Windows Power Shell

Obiettivi

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

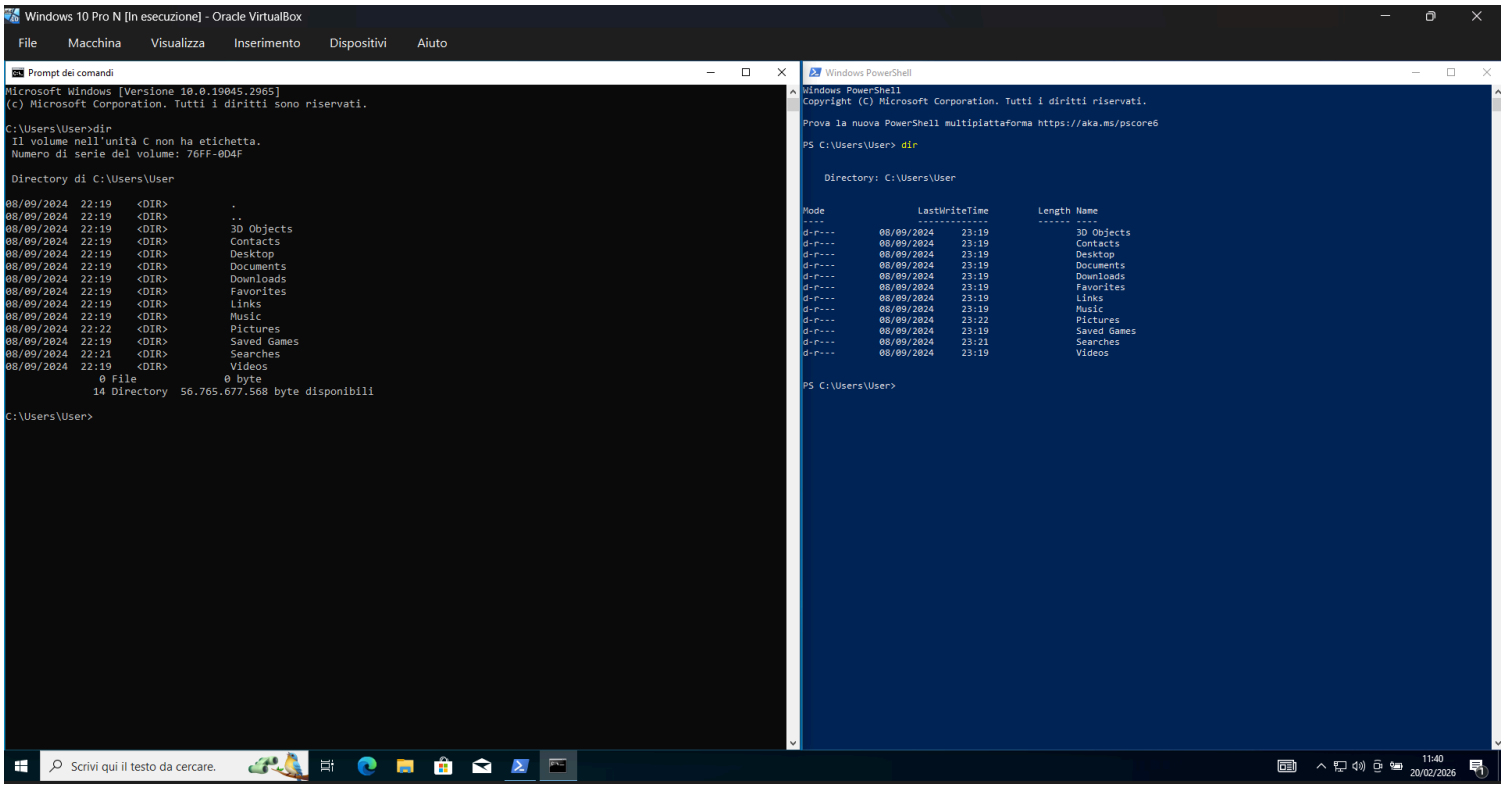
- Parte 1 Accedere alla console PowerShell.
- Parte 2 Esplorare i comandi del Prompt dei Comandi e di PowerShell.
- Parte 3 Esplorare i cmdlet.
- Parte 4 Esplorare il comando netstat usando PowerShell.
- Parte 5 Svuotare il cestino usando PowerShell.

Scenario

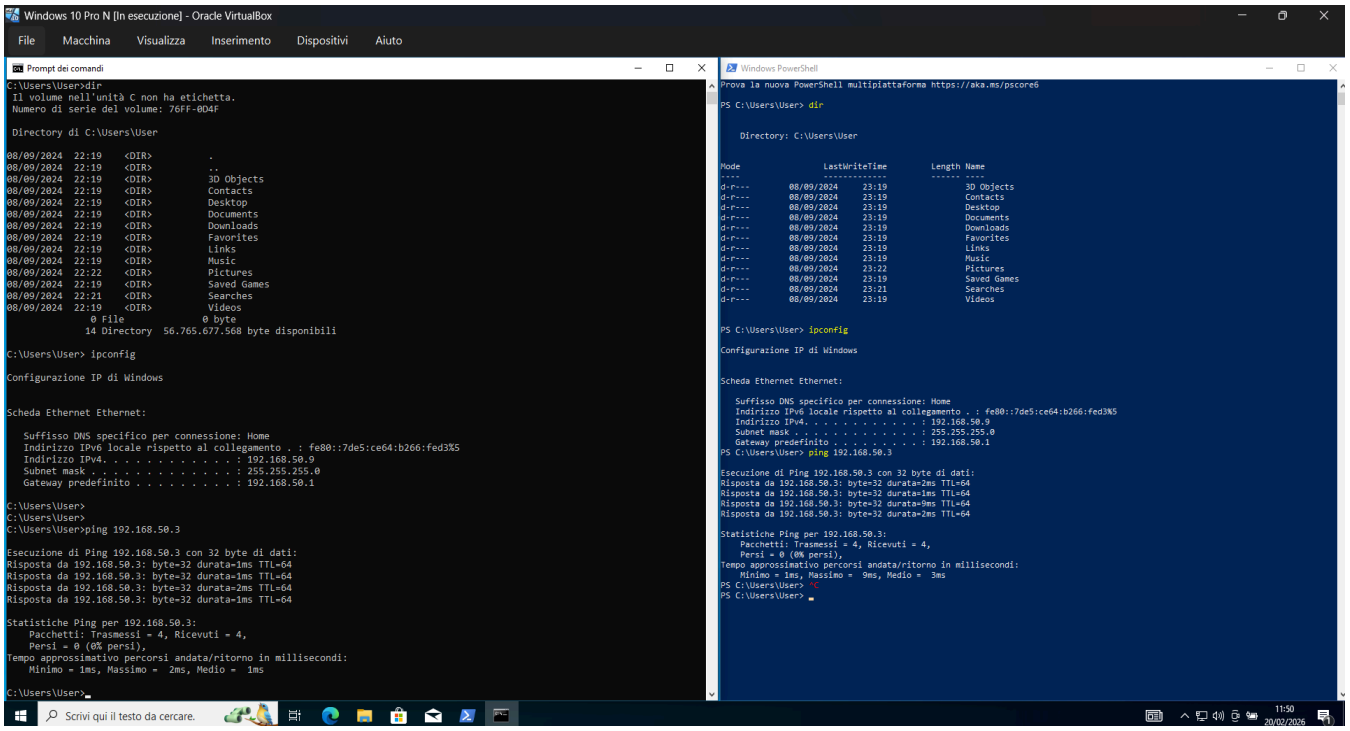
PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell. PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

Azione

Quali sono gli output del comando dir?

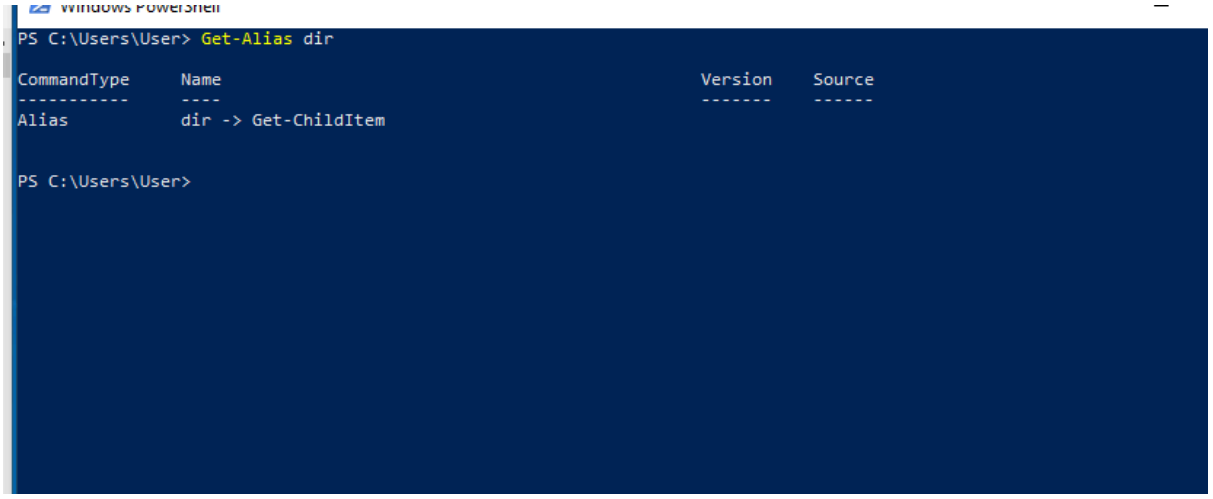


Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. Quali sono i risultati?

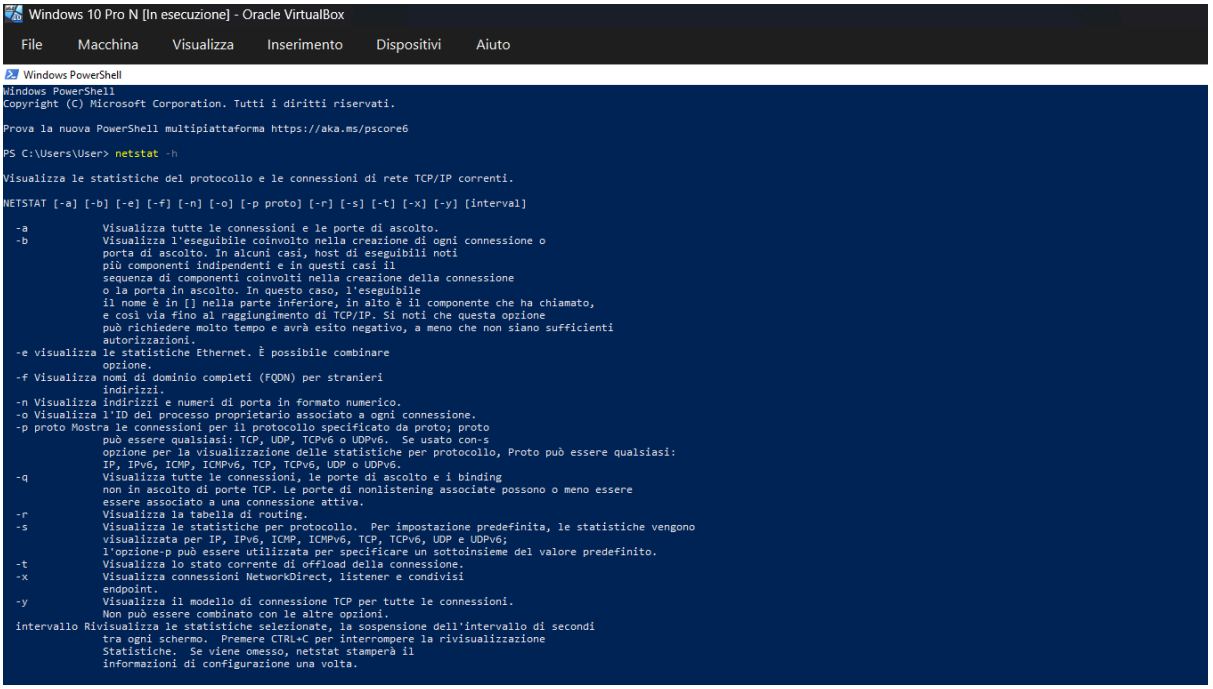


Qual è il comando PowerShell per dir?

Il comando PowerShell per ‘dir’ è Get-ChildItm, come di seguito



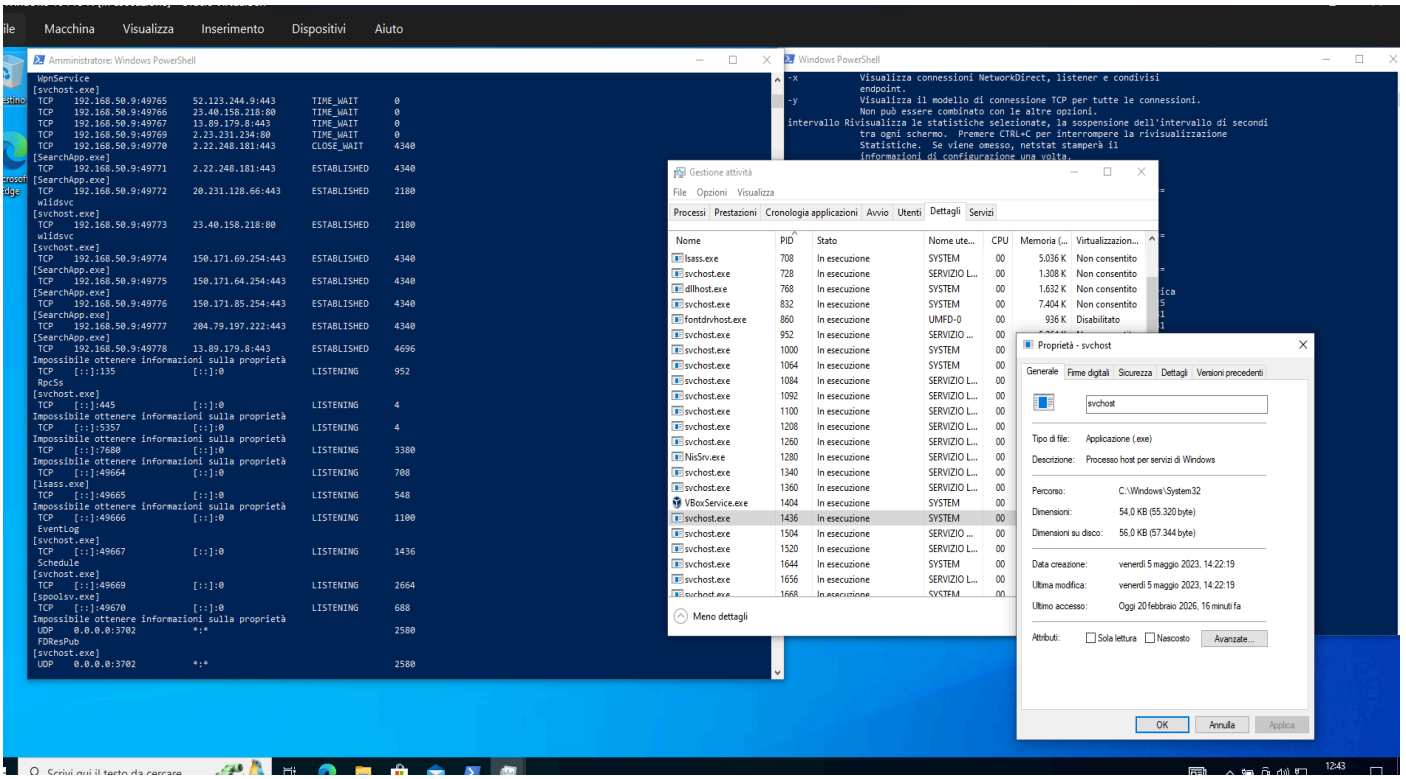
Esplorare il comando netstat usando PowerShell


Windows 10 Pro N [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.
Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6
PS C:\Users\User> netstat -h
Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]
-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
porta di ascolto. In alcuni casi, host di eseguibili noti
più componenti indipendenti e in questi casi il
sequenza di componenti coinvolti nella creazione della connessione
o la porta in ascolto. In questo caso, l'eseguibile
il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
autorizzazioni.
-e visualizza le statistiche Ethernet. È possibile combinare
opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri
indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto
può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6. Se usato con-s
opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza tutte le connessioni, le porte di ascolto e i binding
non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
essere associato a una connessione attiva.
-r Visualizza la tabella di routing.
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono
visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-t Visualizza lo stato corrente di offload della connessione.
-x Visualizza connessioni NetworkDirect, listener e condivisi
endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
Non può essere combinato con le altre opzioni.
intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
Statistiche. Se viene omesso, netstat stamperà il
informazioni di configurazione una volta.

```
              informazioni di configurazione una volta.

PS C:\Users\User> netstat -r
===========================================================================
Elenco interfacce
  8...08 00 27 96 c2 10 ......Intel(R) PRO/1000 MT Desktop 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     192.168.50.1     192.168.50.9     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
     192.168.50.0    255.255.255.0         On-link      192.168.50.9    281
     192.168.50.9  255.255.255.255         On-link      192.168.50.9    281
   192.168.50.255  255.255.255.255         On-link      192.168.50.9    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      192.168.50.9    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      192.168.50.9    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  1    331 ::1/128                  On-link
  8    281 fe80::/64                On-link
  8    281 fe80::7de5:ce64:b266:fed3/128
                                    On-link
  1    331 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
PS C:\Users\User> _
```

Qual è il Gateway IPv4?
Il gateway IPv4 è 192.168.50.1

Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?



Il PID selezionato nella scheda "Dettagli" di Gestione attività è il 1436, corrispondente al processo `svchost.exe`.

Dalla scheda "Dettagli" (Gestione attività)

In questa vista tabellare possiamo monitorare lo stato in tempo reale del processo:

- Nome: `svchost.exe`
- PID: 1436
- Stato: In esecuzione
- Nome utente: SYSTEM (indica che è un processo di sistema con privilegi elevati)
- CPU: 00 (indica che al momento dello screenshot non stava consumando risorse processore significative)
- Memoria (set di lavoro privato): Sebbene la colonna sia parzialmente coperta, per i processi simili si vede un valore in KB.
- Virtualizzazione: Non consentito

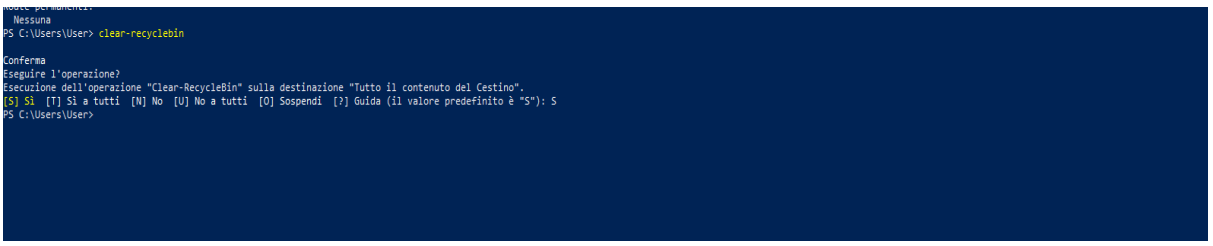
2. Dalla finestra "Proprietà" (Scheda Generale)

Questa finestra fornisce dati statici sul file eseguibile che ha generato quel processo:

- Descrizione: Processo host per servizi di Windows.
- Percorso (Posizione): `C:\Windows\System32` (conferma che si tratta del file di sistema legittimo).
- Dimensioni: 54,0 KB (55.320 byte).
- Dati temporali:
    - Creazione: 5 maggio 2023.
    - Ultima modifica: 5 maggio 2023.
    - Ultimo accesso: Oggi, 20 febbraio 2026 (16 minuti fa).
- Attributi: Il file non è né "Sola lettura" né "Nascosto".

Dalla finestra Proprietà possiamo anche accedere ad altre schede (non visualizzate nel dettaglio ma visibili come tab) per verificare le **Firme digitali** (per assicurarti che il file sia firmato da Microsoft e non sia un malware) e i parametri di **Sicurezza** (permessi di lettura/scrittura).

Svuotare il cestino usando PowerShell.



Cosa è successo ai file nel Cestino?

Con il comando `clear-recyclebin` tutti i file presenti nel cestino sono stati eliminati.

Altri comandi che possiamo usare per semplificare i nostri compiti come analisti di sicurezza:

PowerShell è uno strumento indispensabile per gli analisti di sicurezza (Blue Team/Incident Responder) in ambiente Windows, grazie alla sua capacità di interagire direttamente con gli oggetti di sistema (.NET) e di automatizzare le indagini

Ecco 5 comandi PowerShell fondamentali per l'analisi di sicurezza e il threat hunting:

1. **Analisi dei Log di Sicurezza (Forensics)**

Get-WinEvent

Questo comando è superiore a Get-EventLog per cercare eventi specifici nei log di Windows (Security, System, Application, PowerShell Operational). È fondamentale per individuare tentativi di login falliti o esecuzioni di script sospetti.

es: Get-WinEvent -FilterHashTable @{LogName='Security';ID=4625} -MaxEvents 50

2. **Monitoraggio delle Connessioni di Rete**

Get-NetTCPConnection

Utilizzato per analizzare le connessioni di rete attive e identificare traffico verso IP sospetti o porte non comuni (utile per individuare C2 - Command & Control)

“Get-NetTCPConnection -State Established | Where-Object {$_.RemoteAddress -ne "127.0.0.1"} | Select-Object LocalAddress, RemoteAddress, RemotePort, OwningProces”

```
[S] Sì  [T] Sì a tutti  [N] No  [U] No a tutti  [O] Sospendi  [?] Guida (il valore predefinito è "S"): S
PS C:\Users\User> Get-NetTCPConnection

LocalAddress                        LocalPort RemoteAddress                       RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                       ---------- -----       -------------- -------------
::                                  49670     ::                                  0          Listen                     688
::                                  49669     ::                                  0          Listen                     2664
::                                  49667     ::                                  0          Listen                     1436
::                                  49666     ::                                  0          Listen                     1100
::                                  49665     ::                                  0          Listen                     548
::                                  49664     ::                                  0          Listen                     708
::                                  7680      ::                                  0          Listen                     7960
::                                  5357      ::                                  0          Listen                     4
::                                  445       ::                                  0          Listen                     4
::                                  135       ::                                  0          Listen                     952
0.0.0.0                             49733     0.0.0.0                             0          Bound                      3144
192.168.50.9                        50233     23.206.246.162                      80         TimeWait                   0
192.168.50.9                        49733     4.207.247.139                       443        Established Internet       3144
0.0.0.0                             49670     0.0.0.0                             0          Listen                     688
0.0.0.0                             49669     0.0.0.0                             0          Listen                     2664
0.0.0.0                             49667     0.0.0.0                             0          Listen                     1436
0.0.0.0                             49666     0.0.0.0                             0          Listen                     1100
0.0.0.0                             49665     0.0.0.0                             0          Listen                     548
0.0.0.0                             49664     0.0.0.0                             0          Listen                     708
0.0.0.0                             5040      0.0.0.0                             0          Listen                     3992
192.168.50.9                        139       0.0.0.0                             0          Listen                     4
0.0.0.0                             135       0.0.0.0                             0          Listen                     952
```

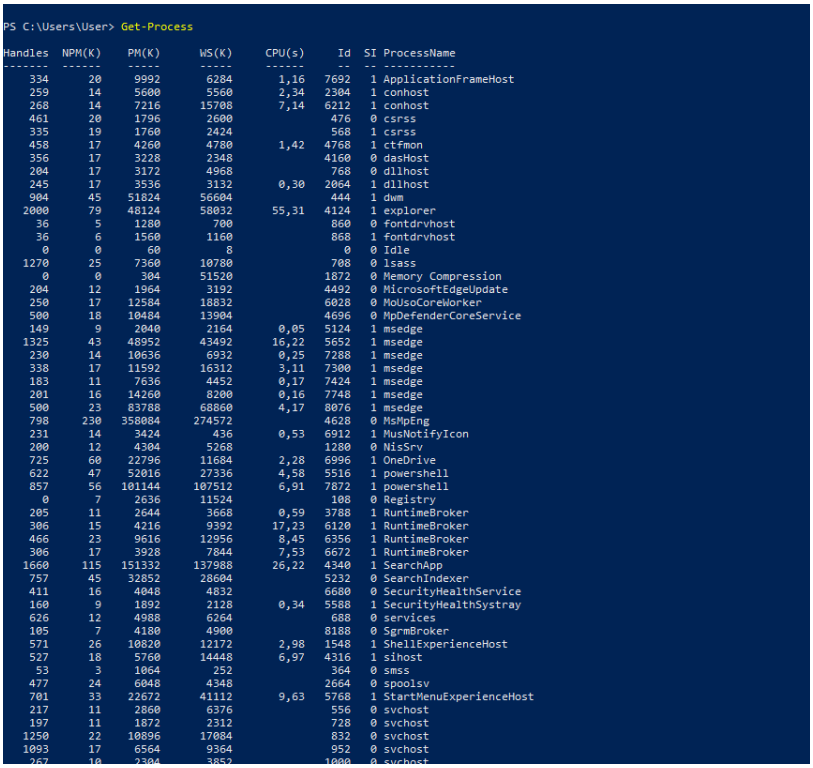
3. Analisi dei Processi in Esecuzione

Get-Process

Indispensabile per il threat hunting in tempo reale per elencare i processi in esecuzione, identificare binari sospetti, o analizzare i processi che consumano risorse anomale.

Esempio (Visualizzare processi con dettagli utili all'analisi):

Get-Process | Select-Object Name, Id, Path, Company | Where-Object {$_.Path -ne $null}



```
PS C:\Users\User> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    334      20     9992       6284       1,16    7692   1 ApplicationFrameHost
    259      14     5600       5560       2,34    2304   1 conhost
    268      14     7216      15708       7,14    6212   1 conhost
    461      20     1796       2600                476   0 csrss
    335      19     1760       2424                568   1 csrss
    458      17     4260       4780       1,42    4768   1 ctfmon
    356      17     3228       2348                4160   0 dasHost
    204      17     3172       4968                768   0 dllhost
    245      17     3536       3132       0,30    2064   1 dllhost
    904      45    51824      56604                444   1 dwm
   2000      79    48124      58032      55,31    4124   1 explorer
     36       5     1280        700                860   0 fontdrvhost
     36       6     1560       1160                868   1 fontdrvhost
      0       0       60          8                  0   0 Idle
   1270      25     7360      10780                708   0 lsass
      0       0      304      51520               1872   0 Memory Compression
    204      12     1964       3192               4492   0 MicrosoftEdgeUpdate
    250      17    12584      18832               6028   0 MoUsoCoreWorker
    500      18    10484      13904               4696   0 MpDefenderCoreService
    149       9     2040       2164       0,05    5124   1 msedge
   1325      43    48952      43492      16,22    5652   1 msedge
    230      14    10636       6932       0,25    7288   1 msedge
    338      17    11592      16312       3,11    7300   1 msedge
    183      11     7636       4452       0,17    7424   1 msedge
    201      16    14260       8200       0,16    7748   1 msedge
    500      23    83788      68860       4,17    8076   1 msedge
    798     230   358084     274572                4628   0 MsMpEng
    231      14     3424        436       0,53    6912   1 MusNotifyIcon
    200      12     4304       5268                1280   0 NisSrv
    725      60    22796      11684       2,28    6996   1 OneDrive
    622      47    52016      27336       4,58    5516   1 powershell
    857      56   101144     107512       6,91    7872   1 powershell
      0       7     2636      11524                108   0 Registry
    205      11     2644       3668       0,59    3788   1 RuntimeBroker
    306      15     4216       9392      17,23    6120   1 RuntimeBroker
    466      23     9616      12956       8,45    6356   1 RuntimeBroker
    306      17     3928       7844       7,53    6672   1 RuntimeBroker
   1660     115   151332     137988      26,22    4340   1 SearchApp
    757      45    32852      28604                5232   0 SearchIndexer
    411      16     4048       4832                6680   0 SecurityHealthService
    160       9     1892       2128       0,34    5588   1 SecurityHealthSystray
    626      12     4988       6264                688   0 services
    105       7     4180       4900                8188   0 SgrmBroker
    571      26    10820      12172       2,98    1548   1 ShellExperienceHost
    527      18     5760      14448       6,97    4316   1 sihost
     53       3     1064        252                364   0 smss
    477      24     6048       4348                2664   0 spoolsv
    701      33    22672      41112       9,63    5768   1 StartMenuExperienceHost
    217      11     2860       6376                556   0 svchost
    197      11     1872       2312                728   0 svchost
   1250      22    10896      17084                832   0 svchost
   1093      17     6564       9364                952   0 svchost
    257      10     2304       3852               1000   0 svchost
```

4. Verifica dell'Integrità dei File

Get-FileHash

Calcola l'hash (SHA256 di default) di un file. È cruciale per confrontare il file sospetto con database di minacce note (come VirusTotal)

Esempio (Calcolare l'hash di un eseguibile):

Get-FileHash -Path "C:\Windows\System32\suspect.exe" -Algorithm SHA256

5. Investigazione su Script PowerShell Malevoli

Get-Content (con script block logging)

Sebbene Get-Content legga file di testo, combinato con i log di PowerShell Operational (Event ID 4104), permette di analizzare blocchi di script codificati o offuscati (spesso in Base64) eseguiti nel sistema

Esempio (Cercare comandi codificati nei log)

Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" | Where-Object {$_.Message -match "-e|-en|-enc|-enco"}

Fonti: Sans Institute / Codetwo.

20/02/2026
Bartolomeo Tarantino