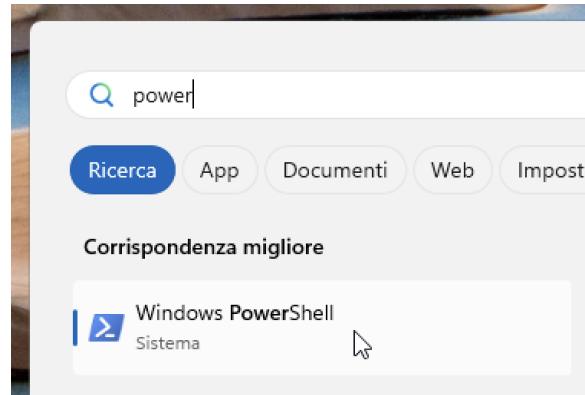


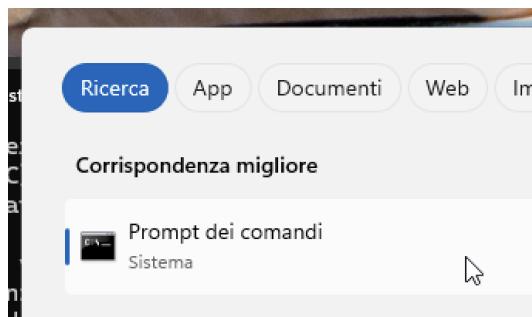
Laboratorio - Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di Cyber Security & Ethical Hacking Cisco CyberOps PowerShell .

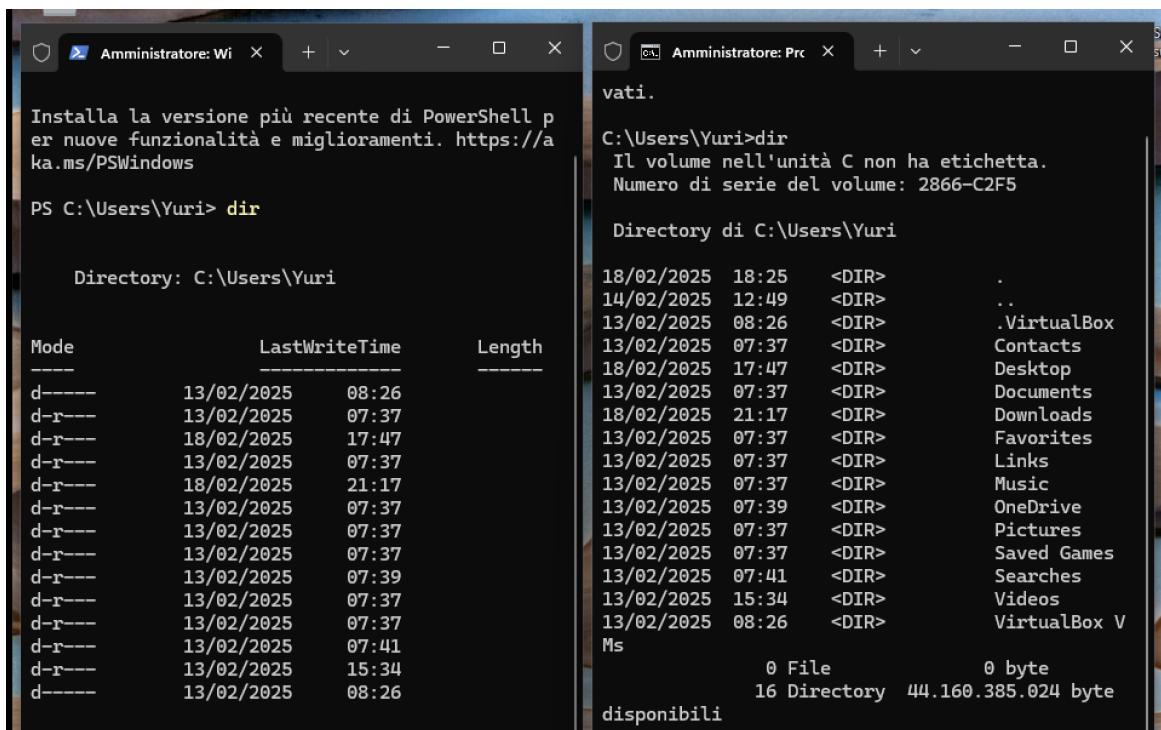
Fare clic su **Start**
Cerca e seleziona **PowerShell**



Fare clic su **Start**
Cerca e seleziona **prompt dei comandi**



Immettere **dir** al prompt in entrambe le finestre



```
Amministratore: Wi
Install la versione più recente di PowerShell p
er nuove funzionalità e miglioramenti. https://a
ka.ms/PSWindows
PS C:\Users\Yuri> dir

Directory: C:\Users\Yuri

Mode LastWriteTime Length
---- ---

d----- 13/02/2025 08:26
d-r--- 13/02/2025 07:37
d-r--- 18/02/2025 17:47
d-r--- 13/02/2025 07:37
d-r--- 18/02/2025 21:17
d-r--- 13/02/2025 07:37
d-r--- 13/02/2025 07:37
d-r--- 13/02/2025 07:37
d-r--- 13/02/2025 07:39
d-r--- 13/02/2025 07:37
d-r--- 13/02/2025 07:37
d-r--- 13/02/2025 07:41
d-r--- 13/02/2025 15:34
d----- 13/02/2025 08:26

Amministratore: Prc
vati.

C:\Users\Yuri>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 2866-C2F5

Directory di C:\Users\Yuri

18/02/2025 18:25 <DIR> .
14/02/2025 12:49 <DIR> ..
13/02/2025 08:26 <DIR> .VirtualBox
13/02/2025 07:37 <DIR> Contacts
18/02/2025 17:47 <DIR> Desktop
13/02/2025 07:37 <DIR> Documents
18/02/2025 21:17 <DIR> Downloads
13/02/2025 07:37 <DIR> Favorites
13/02/2025 07:37 <DIR> Links
13/02/2025 07:37 <DIR> Music
13/02/2025 07:39 <DIR> OneDrive
13/02/2025 07:37 <DIR> Pictures
13/02/2025 07:37 <DIR> Saved Games
13/02/2025 07:41 <DIR> Searches
13/02/2025 15:34 <DIR> Videos
13/02/2025 08:26 <DIR> VirtualBox V
Ms
          0 File          0 byte
      16 Directory  44.160.385.024 byte
disponibili
```

Prova un altro comando che hai utilizzato nel prompt dei comandi, ad esempio **ping** e **ipconfig**

```

    potrebbero ignorare le richie
ste echo se viene utilizzata
questa intestazione.
-S srcaddr Indirizzo di origine da utili
zzare.
-c compartment Identificatore del raggruppam
ento di routing.
-p Esegue il ping dell'indirizzo
di un provider di virtualizzazione di rete d
i Hyper-V.
-4 Impone l'utilizzo di IPv4.
-6 Impone l'utilizzo di IPv6.

PS C:\Users\Yuri> 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=49ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=49ms TTL=115
Risposta da 8.8.8.8: byte=32 durata=50ms TTL=115

Statistiche Ping per 8.8.8.8:
Pacchetti: Trasmessi = 3, Ricevuti = 3,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in
millisecondi:
    Minimo = 49ms, Massimo = 50ms, Medio = 49m
s
Control-C
PS C:\Users\Yuri>

C:\Users\Yuri> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv6 . . . . . : fdf4:e414:ef6f:2ddb:f8f5:5c17:74a3:193c
  Indirizzo IPv6 temporaneo. . . . . : fdf4:e414:ef6f:2ddb:4431:9ac0:cdae:6f7d
  Indirizzo IPv6 locale rispetto al collegamento . . : fe80::7830:4d12:3f85:4151%12
  Indirizzo IPv4. . . . . : 192.168.64.44
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.64.1

C:\Users\Yuri>
  
```

```

PS C:\Users\Yuri> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv6 . . . . . : fdf4:e414:ef6f:2ddb:f8f5:5c17:74a3:193c
  Indirizzo IPv6 temporaneo. . . . . : fdf4:e414:ef6f:2ddb:4431:9ac0:cdae:6f7d
  Indirizzo IPv6 locale rispetto al collegamento . . : fe80::7830:4d12:3f85:4151%12
  Indirizzo IPv4. . . . . : 192.168.64.44
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.64.1

C:\Users\Yuri>
  
```

Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, immettere **Get-Alias dir** al prompt PowerShell.

```
PS C:\Users\Yuri> Get-Alias dir

 CommandType      Name
-----          -----
 Alias           dir -> Get-ChildItem
```

Al prompt di PowerShell, premere invio **netstat -h** per visualizzare le opzioni disponibili

```
Windows 11 Pro
Amministratore: Windows Pow + ▾ Ven 21 feb 11:46
CommandType      Name
-----          -----
Alias           dir -> Get-ChildItem

PS C:\Users\Yuri> netstat -h

Socket Handle Count

 PID      Count  Closing Count
 768       10      0
1800        1      0
1548        4      0
5408        4      0
8740        2      0
3644        3      0
6464        1      0
2644        4      0
8032        2      0
612         4      0
1396        5      0
6008        6      0
3200        2      0
2436        2      0
3468        6      0
8348        8      0
1456        1      0
6332        1      0
748         4      0
1004        9      0
1772        4      0
3564        1      0
8688        3      0
1276        4      0

PS C:\Users\Yuri> |
```

Per visualizzare la tabella di routing con i percorsi attivi, digitare **netstat -r** al prompt

```
PS C:\Users\Yuri> netstat -r
=====
Elenco interfacce
12...56 6b 48 3c 3d 85 .....Red Hat VirtIO Ethernet Adapter
 1.....Software Loopback Interface 1
=====

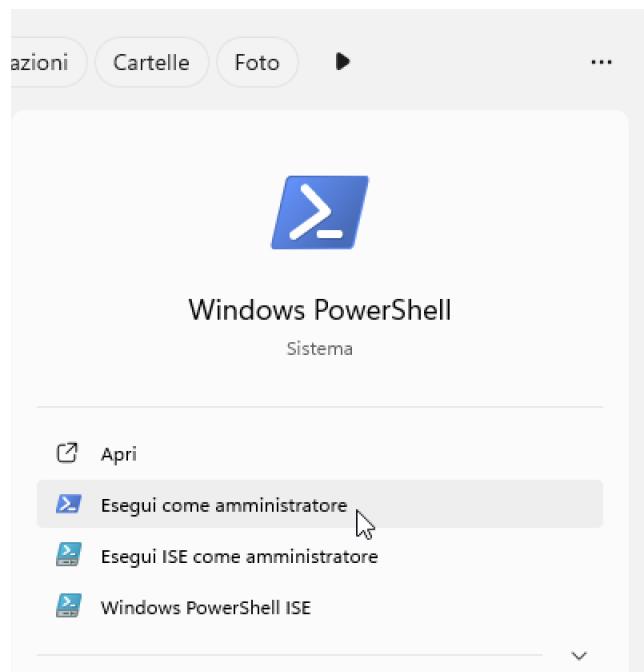
IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask       Gateway     Interfaccia Metrica
    0.0.0.0        0.0.0.0   192.168.64.1  192.168.64.44    15
    127.0.0.0      255.0.0.0   On-link      127.0.0.1     331
    127.0.0.1      255.255.255.255  On-link      127.0.0.1     331
  127.255.255.255 255.255.255.255  On-link      127.0.0.1     331
    192.168.64.0    255.255.255.0   On-link      192.168.64.44    271
    192.168.64.44    255.255.255.255  On-link      192.168.64.44    271
    192.168.64.255  255.255.255.255  On-link      192.168.64.44    271
    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      192.168.64.44    271
  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      192.168.64.44    271
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
    1      331 ::1/128          On-link
    12     271 fdf4:e414:ef6f:2ddb::/64  On-link
    12     271 fdf4:e414:ef6f:2ddb:4431:9ac0:cdae:6f7d/128
                                         On-link
    12     271 fdf4:e414:ef6f:2ddb:f8f5:5c17:74a3:193c/128
                                         On-link
    12     271 fe80::/64          On-link
    12     271 fe80::7830:4d12:3f85:4151/128
                                         On-link
    1      331 ff00::/8          On-link
    12     271 ff00::/8          On-link
```

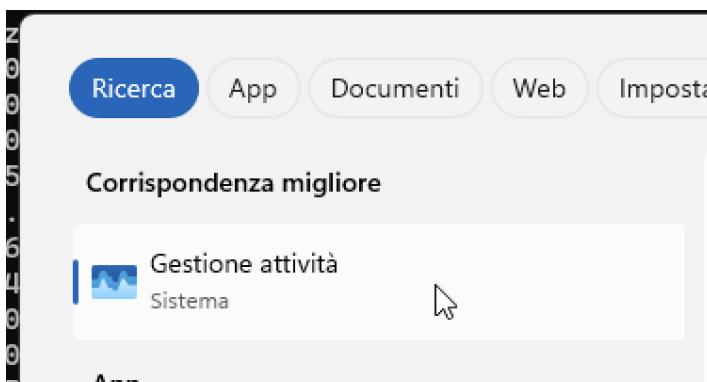
Apri ed esegui un secondo PowerShell con privilegi elevati.

Fai clic su Start . Cerca PowerShell e fai clic con il pulsante destro del mouse su Windows PowerShell e seleziona

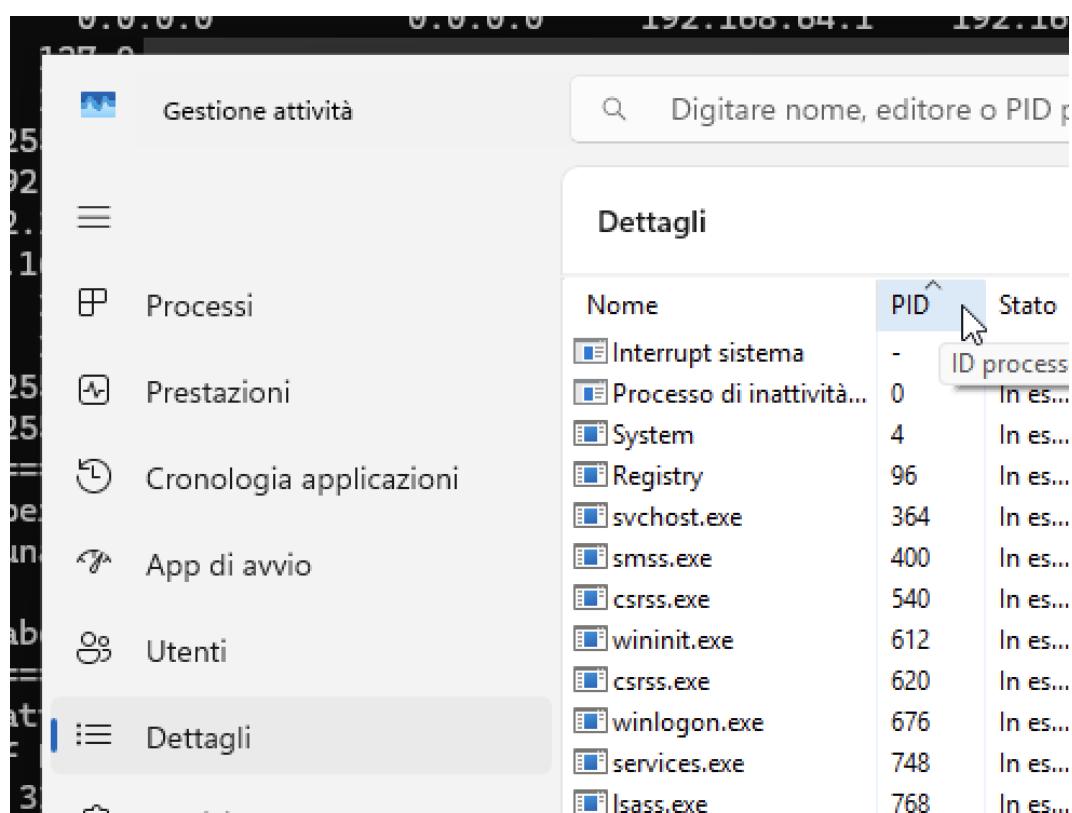
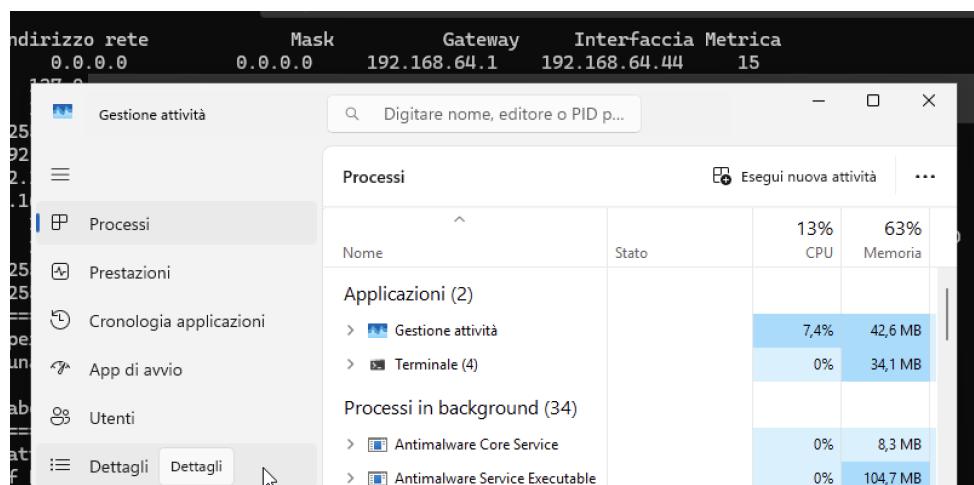
Esegui come amministratore . Fai clic su Sì per consentire a questa app di apportare modifiche al dispositivo.



Il comando netstat può anche visualizzare i processi associati alle connessioni TCP attive. Digitare netstat -abnoal prompt

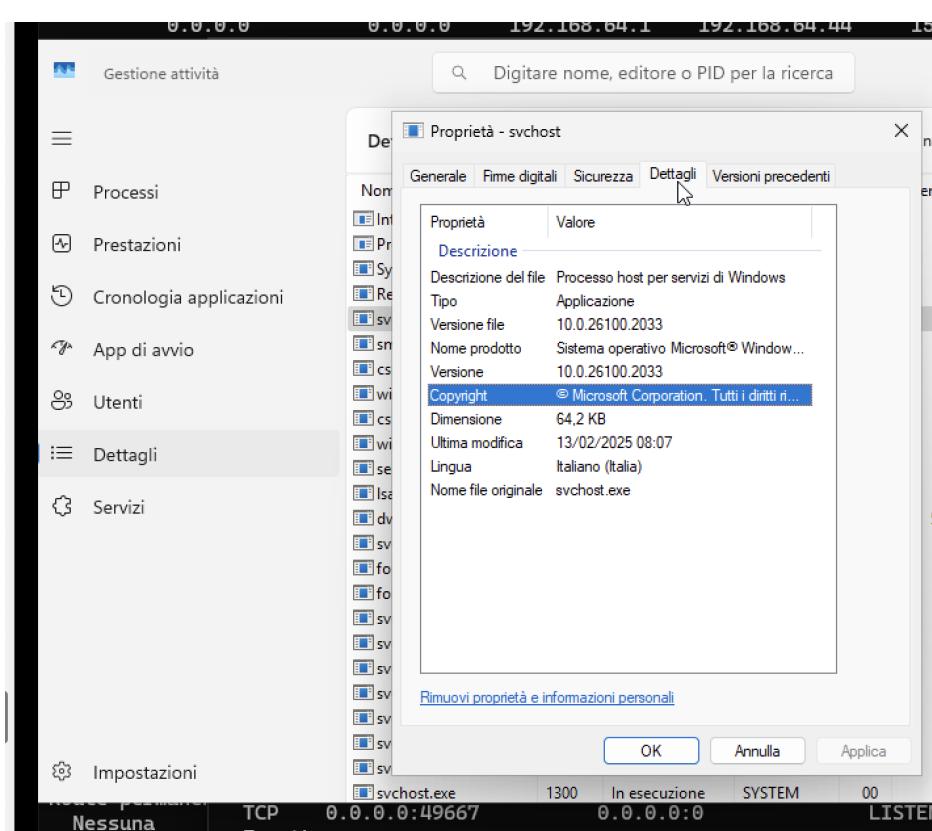
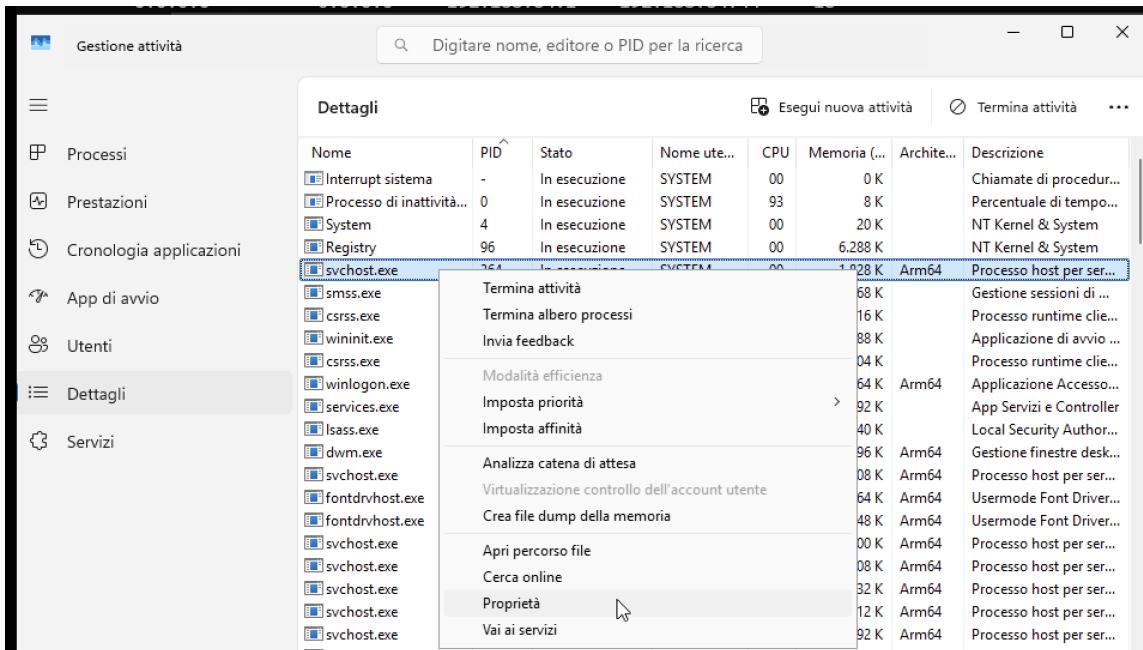


Apri Task Manager. Vai alla scheda Dettagli . Fai clic sull'intestazione PID in modo che i PID siano in ordine.

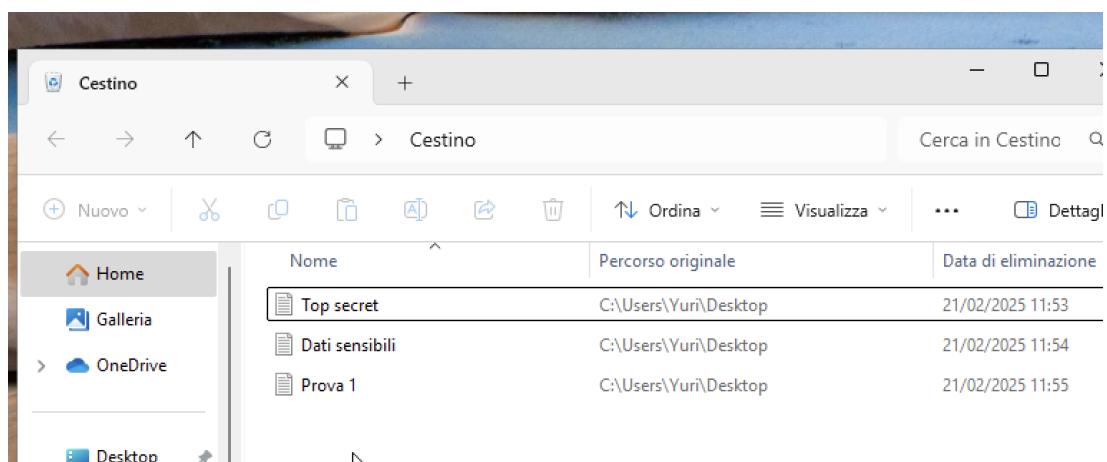
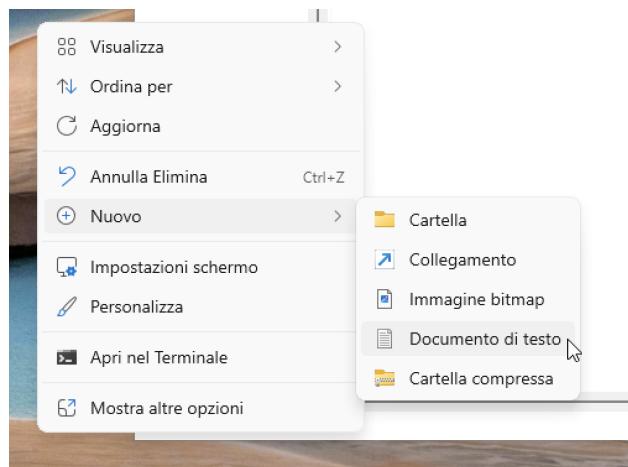


Selezionare uno dei PID dai risultati di netstat -abno. In questo esempio viene utilizzato il PID 756.

Individuare il PID selezionato nel Task Manager. Fare clic con il pulsante destro del mouse sul PID selezionato nel Task Manager per aprire la finestra di dialogo Proprietà per ulteriori informazioni.



Apriamo il cestino, e crea alcuni file, ad esempio un file di testo, utilizzando Blocco note e posizionali nel Cestino.



In una console di PowerShell, immettere clear-recyclebin prompt.

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

A screenshot of a PowerShell window. The command 'clear-recyclebin' is entered at the prompt. A confirmation dialog box appears, asking 'Conferma' (Confirm) and 'Eseguire l'operazione?' (Execute operation?). The message below states 'Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino"' (Execution of the "Clear-RecycleBin" operation on the destination "All contents of the Recycle Bin"). The user is prompted with '[S] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S")' (S) Yes [T] Yes to all [N] No [U] No to all [O] Suspend [?] Help (the default value is "S")).

Il sito **any.run** sta analizzando un file o un URL e ha rilevato attività sospette.

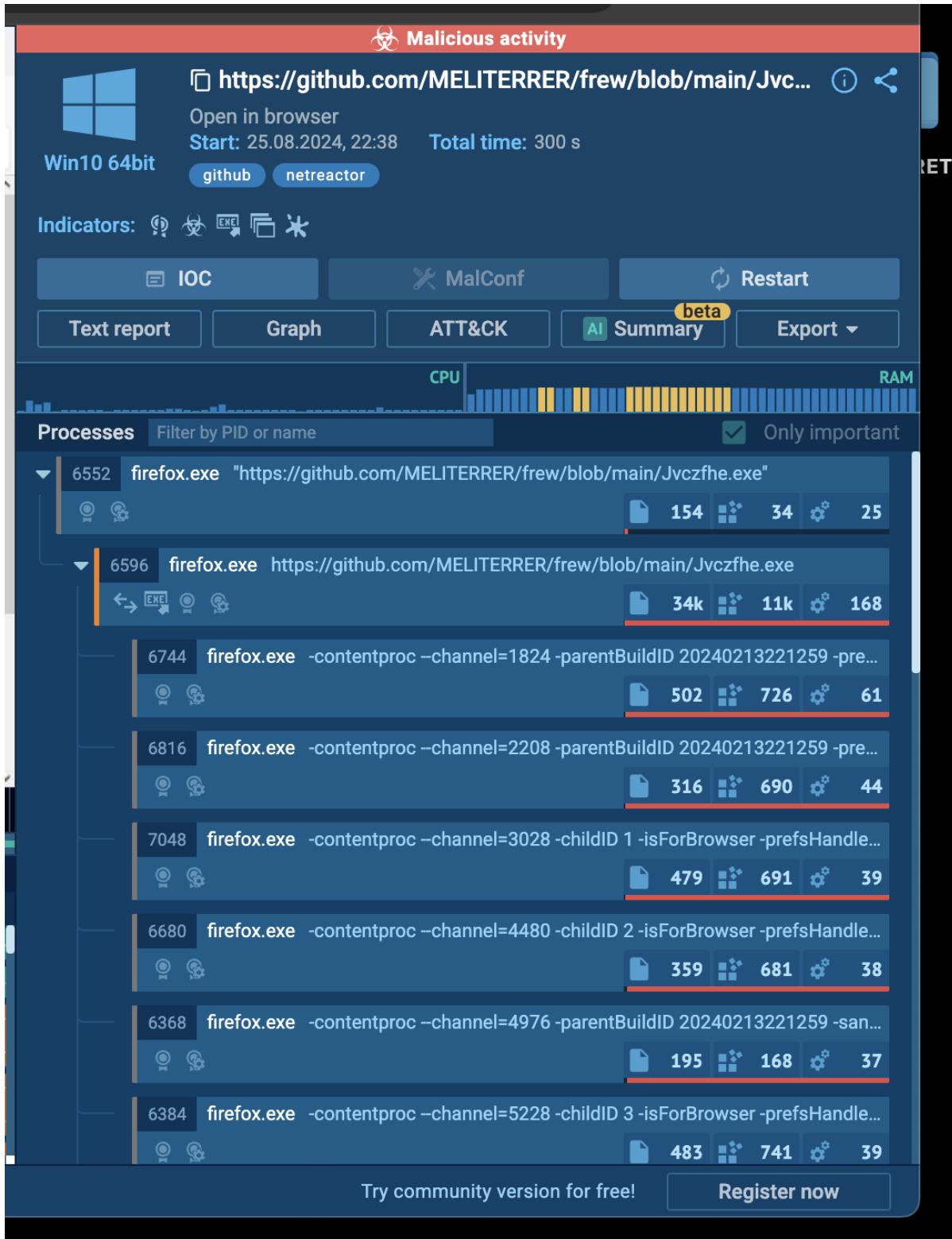
Sembra che il processo “**firefox.exe**” abbia avviato qualcosa di potenzialmente pericoloso nel browser. Ci sono anche dettagli sui processi in esecuzione e su eventuali comportamenti anomali.

L'avviso “**Application launched itself**” indica che il file potrebbe eseguire codice da solo, un comportamento tipico dei malware.

The screenshot shows the any.run analysis interface. At the top, there are tabs for 'Analysis https://github.com/M...', 'Discord | Hospice', and a new tab. The main window displays a GitHub file upload page for 'kiolu / Muadnrd.exe' from the 'MELITERRER / kiolu' repository. The file 'Muadnrd.exe' was uploaded by 'MELITERRER' and has a size of 106 KB. Below this, the 'HTTP Requests' section shows four entries:

Time	Method	Status	Process name	URL	Content
3675 ms	GET	200: OK	6596 firefox.exe	http://detectportal.firefox.com/canonic...	90 b ↓
3729 ms	GET	200: OK	6596 firefox.exe	http://detectportal.firefox.com/success...	8 b ↓
3812 ms	POST	200: OK	6596 firefox.exe	http://ocsp.sectigo.com/	83 b ↑ 282 b ↓
3813 ms	POST	200: OK	6596 firefox.exe	http://r11.o.lencr.org/	85 b ↑ 504 b ↓ 25 b ↓

At the bottom, an info message states: '[7248] Muadnrd.exe .NET Reactor protector has been detected'.



HTTP Requests		31	Connections	99	DNS Requests	161	Threats	19	
Timestamp	Class				PID	Process name			Message
14529 ms	Not Suspicious Traffic				2256	svchost.exe			INFO [ANY.RUN] Attempting to access raw user content on ...
14530 ms	Not Suspicious Traffic				2256	svchost.exe			INFO [ANY.RUN] Attempting to access raw user content on ...
55610 ms	Potentially Bad Traffic				2256	svchost.exe			ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
55607 ms	Potentially Bad Traffic				2256	svchost.exe			ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
55609 ms	Potentially Bad Traffic				2256	svchost.exe			ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
55611 ms	Misc activity				2256	svchost.exe			ET INFO DYNAMIC_DNS Query to *.duckdns. Domain

Info [7248] Muadrd.exe .NET Reactor protector has been detected

Malicious activity

Win10 64bit

https://github.com/MELITERRER/frew/blob/main/Jvc... (i) <

Open in browser
Start: 25.08.2024, 22:38 Total time: 300 s

github netreactor

Indicators: 🛡️ 🌐 EXE 🚫 *

IOC MalConf Restart

Text report Graph ATT&CK AI Summary Export

CPU RAM

Processes Filter by PID or name Only important

- 6552 firefox.exe "https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe" 154 34 25
- 6596 firefox.exe https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe 34k 11k 168

Process details ID 6596 Suspicious

Warning 1

T1036.003 Rename System Utilities (1)

Process drops legitimate windows executable

Other 3

Executable content was dropped or overwritten

T1012 Query Registry (1)

Reads Microsoft Office registry keys

Application launched itself

Try community version for free! Register now

The screenshot shows a security monitoring interface with a central modal window titled "Behavior activities". The window details an alert for a process named "InstallUtil.exe" with PID 5152. The alert is categorized as a "Warning / Unusual Activities" and specifically notes "Connects to unusual port". A sub-section titled "T1571 Non-Standard Port" provides technical details about the connection, including the process path (C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe), destination IP (91.92.253.47), destination port (7702), source port (59005), and protocol (TCP). The background of the interface shows a timeline or log with various entries, some of which are partially visible or blurred.

Behavior activities

(PID: 5152) InstallUtil.exe

Source: network First seen: 56587 ms

?

Warning / Unusual Activities

Connects to unusual port

T1571 Non-Standard Port

Process: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

IpDst: 91.92.253.47

PortDst: 7702

PortSrc: 59005

Protocol: TCP

INFO [ANY.RUN] Attempting to access raw user content on ...

Other 3