Report Esercizio 1: Usare Windows PowerShell

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

Contesto / Scenario

PowerShell è uno strumento di automazione avanzato che funge sia da console di comando sia da linguaggio di scripting. Permette di automatizzare attività e interagire in modo efficiente con il sistema operativo Windows.

Parte 1: Accesso alla console

- Sono state aperte entrambe le console: **Prompt dei Comandi (cmd)** e **Windows PowerShell**, tramite il menu Start.

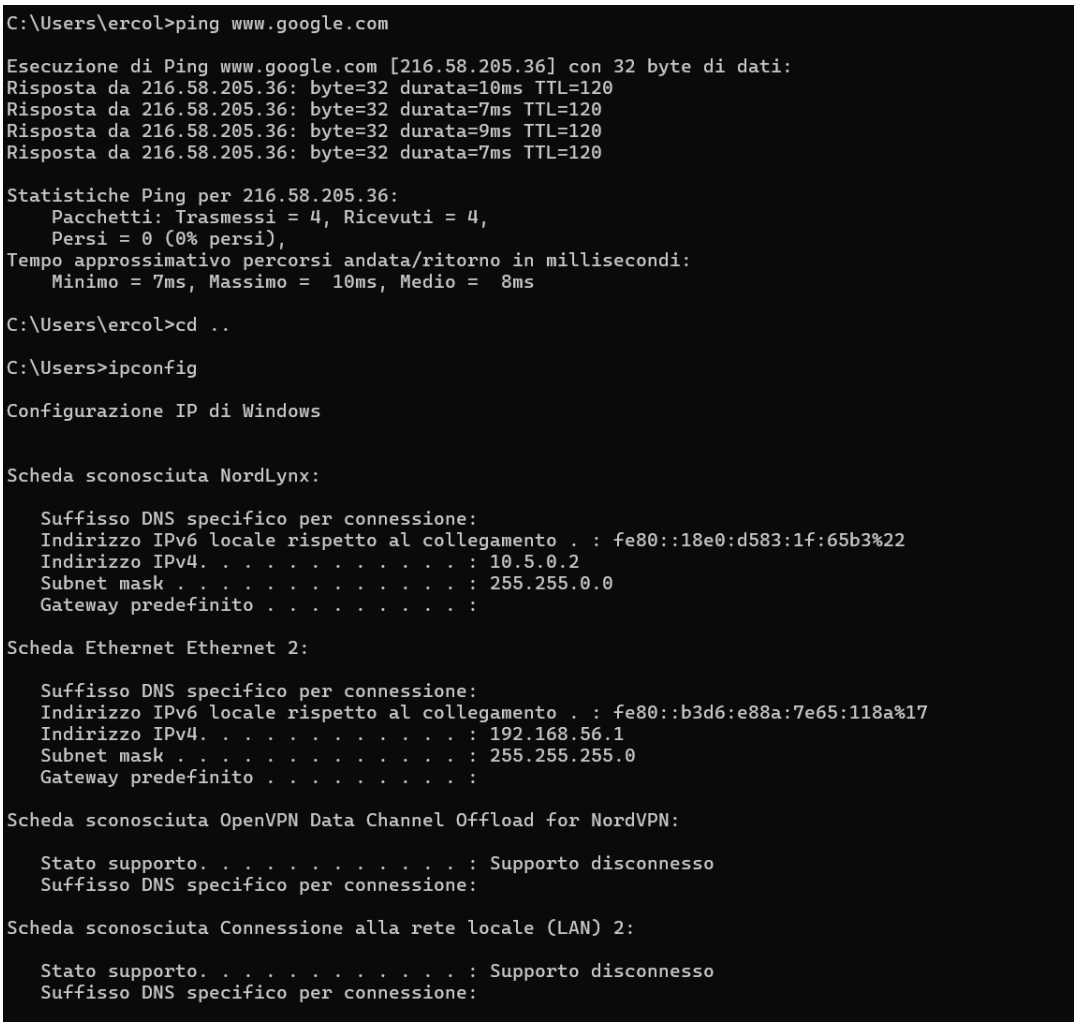
Parte 2: Confronto comandi base

Comando	CMD	PowerShell
`dir`	Elenco base	Alias di `Get-ChildItem`
`ping`	Funziona	Funziona
`cd ..`	Funziona	Funziona

`ipconfig`	Output di rete	Output identico, ma più completo in PowerShell

Le differenze principali riguardano la formattazione dell'output e la gestione delle interfacce.

cmd



```
PS C:\Users\ercol> ping www.google.com

Esecuzione di Ping www.google.com [216.58.205.36] con 32 byte di dati:
Risposta da 216.58.205.36: byte=32 durata=8ms TTL=120
Risposta da 216.58.205.36: byte=32 durata=7ms TTL=120
Risposta da 216.58.205.36: byte=32 durata=7ms TTL=120
Risposta da 216.58.205.36: byte=32 durata=6ms TTL=120

Statistiche Ping per 216.58.205.36:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 6ms, Massimo =  8ms, Medio =  7ms
PS C:\Users\ercol> cd ..
PS C:\Users> ipconfig

Configurazione IP di Windows


Scheda sconosciuta NordLynx:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::18e0:d583:1f:65b3%22
   Indirizzo IPv4. . . . . . . . . . . . : 10.5.0.2
   Subnet mask . . . . . . . . . . . . . : 255.255.0.0
   Gateway predefinito . . . . . . . . . :

Scheda Ethernet Ethernet 2:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::b3d6:e88a:7e65:118a%17
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.56.1
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . :

Scheda sconosciuta OpenVPN Data Channel Offload for NordVPN:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda sconosciuta Connessione alla rete locale (LAN) 2:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:
```

powershell

Parte 3: Cmdlet in PowerShell

- Comando `Get-Alias dir` mostra che `dir` è un alias del cmdlet `Get-ChildItem`
- Comando `Get-Command` elenca tutti i cmdlet disponibili

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

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

```
PS C:\Users> Get-Command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           Add-AppPackage                                     2.0.1.0    Appx
Alias           Add-AppPackageVolume                               2.0.1.0    Appx
Alias           Add-AppProvisionedPackage                          3.0        Dism
Alias           Add-MsixPackage                                    2.0.1.0    Appx
Alias           Add-MsixPackageVolume                              2.0.1.0    Appx
Alias           Add-MsixVolume                                     2.0.1.0    Appx
Alias           Add-ProvisionedAppPackage                          3.0        Dism
Alias           Add-ProvisionedAppSharedPackageContainer           3.0        Dism
Alias           Add-ProvisionedAppxPackage                         3.0        Dism
Alias           Add-ProvisioningPackage                            3.0        Provisioning
Alias           Add-TrustedProvisioningCertificate                 3.0        Provisioning
Alias           Apply-WindowsUnattend                              3.0        Dism
Alias           Disable-PhysicalDiskIndication                     2.0.0.0    Storage
Alias           Disable-PhysicalDiskIndication                     1.0.0.0    VMDirectStorage
Alias           Disable-StorageDiagnosticLog                       2.0.0.0    Storage
Alias           Disable-StorageDiagnosticLog                       1.0.0.0    VMDirectStorage
Alias           Dismount-AppPackageVolume                          2.0.1.0    Appx
Alias           Dismount-MsixPackageVolume                         2.0.1.0    Appx
Alias           Dismount-MsixVolume                                2.0.1.0    Appx
Alias           Enable-PhysicalDiskIndication                      2.0.0.0    Storage
Alias           Enable-PhysicalDiskIndication                      1.0.0.0    VMDirectStorage
Alias           Enable-StorageDiagnosticLog                        2.0.0.0    Storage
Alias           Enable-StorageDiagnosticLog                        1.0.0.0    VMDirectStorage
Alias           Flush-Volume                                       2.0.0.0    Storage
Alias           Flush-Volume                                       1.0.0.0    VMDirectStorage
Alias           Get-AppPackage                                     2.0.1.0    Appx
Alias           Get-AppPackageAutoUpdateSettings                   2.0.1.0    Appx
Alias           Get-AppPackageDefaultVolume                        2.0.1.0    Appx
Alias           Get-AppPackageLastError                            2.0.1.0    Appx
Alias           Get-AppPackageLog                                  2.0.1.0    Appx
Alias           Get-AppPackageManifest                             2.0.1.0    Appx
Alias           Get-AppPackageVolume                               2.0.1.0    Appx
Alias           Get-AppProvisionedPackage                          3.0        Dism
Alias           Get-DiskSNV                                        2.0.0.0    Storage
Alias           Get-DiskSNV                                        1.0.0.0    VMDirectStorage
Alias           Get-Language                                       1.0        LanguagePackManagement
Alias           Get-MsixDefaultVolume                              2.0.1.0    Appx
Alias           Get-MsixLastError                                  2.0.1.0    Appx
Alias           Get-MsixLog                                        2.0.1.0    Appx
Alias           Get-MsixPackage                                    2.0.1.0    Appx
Alias           Get-MsixPackageAutoUpdateSettings                  2.0.1.0    Appx
Alias           Get-MsixPackageDefaultVolume                       2.0.1.0    Appx
Alias           Get-MsixPackageLastError                           2.0.1.0    Appx
Alias           Get-MsixPackageLog                                 2.0.1.0    Appx
Alias           Get-MsixPackageManifest                            2.0.1.0    Appx
Alias           Get-MsixPackageVolume                              2.0.1.0    Appx
```

Parte 4: Comando `netstat`

a. `netstat`

```
PS C:\Users> netstat

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    127.0.0.1:1042         ASUS-di-Antonio:55407  ESTABLISHED
  TCP    127.0.0.1:1042         ASUS-di-Antonio:55450  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51035  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51037  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51056  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51058  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51109  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51111  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51121  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51123  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51151  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51152  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51293  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51294  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51295  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51296  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51786  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:51791  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53023  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53024  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53050  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53053  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53676  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53678  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53798  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:53799  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:54940  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:54942  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55310  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55311  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55352  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55355  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55508  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55510  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55516  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:55518  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:56564  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:56566  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:57616  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:57617  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:57676  ESTABLISHED
  TCP    127.0.0.1:6850         ASUS-di-Antonio:57677  ESTABLISHED
```

- Mostra tutte le connessioni attive
- Protocolli, indirizzi locali/remoti, stato (es. ESTABLISHED)

b. `netstat -ano`

```
PS C:\Users> netstat -ano

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:135             0.0.0.0:0              LISTENING       1908
  TCP    0.0.0.0:445             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040            0.0.0.0:0              LISTENING       14172
  TCP    0.0.0.0:6850            0.0.0.0:0              LISTENING       48404
  TCP    0.0.0.0:6881            0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:7680            0.0.0.0:0              LISTENING       19896
  TCP    0.0.0.0:8000            0.0.0.0:0              LISTENING       6928
  TCP    0.0.0.0:8089            0.0.0.0:0              LISTENING       6928
  TCP    0.0.0.0:8191            0.0.0.0:0              LISTENING       19796
  TCP    0.0.0.0:9012            0.0.0.0:0              LISTENING       17084
  TCP    0.0.0.0:9013            0.0.0.0:0              LISTENING       17084
  TCP    0.0.0.0:9014            0.0.0.0:0              LISTENING       27432
  TCP    0.0.0.0:12177           0.0.0.0:0              LISTENING       35516
  TCP    0.0.0.0:19575           0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:19576           0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:19577           0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:49664           0.0.0.0:0              LISTENING       1528
  TCP    0.0.0.0:49665           0.0.0.0:0              LISTENING       1428
  TCP    0.0.0.0:49666           0.0.0.0:0              LISTENING       2356
  TCP    0.0.0.0:49669           0.0.0.0:0              LISTENING       3740
  TCP    0.0.0.0:49670           0.0.0.0:0              LISTENING       5304
  TCP    0.0.0.0:49697           0.0.0.0:0              LISTENING       1500
  TCP    10.5.0.2:139            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1042          0.0.0.0:0              LISTENING       39696
  TCP    127.0.0.1:1042          127.0.0.1:55407        ESTABLISHED     39696
  TCP    127.0.0.1:1042          127.0.0.1:55450        ESTABLISHED     39696
  TCP    127.0.0.1:1043          0.0.0.0:0              LISTENING       39696
  TCP    127.0.0.1:2000          0.0.0.0:0              LISTENING       37872
  TCP    127.0.0.1:3215          0.0.0.0:0              LISTENING       42332
  TCP    127.0.0.1:3216          0.0.0.0:0              LISTENING       67452
  TCP    127.0.0.1:3217          0.0.0.0:0              LISTENING       67452
  TCP    127.0.0.1:5939          0.0.0.0:0              LISTENING       6876
  TCP    127.0.0.1:6850          127.0.0.1:51035        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51037        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51056        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51058        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51109        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51111        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51121        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51123        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51151        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51152        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51293        ESTABLISHED     48404
  TCP    127.0.0.1:6850          127.0.0.1:51294        ESTABLISHED     48404
```

- Aggiunge la colonna PID (Process ID) per ogni connessione

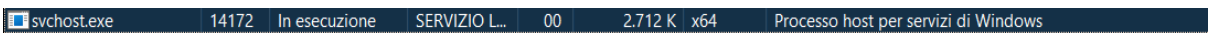
c. `netstat -ano | findstr LISTENING`

```
PS C:\Users> netstat -ano | findstr LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1908
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       14172
  TCP    0.0.0.0:6850           0.0.0.0:0              LISTENING       48404
  TCP    0.0.0.0:6881           0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       19896
  TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING       6928
  TCP    0.0.0.0:8089           0.0.0.0:0              LISTENING       6928
  TCP    0.0.0.0:8191           0.0.0.0:0              LISTENING       19796
  TCP    0.0.0.0:9012           0.0.0.0:0              LISTENING       17084
  TCP    0.0.0.0:9013           0.0.0.0:0              LISTENING       17084
  TCP    0.0.0.0:9014           0.0.0.0:0              LISTENING       27432
  TCP    0.0.0.0:12177          0.0.0.0:0              LISTENING       35516
  TCP    0.0.0.0:19575          0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:19576          0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:19577          0.0.0.0:0              LISTENING       24788
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1528
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1428
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2356
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       3740
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       5304
  TCP    0.0.0.0:49697          0.0.0.0:0              LISTENING       1500
  TCP    10.5.0.2:139           0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1042         0.0.0.0:0              LISTENING       39696
  TCP    127.0.0.1:1043         0.0.0.0:0              LISTENING       39696
  TCP    127.0.0.1:2000         0.0.0.0:0              LISTENING       37872
  TCP    127.0.0.1:3215         0.0.0.0:0              LISTENING       42332
  TCP    127.0.0.1:3216         0.0.0.0:0              LISTENING       67452
  TCP    127.0.0.1:3217         0.0.0.0:0              LISTENING       67452
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       6876
  TCP    127.0.0.1:7778         0.0.0.0:0              LISTENING       5980
  TCP    127.0.0.1:8065         0.0.0.0:0              LISTENING       19176
  TCP    127.0.0.1:9010         0.0.0.0:0              LISTENING       18136
  TCP    127.0.0.1:9180         0.0.0.0:0              LISTENING       61252
  TCP    127.0.0.1:9247         0.0.0.0:0              LISTENING       5404
  TCP    127.0.0.1:11000        0.0.0.0:0              LISTENING       37872
  TCP    127.0.0.1:11001        0.0.0.0:0              LISTENING       59760
  TCP    127.0.0.1:13010        0.0.0.0:0              LISTENING       5988
  TCP    127.0.0.1:13030        0.0.0.0:0              LISTENING       6736
  TCP    127.0.0.1:13031        0.0.0.0:0              LISTENING       20320
  TCP    127.0.0.1:13032        0.0.0.0:0              LISTENING       20320
  TCP    127.0.0.1:17532        0.0.0.0:0              LISTENING       5988
  TCP    127.0.0.1:17945        0.0.0.0:0              LISTENING       20320
  TCP    127.0.0.1:22112        0.0.0.0:0              LISTENING       6736
  TCP    127.0.0.1:24830        0.0.0.0:0              LISTENING       6020
  TCP    127.0.0.1:27339        0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:45654        0.0.0.0:0              LISTENING       18136
  TCP    127.0.0.1:49679        0.0.0.0:0              LISTENING       6756
```

- Filtra le sole connessioni in ascolto

d. e. f. g. Gestione Attività (Task Manager)

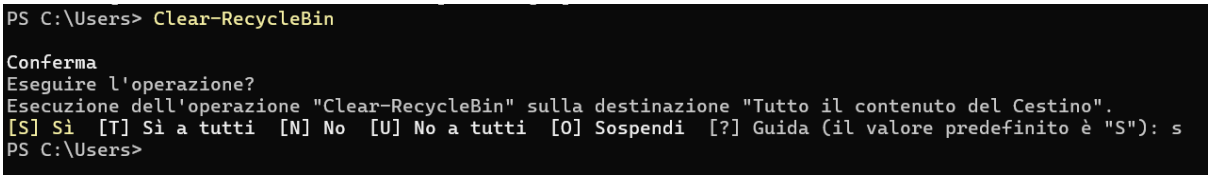
- Tramite `netstat -ano` sono stati identificati alcuni PID attivi



- È stato aperto **Task Manager**, scheda **Dettagli**, ordinati i processi per PID
- Identificato un processo attivo, in questo caso `svchost.exe`, corrispondente al PID 14172 visualizzato in PowerShell
- Tramite clic destro è stato aperto il menu "Proprietà" per ottenere maggiori informazioni sul processo

---

Parte 5: Svuotare il Cestino



- Comando usato: `Clear-RecycleBin`
- L'operazione ha richiesto conferma
- Confermata l'eliminazione con `s`, il contenuto è stato rimosso

---

Domanda di riflessione

Quali comandi potresti usare per semplificare i tuoi compiti come analista di sicurezza?

Come analista di sicurezza, PowerShell può semplificare varie attività, come:

- Monitoraggio della rete: `netstat`, `Get-NetTCPConnection`
- Raccolta informazioni sul sistema: `Get-Process`, `Get-Service`, `Get-EventLog`
- Analisi degli utenti e permessi: `Get-LocalUser`, `Get-LocalGroupMember`
- Automazione delle scansioni e controlli di sicurezza periodici
- Interazione con file e cartelle in modo sicuro e controllato con `Get-ChildItem`, `Remove-Item`, `Copy-Item`
  PowerShell consente di creare script ripetibili, modificabili e condivisibili, rendendo più veloce ed efficiente la gestione di task quotidiani nel campo della cybersecurity.