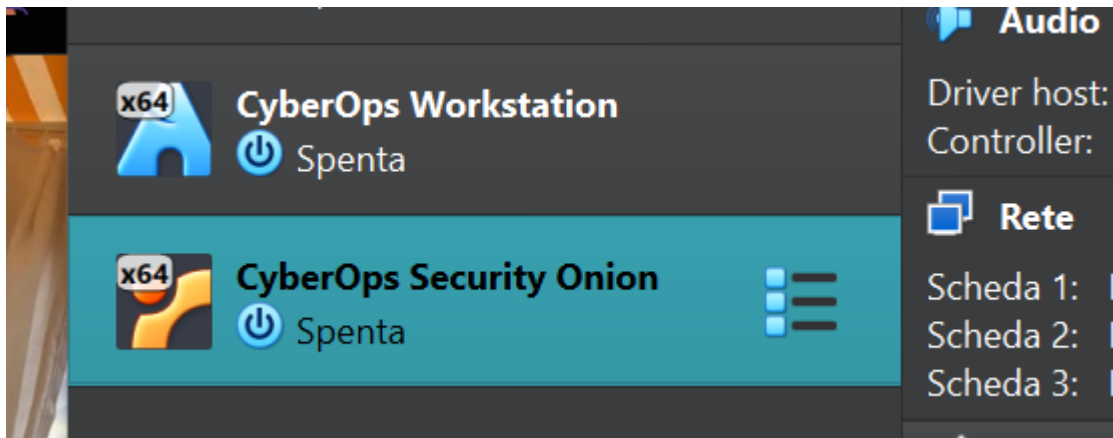


## Esercizio S11L2 - CyberOps Workstation, Onion, ProcExp64.exe & RegEdit

Prova di installazione CyberOps Workstation e Onion:



Esercizi su procepx64.exe:

Individuazione con drag & drop di servizi all'interno di procepx

Process Name	Private Bytes	Working Set	Private Bytes	Working Set	Process Name	Process Name
Discord.exe	< 0.01	105.948 K	140.920 K	4512	Discord	Discord Inc.
Discord.exe	< 0.01	11.192 K	32.956 K	19700	Discord	Discord Inc.
Discord.exe	< 0.01	393.588 K	180.284 K	9916	Discord	Discord Inc.
Discord.exe		16.508 K	53.604 K	7132	Discord	Discord Inc.
Discord.exe	0.13	332.656 K	354.424 K	31516	Discord	Discord Inc.
Discord.exe		12.608 K	81.448 K	21512	Discord	Discord Inc.
chrome.exe	0.09	168.640 K	318.596 K	14808	Google Chrome	Google LLC
chrome.exe		6.020 K	0.741 K	18880	Google Chrome	Google LLC

Dimostrazione di kill process da comando



Esplorazione di creazione di nuovi sottoprocessi in tempo reale attraverso un ping da cmd.exe:

```
C:\Users\uomos>ping 192.168.1.250

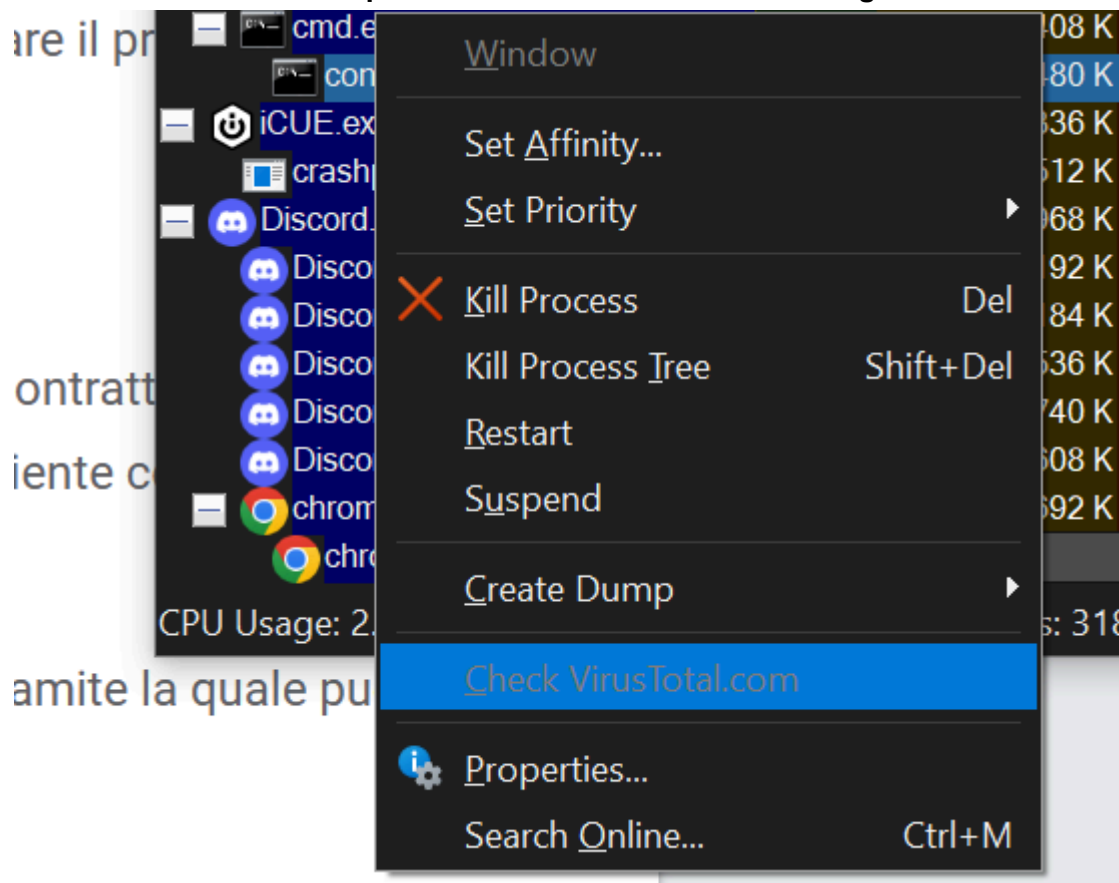
Esecuzione di Ping 192.168.1.250 con 32 byte di dati:
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.
Risposta da 192.168.1.196: Host di destinazione non raggiungibile.

Statistiche Ping per 192.168.1.250:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
```

Visibilità di PING.EXE che rappresenta il ping comandato:

cmd.exe	3.348 K	5.204 K	1708 Processore dei comandi di Wi...	Microsoft Corporation
conhost.exe	< 0.01	7.556 K	20.088 K	11716 Host finestra console
PING.EXE	904 K	4.500 K	29708 Comando Ping TCP/IP	Microsoft Corporation

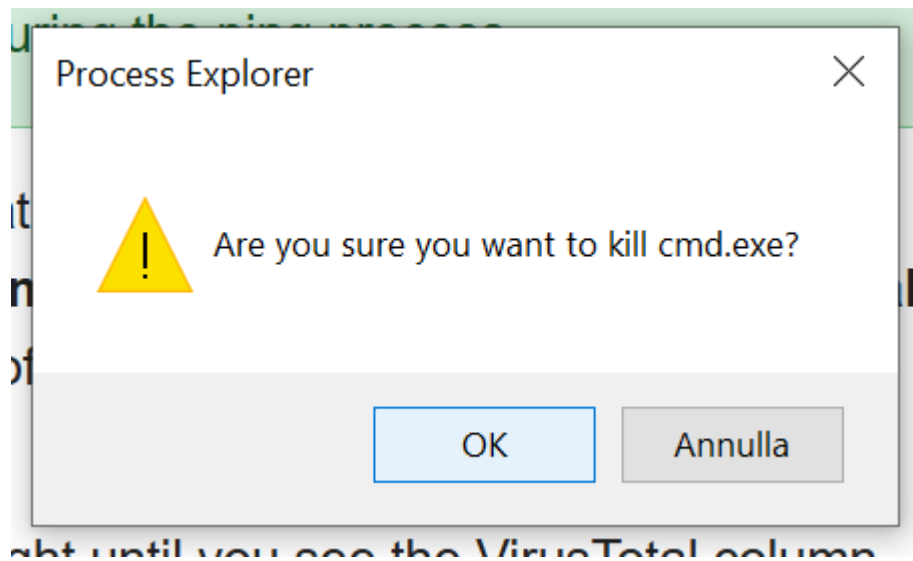
Check da VirusTotal.com per sicurezza e vulnerabilità dei singoli servizi:



Risultato su conhost.exe, 0/76:

cmd.exe	2.380 K	5.204 K	1708 Processore dei comandi di Wi...	Microsoft Corporation
conhost.exe	7.480 K	20.100 K	11716 Host finestra console	Microsoft Corporation
PING.EXE	904 K	4.500 K	29708 Comando Ping TCP/IP	Microsoft Corporation

**Kill di processo cmd.exe per dimostrazione di chiusura anche dei sottoprocessi uccidendo il processo madre:**



**Visibilità dei Threads da procexp64.exe esplorando le proprietà del processo:**

conhost.exe:28908 Properties

TCP/IP

Security

Environment

Strings

Image

Performance

Performance Graph

GPU Graph

Threads

Count: 8

TID	CPU	Cycles Delta	Suspend Count	Start Address
21052				conhost.exe+0x10ed0
13444				ntdll.dll!TpReleaseCleanupGr...
6844				ntdll.dll!TpReleaseCleanupGr...
18504				ntdll.dll!TpReleaseCleanupGr...
4752				ntdll.dll!TpReleaseCleanupGr...
30604				ntdll.dll!TpReleaseCleanupGr...
5788				conhost.exe+0x1b760
3012				conhost.exe+0x2f00

Thread ID: 5788

Stack

Module

Start Time: 15:41:06 10/12/2024

State: Wait:UserRequest

Base Priority: 8

Kernel Time: 0:00:00.000

Dynamic Priority: 8

User Time: 0:00:00.000

I/O Priority: Normal

Context Switches: 40

Memory Priority: 5

Cycles: 18.553.528

Ideal Processor: 7

Permissions

Kill

Suspend

OK

Cancel

**Visibilità delle handles; chiavi di registro e i threads visualizzati poco fa:**

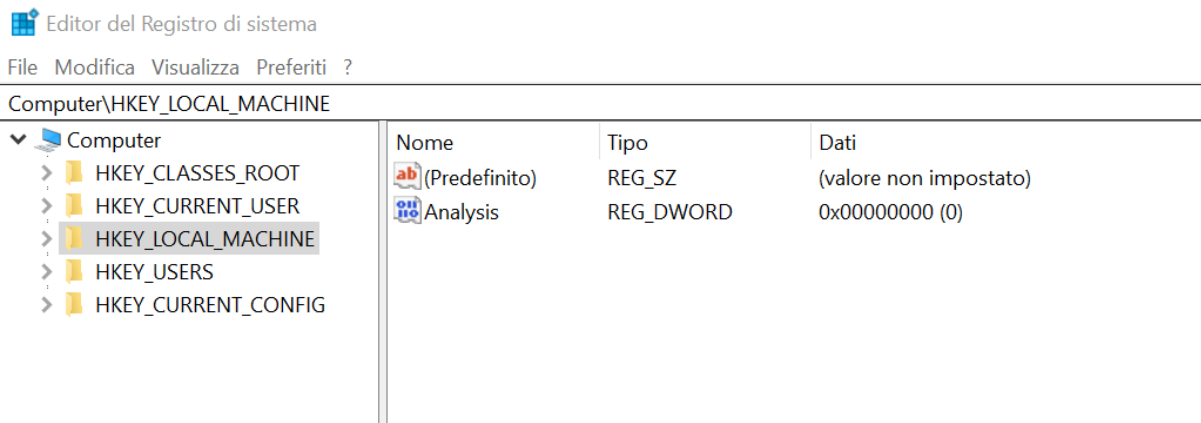
```
Thread      conhost.exe(28908): 5788
Thread      conhost.exe(28908): 3012
Thread      conhost.exe(28908): 3012
Thread      conhost.exe(28908): 3012
Thread      conhost.exe(28908): 3012
Thread      conhost.exe(28908): 4752
```

```
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{E25B58...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{18989B...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{24D89E...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{240018...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{33E281...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{491E92...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{567848...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{2B20DF...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{4BD8D...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A30254...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{52528A...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{7b0db1...
Key          HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{D65231...
```

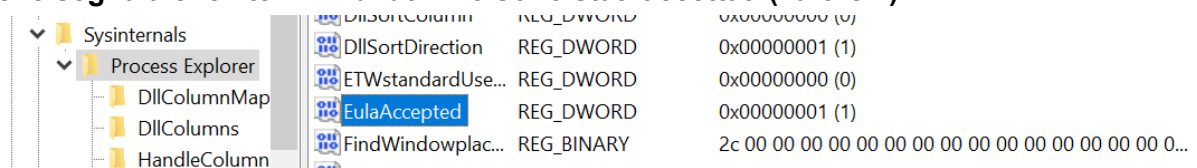
**Esercizi su regedit:**

**Visibilità delle chiavi dei 5 macrogruppi di chiavi di sistema:**

**Ub**



**Individuazione di procexp all'interno delle chiavi del registro, in particolare la stringa che segnala che i termini di utilizzo sono stati accettati (valore 1):**



Modifica del valore 1 in valore 0, per riprodurre nuovamente la richiesta di accettazione:

Process Explorer	REG_DWORD	0x00000000 (0)
EulaAccepted	REG_DWORD	0x00000000 (0)

Dimostrazione della ricomparsa della richiesta di accettazione dei termini di utilizzo:

