PowerShell runtime also invokes them programmatically through PowerShell APIs.

Cmdlets

Cmdlets perform an action and typically return a Microsoft .NET object to the next command in the pipeline. A cmdlet is a single command that participates in the pipeline semantics of PowerShell.

4. Netstat

Qui ci chiede di aprire la **PowerShell** e digitare il comando **netstat -h**.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\pinom> netstat -h

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

NETSTAT[-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Visualizza tutte le connessioni e le porte di ascolto.
-b          Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o
            porta di ascolto. Alcuni file eseguibili conosciuti includono
            più componenti indipendenti. In tali casi
            viene visualizzata la sequenza dei componenti utilizzati per la creazione della connessione
            o porta di ascolto e il
            nome del file eseguibile viene visualizzato in fondo, tra parentesi quadre ([]). Nella parte superiore è
            indicato il componente chiamato
            e così via, fino al raggiungimento di TCP/IP. Se si utilizza questa opzione,
            l'esecuzione del comando può richiedere molto tempo e riuscirà solo se si dispone di autorizzazioni
            sufficienti.
-e          Visualizza le statistiche Ethernet. Può essere utilizzata insieme all'opzione -s.
-f          Visualizza i nomi di dominio completi (FQDN, Fully Qualified Domain Name) per gli indirizzi
            esterni.
-i          Visualizza il tempo trascorso da una connessione TCP nel suo stato corrente.
-n          Visualizza indirizzi e numeri di porta in forma numerica.
-o          Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto    Visualizza le connessioni relative al protocollo specificato da "proto",
```

Poi ci fa testare il comando **netstat -r** per visionare la tabella di routing per conoscere il gateway IPv4.

```
Windows PowerShell

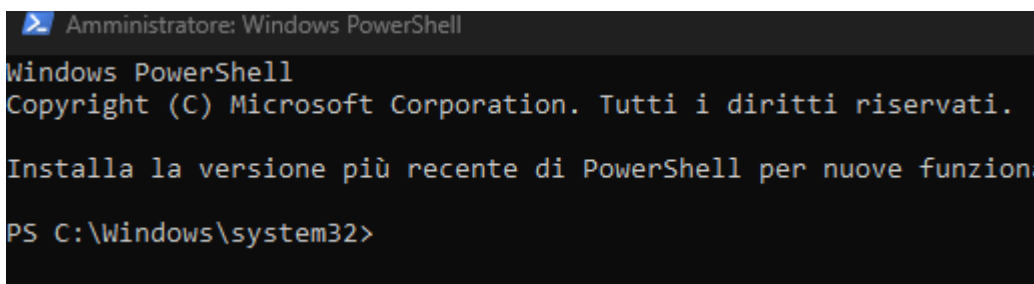
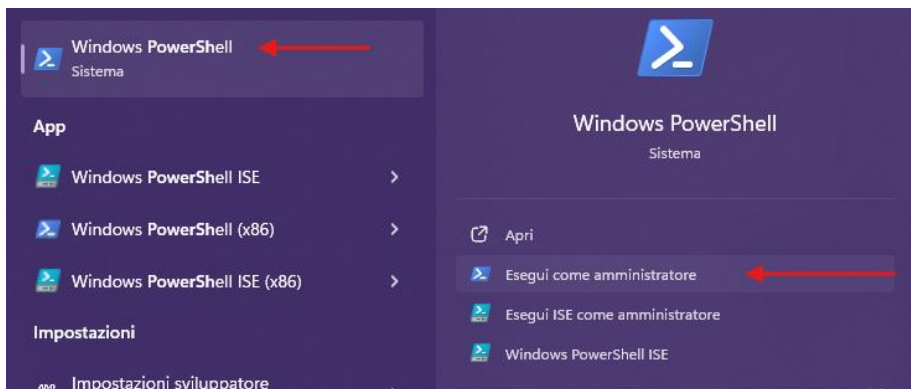
PS C:\Users\pinom> netstat -r

=====
Elenco interfacce
10...70 85 c2 94 59 7c .....Realtek Gaming 2.5GbE Family Controller
6...0a 00 27 00 00 06 .....VirtualBox Host-Only Ethernet Adapter
1.....Software Loopback Interface 1
=====

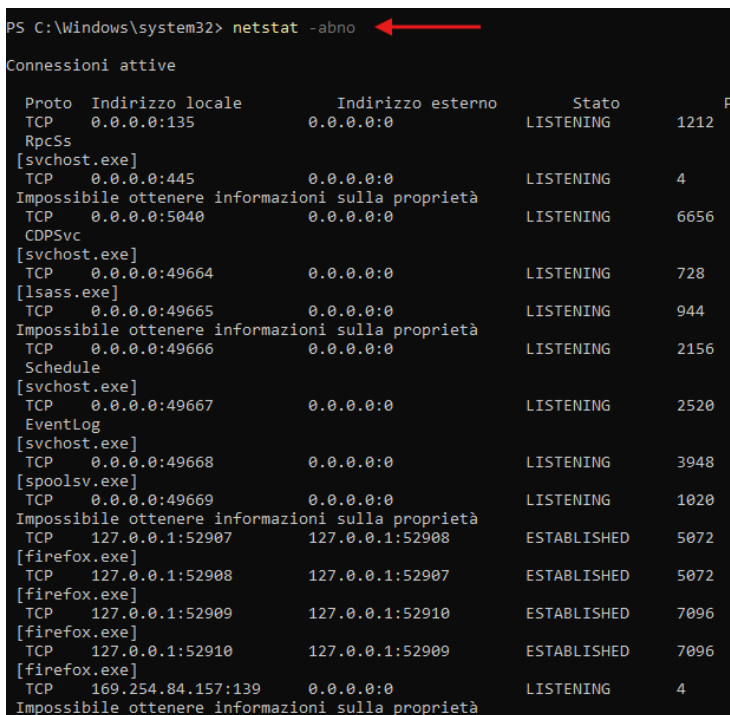
IPv4 Tabella route
=====
Route attive:
=====
Indirizzo rete      Mask      Gateway      Interfaccia Metrica
-----
0.0.0.0             0.0.0.0   192.168.1.1  192.168.1.140  25
127.0.0.0           255.0.0.0 On-link      127.0.0.1      331
127.0.0.1           255.255.255.255 On-link      127.0.0.1      331
127.255.255.255     255.255.255.255 On-link      127.0.0.1      331
169.254.0.0         255.255.0.0 On-link      169.254.84.157 281
169.254.84.157      255.255.255.255 On-link      169.254.84.157 281
169.254.255.255     255.255.255.255 On-link      169.254.84.157 281
192.168.1.0         255.255.255.0 On-link      192.168.1.140 281
192.168.1.140       255.255.255.255 On-link      192.168.1.140 281
192.168.1.255       255.255.255.255 On-link      192.168.1.140 281
224.0.0.0           240.0.0.0 On-link      127.0.0.1      331
224.0.0.0           240.0.0.0 On-link      169.254.84.157 281
224.0.0.0           240.0.0.0 On-link      192.168.1.140 281
255.255.255.255     255.255.255.255 On-link      127.0.0.1      331
255.255.255.255     255.255.255.255 On-link      169.254.84.157 281
255.255.255.255     255.255.255.255 On-link      192.168.1.140 281
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
=====
Interf Metrica Rete Destinazione Gateway
-----
1 331 ::1/128 On-link
10 281 fd00::/64 On-link
10 281 fd00::/64 fe80::5e49:79ff:fe76:3fba
10 281 fd00::714c:229e:a97b:ed60/128 On-link
10 281 fd00::8d53:187:9c60:eb76/128 On-link
6 281 fe80::/64 On-link
10 281 fe80::/64 On-link
6 281 fe80::2e91:fbf9:8bc8:f05/128 On-link
10 281 fe80::5a47:adf1:c61a:bcfa/128 On-link
1 331 ff00::/8 On-link
6 281 ff00::/8 On-link
10 281 ff00::/8 On-link
=====
Route permanenti:
```

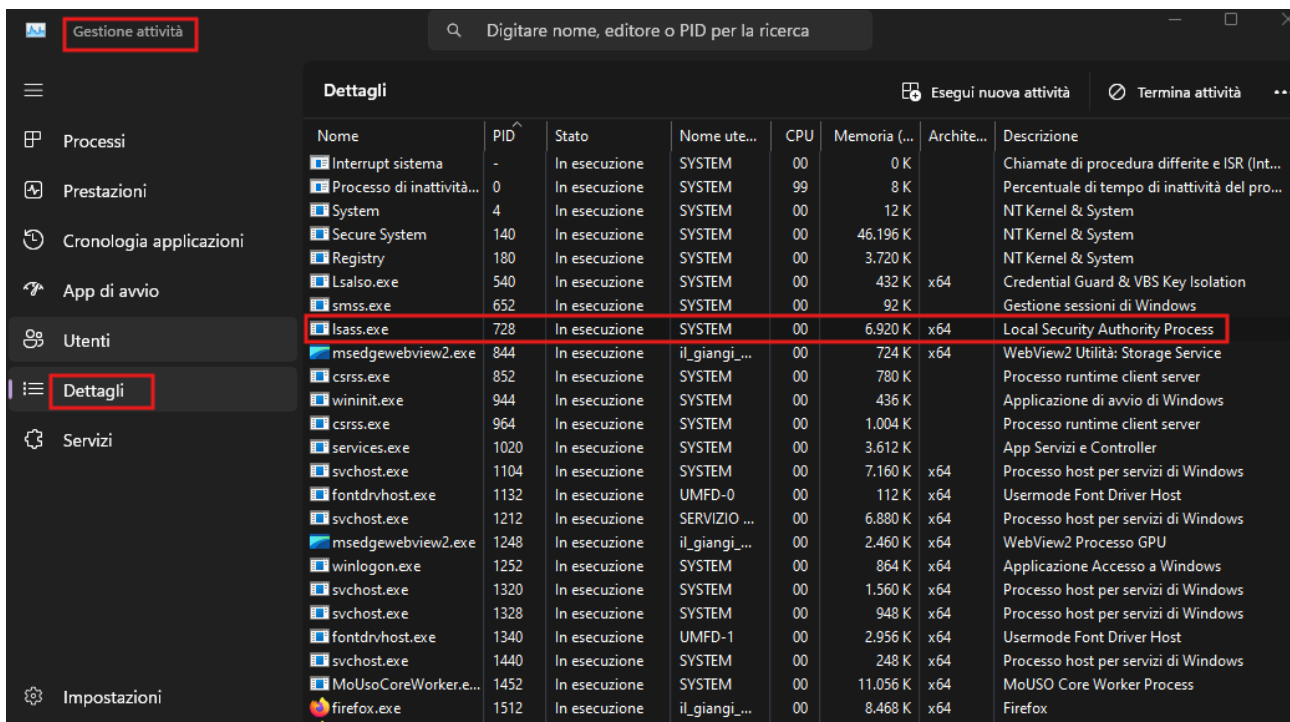
Successivamente ci fa avviare la **PowerShell** coi diritti da amministratore.



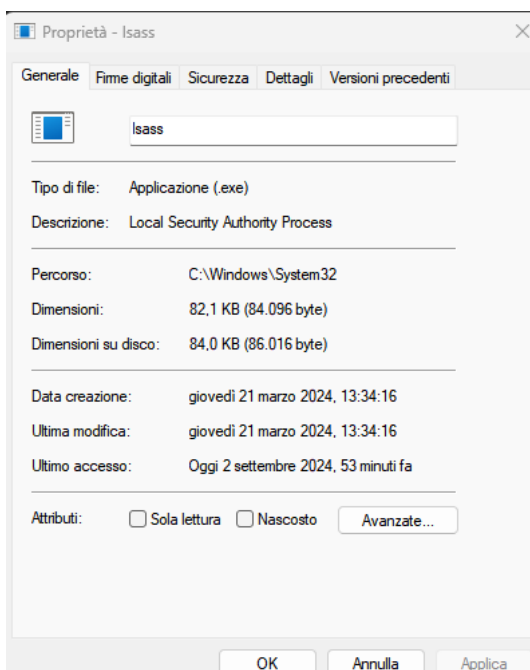
Adesso ci fa immettere il comando **netstat -abno**. Esso ci mostra tutti i processi che hanno connessioni TCP attive.



Poi ci chiede di aprire il pannello **Dettagli** in **Gestione Attività** e di selezionare, tramite identificativo **PID** uno dei processi che appaiono nell'output del comando **netstat** dentro la **PowerShell**. Abbiamo scelto il **PID 728**, associato a **lsass.exe**.



Ci fa poi aprire la scheda **Proprietà** cliccando col tasto destro sul nome del processo.



5. Svuotamento Cestino con PowerShell

Tramite comando **clear-recyclebin** si può svuotare il cestino da riga di comando.

```
PS C:\Users\pinom> clear-recyclebin  
  
Conferma  
Eseguire l'operazione?  
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".  
[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S  
PS C:\Users\pinom>
```

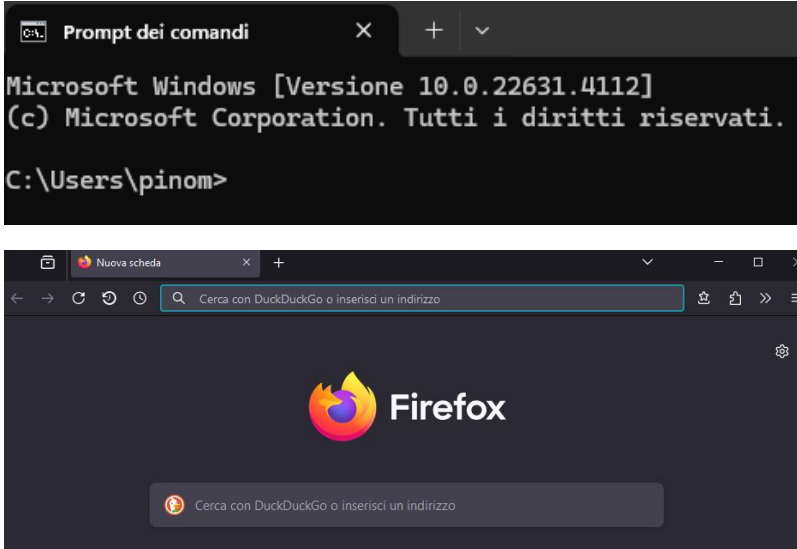
6. Cmdlets utili per la sicurezza

- **Get-Service**: mostra tutti i servizi sul computer
- **Start-Service**: avvia un servizio
- **Stop-Service**: ferma un servizio
- **Restart-Service**: riavvia un servizio
- **Test-Connection**: invia delle echo request ad un host target per verificare la connessione
- **Get-NetIPAddress**: recupera la configurazione IP
- **Get-NetAdapter**: fa una lista degli adattatori di rete
- **Resolve-DnsName**: ricava l'IP da un nome di dominio
- **Get-Process**: mostra i processi in esecuzione.
- **Start-Process**: avvia un processo.
- **Stop-Process**: ferma un processo.
- **Wait-Process**: attende che un processo finisca l'esecuzione.

CYBER OPS PRACTICE 3

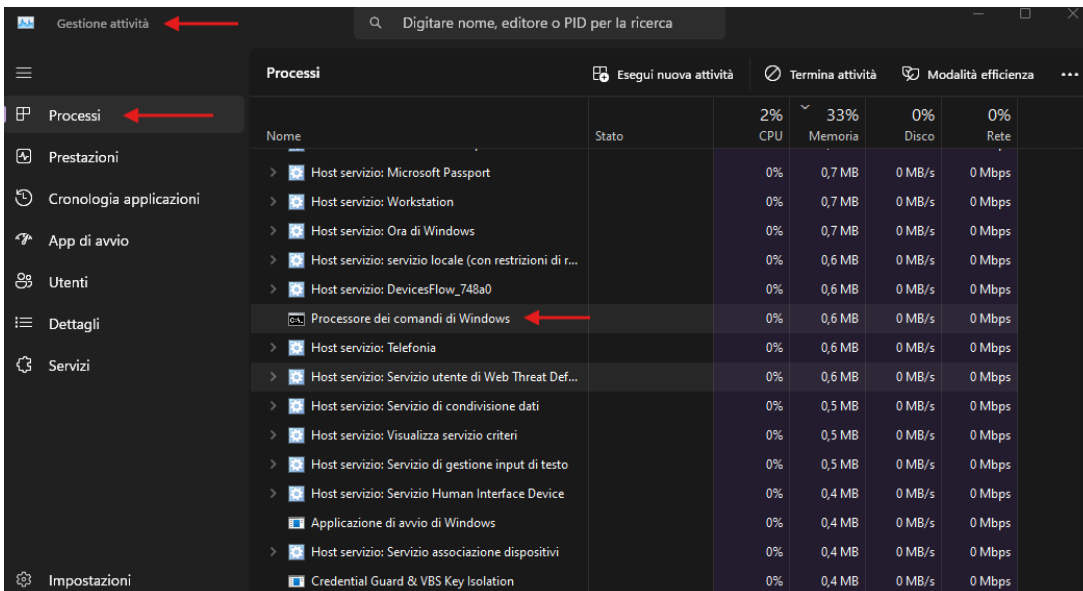
1. Tab Processi

Prima di tutto ci chiede di avviare un prompt dei comandi e un browser.

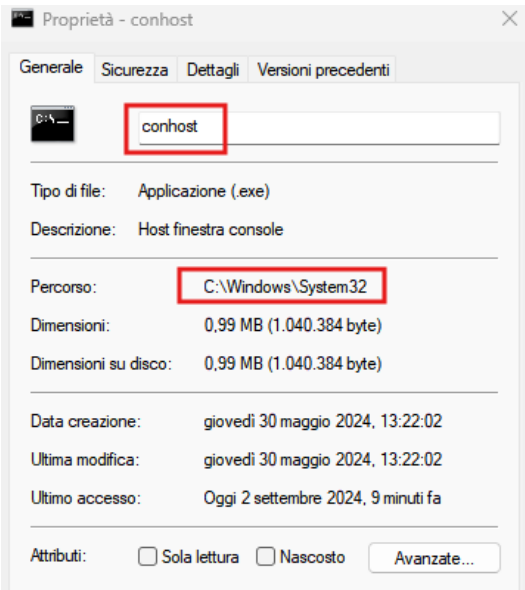


Poi ci chiede di cliccare sulla voce **Processore di Comandi Di Windows** nella schermata **Processi** di **Gestione Attività** di Windows e verificare che sotto compaia il processo del **Prompt dei Comandi**.

In questo caso non appare nulla.



Successivamente chiede di cercare il processo **Console Windows Host** e di selezionare **Proprietà** facendo click destro su di esso. Vediamo che il percorso dell'eseguibile si trova in **C:\Windows\System32**.



Dopo aver chiuso il **Prompt**, i processi che abbiamo appena cercato scompaiono.

Cliccando sul tab **Memoria**, i processi vengono ordinati in ordine di utilizzo memoria crescente o decrescente.

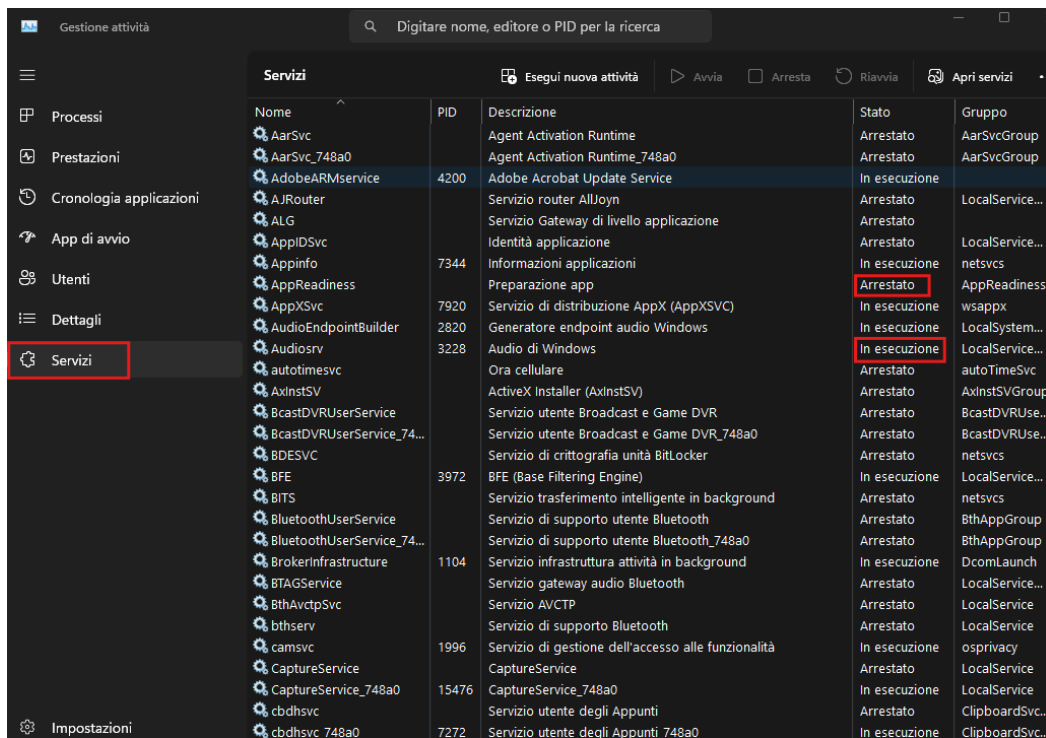
Nome	Stato	2% CPU	33% Memoria	0% Disco	0% Rete
Impostazioni		0%	0 MB	0 MB/s	0 Mbps
Interrupt sistema		0%	0 MB	0 MB/s	0 Mbps
System		0%	0,1 MB	0,1 MB/s	0 Mbps
Acrobat Update Service (32 bit)		0%	0,1 MB	0 MB/s	0 Mbps
Gestione sessioni di Windows		0%	0,1 MB	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	0,1 MB	0 MB/s	0 Mbps
Host servizio: Manutenzione collegamenti distri...		0%	0,2 MB	0 MB/s	0 Mbps

Si può anche impostare la percentuale di memoria facendo click destro sul tab **Memoria**.

Nome	Stato	3% CPU	33% Memoria	1% Disco	0% Rete
Impostazioni		0%	0%	0 MB/s	0 Mbps
Interrupt sistema		0%	0%	0 MB/s	0 Mbps
System		0%	0,1%	0,6 MB/s	0 Mbps
Acrobat Update Service (32 bit)		0%	0,1%	0 MB/s	0 Mbps
Gestione sessioni di Windows		0%	0,1%	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	0,1%	0 MB/s	0 Mbps
Host servizio: Manutenzione collegamenti distri...		0%	0,1%	0 MB/s	0 Mbps

2. Tab dei Servizi

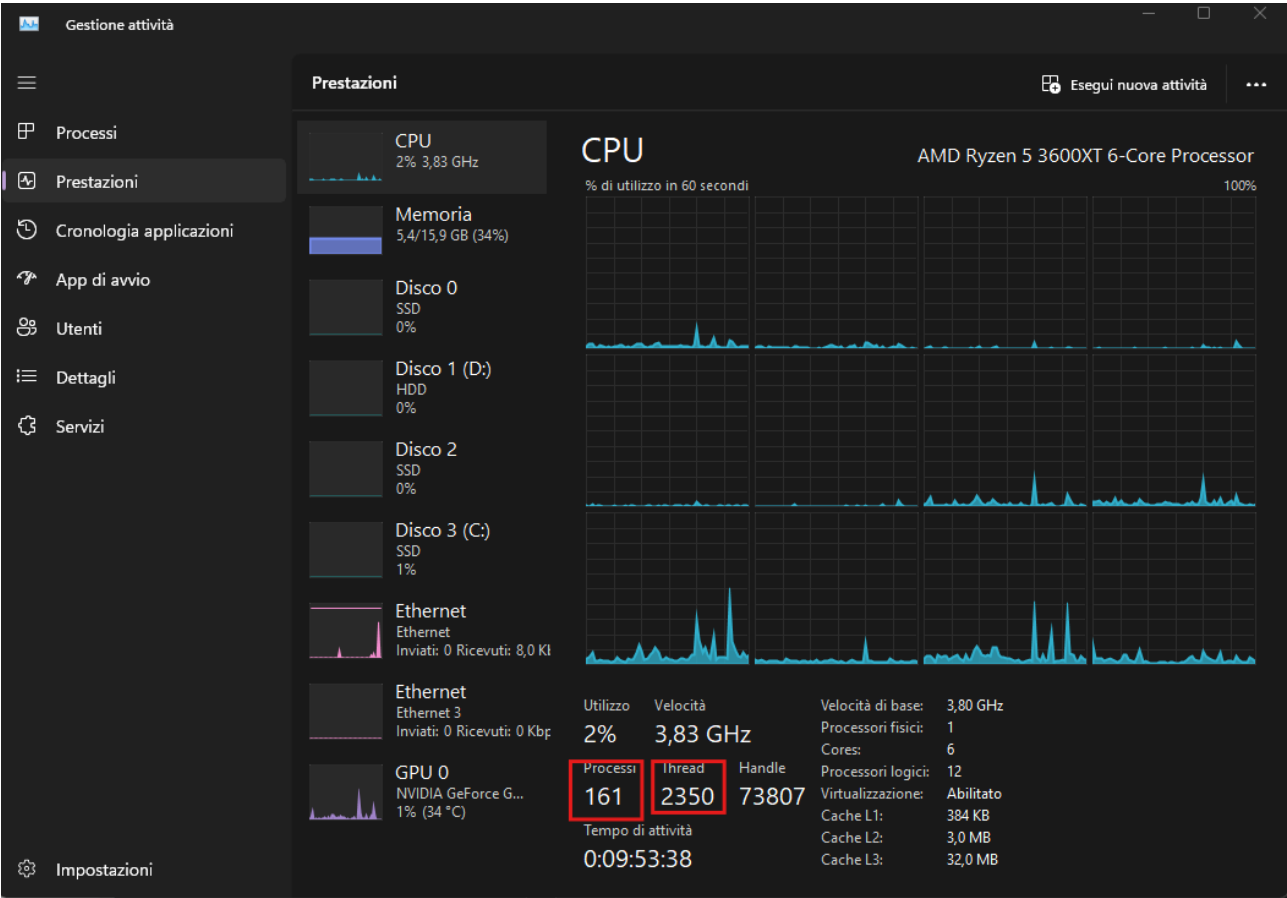
I vari servizi ed il loro stato di esecuzione.

The image is a screenshot of the Windows Task Manager application, specifically the 'Servizi' (Services) tab. The interface is in dark mode. On the left, there is a navigation pane with icons and labels for 'Processi', 'Prestazioni', 'Cronologia applicazioni', 'App di avvio', 'Utenti', 'Dettagli', and 'Servizi'. The 'Servizi' tab is selected and highlighted with a red rectangle. The main area displays a table of system services. The table has columns for 'Nome' (Name), 'PID', 'Descrizione' (Description), 'Stato' (Status), and 'Gruppo' (Group). The 'Stato' column contains values like 'Arrestato' (Stopped), 'In esecuzione' (Running), and 'Arrestato'. Several status entries are highlighted with red rectangles: 'Arrestato' for 'AppReadiness', 'In esecuzione' for 'AdobeARMService', 'Arrestato' for 'AppReadiness', 'In esecuzione' for 'AppXSvc', 'In esecuzione' for 'AudioEndpointBuilder', and 'In esecuzione' for 'AudioSrv'. The table lists various services such as 'AarSvc', 'AarSvc_748a0', 'AdobeARMService', 'AJRouter', 'ALG', 'AppIDSvc', 'Appinfo', 'AppReadiness', 'AppXSvc', 'AudioEndpointBuilder', 'AudioSrv', 'autotimesvc', 'AxinstSV', 'BcastDVRUserService', 'BcastDVRUserService_74...', 'BDESVC', 'BFE', 'BITS', 'BluetoothUserService', 'BluetoothUserService_74...', 'BrokerInfrastructure', 'BTAGService', 'BthAvctpSvc', 'bthserv', 'camsvc', 'CaptureService', 'CaptureService_748a0', 'cbdhsvc', and 'cbdhsvc_748a0'.

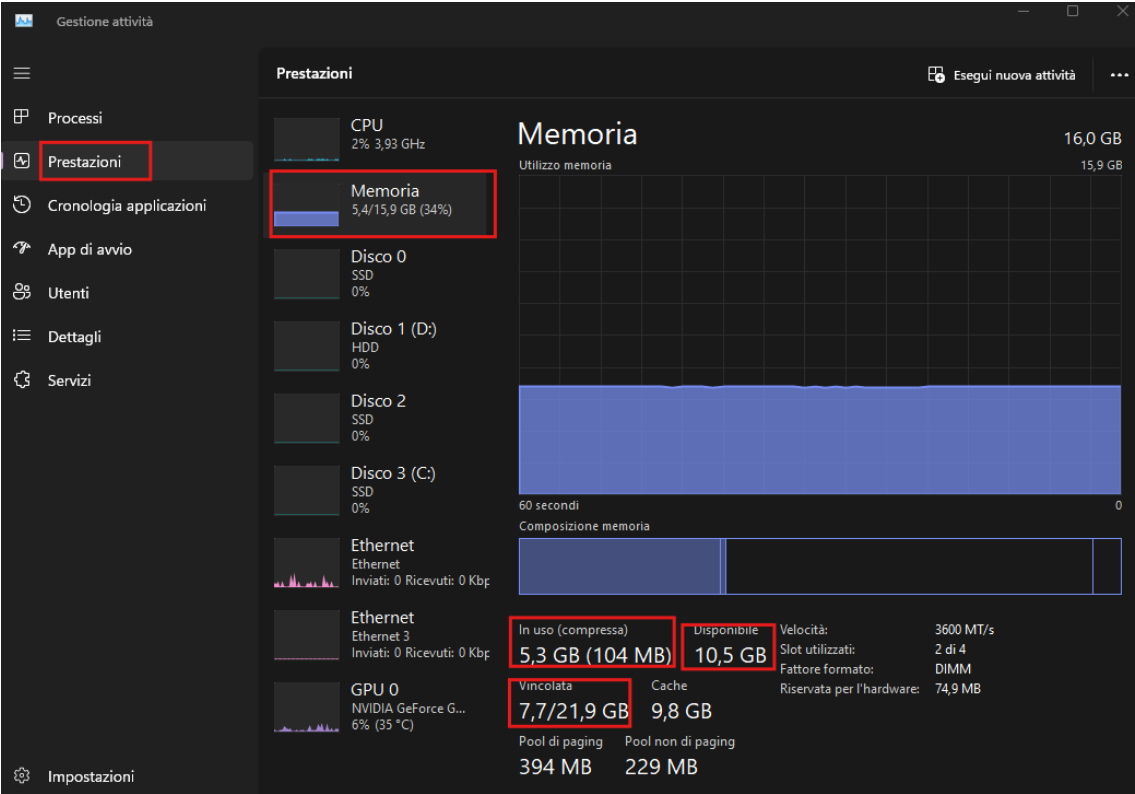
Nome	PID	Descrizione	Stato	Gruppo
AarSvc		Agent Activation Runtime	Arrestato	AarSvcGroup
AarSvc_748a0		Agent Activation Runtime_748a0	Arrestato	AarSvcGroup
AdobeARMService	4200	Adobe Acrobat Update Service	In esecuzione	
AJRouter		Servizio router AllJoyn	Arrestato	LocalService...
ALG		Servizio Gateway di livello applicazione	Arrestato	
AppIDSvc		Identità applicazione	Arrestato	LocalService...
Appinfo	7344	Informazioni applicazioni	In esecuzione	netsvcs
AppReadiness		Preparazione app	Arrestato	AppReadiness
AppXSvc	7920	Servizio di distribuzione AppX (AppXSVC)	In esecuzione	wsappx
AudioEndpointBuilder	2820	Generatore endpoint audio Windows	In esecuzione	LocalSystem...
AudioSrv	3228	Audio di Windows	In esecuzione	LocalService...
autotimesvc		Ora cellulare	Arrestato	autoTimeSvc
AxinstSV		ActiveX Installer (AxinstSV)	Arrestato	AxinstSVGroup
BcastDVRUserService		Servizio utente Broadcast e Game DVR	Arrestato	BcastDVRUse...
BcastDVRUserService_74...		Servizio utente Broadcast e Game DVR_748a0	Arrestato	BcastDVRUse...
BDESVC		Servizio di crittografia unità BitLocker	Arrestato	netsvcs
BFE	3972	BFE (Base Filtering Engine)	In esecuzione	LocalService...
BITS		Servizio trasferimento intelligente in background	Arrestato	netsvcs
BluetoothUserService		Servizio di supporto utente Bluetooth	Arrestato	BthAppGroup
BluetoothUserService_74...		Servizio di supporto utente Bluetooth_748a0	Arrestato	BthAppGroup
BrokerInfrastructure	1104	Servizio infrastruttura attività in background	In esecuzione	DcomLaunch
BTAGService		Servizio gateway audio Bluetooth	Arrestato	LocalService...
BthAvctpSvc		Servizio AVCTP	Arrestato	LocalService
bthserv		Servizio di supporto Bluetooth	Arrestato	LocalService
camsvc	1996	Servizio di gestione dell'accesso alle funzionalità	In esecuzione	osprivacy
CaptureService		CaptureService	Arrestato	LocalService
CaptureService_748a0	15476	CaptureService_748a0	In esecuzione	LocalService
cbdhsvc		Servizio utente degli Appunti	Arrestato	ClipboardSvc...
cbdhsvc_748a0	7272	Servizio utente degli Appunti 748a0	In esecuzione	ClipboardSvc...

3. Tab delle Performance

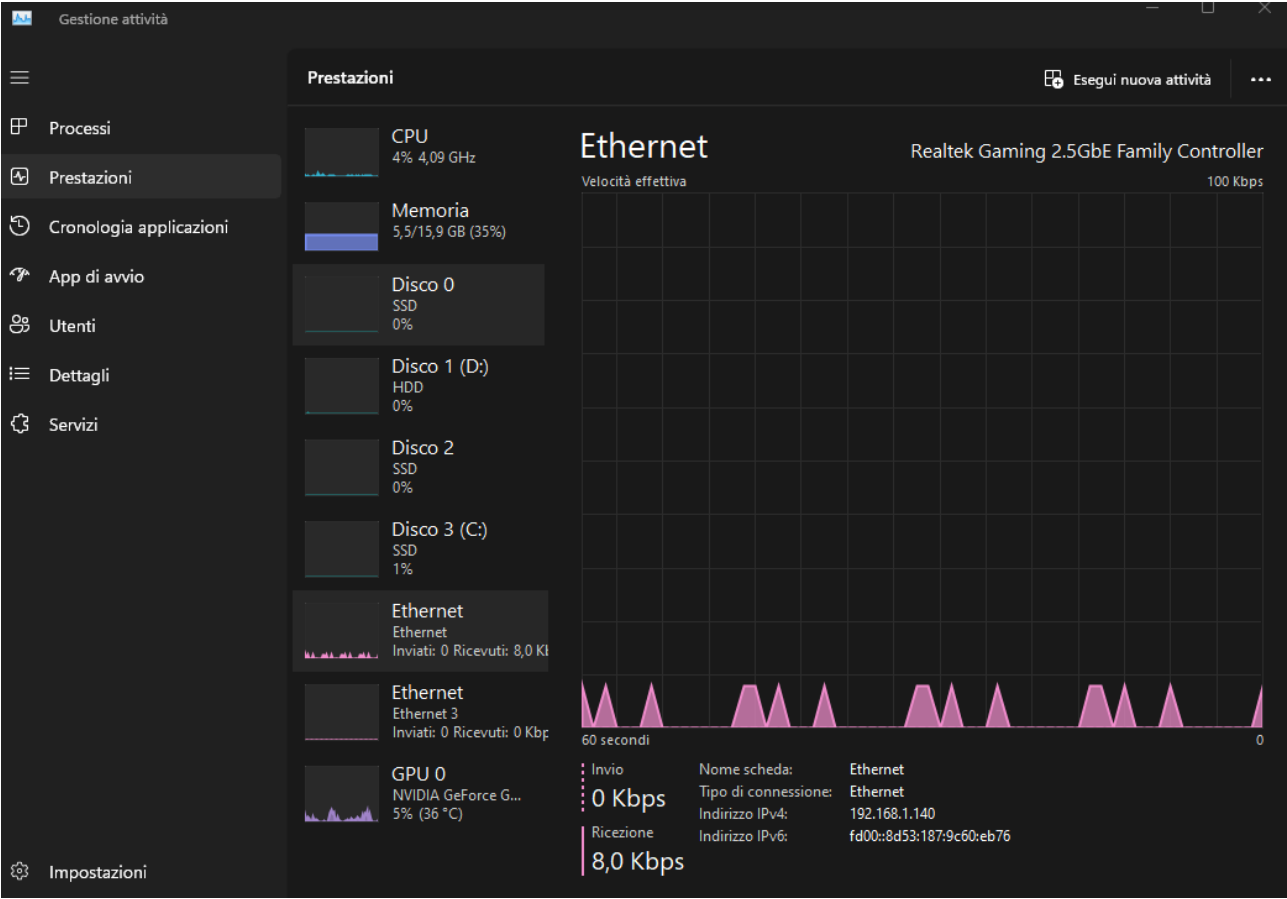
Verifica dei Threads e Processi attivi.



Tab della memoria.



Tab di rete.



Monitoraggio Risorse.

