

UTILIZZO DI POWERSHELL

- Parte 1: accedere alla console di PowerShell.
- Parte 2: Esplora i comandi del prompt dei comandi e di PowerShell.
- Parte 3: Esplora i cmdlet.
- Parte 4: Esplora il comando netstat utilizzando PowerShell.
- Parte 5: Svuotare il cestino tramite PowerShell.

1) Apriamo Powershell = Start >PowerShell

2) Tramite il comando dir su prompt dei comandi e sulla console di PowerShell notiamo che le interfacce sono simili mostrandoci una lista di sottodirectory e file, sulla console di PowerShell si possono notare anche gli attributi/modalità

```
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\admin>dir
Il volume nell'unità C è Windows
Numero di serie del volume: E217-1F93

Directory di C:\Users\admin

10/04/2025  18:05    <DIR>          .
14/02/2025  11:49    <DIR>          ..
10/01/2023  13:53    <DIR>          .cache
21/02/2025  17:28                176 .packettracer
11/04/2025  09:41    <DIR>          .VirtualBox
21/02/2025  19:10    <DIR>          Cisco Packet Tracer 8.2.2
14/02/2025  13:38    <DIR>          Contacts
13/06/2024  10:12    <DIR>          Documents
09/04/2025  15:47    <DIR>          Downloads
14/02/2025  13:38    <DIR>          Favorites
14/02/2025  13:38    <DIR>          Links
14/02/2025  13:38    <DIR>          Music
14/02/2025  13:32    <DIR>          OneDrive
14/02/2025  13:38    <DIR>          Saved Games
14/02/2025  13:38    <DIR>          Searches
18/12/2023  12:30    <DIR>          Tracing
14/02/2025  16:29    <DIR>          Videos
09/04/2025  14:10    <DIR>          VirtualBox VMs
               1 File                176 byte
            17 Directory 41.901.465.600 byte disponibili
```

3) Esploriamo ora il cmdlet su PowerShell. Digitando il comando Get-Alias dir e notiamo che il comando per dir è Get-ChildItem.

```
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\admin> Get-Alias dir

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

4) Netstat con Powershell. Digitiamo netstat -r e visualizziamo l'elenco interfaccia e la tabella di route ipv4 notando che il Gateway risulta 192.168.1.1

```
PS C:\Users\admin> netstat -r

=====
Elenco interfacce
15...00 ff 93 c2 12 8e .....ExpressVPN TAP Adapter
12.....ExpressVPN TUN Driver
4...0a 00 27 00 00 04 .....VirtualBox Host-Only Ethernet Adapter
16...ae 50 de 06 3a 25 .....Microsoft Wi-Fi Direct Virtual Adapter
10...ee 50 de 06 3a 25 .....Microsoft Wi-Fi Direct Virtual Adapter #2
2...ac 50 de 06 3a 25 .....Realtek RTL8822CE 802.11ac PCIe Adapter
18...ac 50 de 06 3a 26 .....Bluetooth Device (Personal Area Network)
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      192.168.1.5      35
      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
      192.168.1.0      255.255.255.0      On-link      192.168.1.5      291
      192.168.1.5      255.255.255.255      On-link      192.168.1.5      291
      192.168.1.255      255.255.255.255      On-link      192.168.1.5      291
      192.168.253.0      255.255.255.0      On-link      192.168.253.1      281
      192.168.253.1      255.255.255.255      On-link      192.168.253.1      281
      192.168.253.255      255.255.255.255      On-link      192.168.253.1      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      192.168.253.1      281
      224.0.0.0      240.0.0.0      On-link      192.168.1.5      291
      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      192.168.253.1      281
      255.255.255.255      255.255.255.255      On-link      192.168.1.5      291
=====
Route permanenti:
Nessuna
```

Dopo essere entrato come amministratore vado a digitare il comando netstat -abno dal prompt

```
PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto Indirizzo locale          Indirizzo esterno          Stato      PID
TCP    0.0.0.0:135                  0.0.0.0:0                 LISTENING  908
RpcSs
[svchost.exe]
TCP    0.0.0.0:445                  0.0.0.0:0                 LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:5040                 0.0.0.0:0                 LISTENING  1152
CDPSvc
[svchost.exe]
TCP    0.0.0.0:49664               0.0.0.0:0                 LISTENING  688
[lsass.exe]
TCP    0.0.0.0:49665               0.0.0.0:0                 LISTENING  524
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666               0.0.0.0:0                 LISTENING  844
EventLog
[svchost.exe]
TCP    0.0.0.0:49667               0.0.0.0:0                 LISTENING  400
Schedule
[svchost.exe]
TCP    0.0.0.0:49668               0.0.0.0:0                 LISTENING  1860
[spoolsv.exe]
TCP    0.0.0.0:49669               0.0.0.0:0                 LISTENING  664
Impossibile ottenere informazioni sulla proprietà
TCP    [::]:135                    [::]:0                    LISTENING  908
RpcSs
[svchost.exe]
TCP    [::]:445                    [::]:0                    LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    [::]:49664                  [::]:0                    LISTENING  688
[lsass.exe]
TCP    [::]:49665                  [::]:0                    LISTENING  524
Impossibile ottenere informazioni sulla proprietà
TCP    [::]:49666                  [::]:0                    LISTENING  844
EventLog
[svchost.exe]
TCP    [::]:49667                  [::]:0                    LISTENING  400
Schedule
[svchost.exe]
TCP    [::]:49668                  [::]:0                    LISTENING  1860
[spoolsv.exe]
TCP    [::]:49669                  [::]:0                    LISTENING  664
Impossibile ottenere informazioni sulla proprietà
UDP    0.0.0.0:5050                *:0                        LISTENING  1152
CDPSvc
[svchost.exe]
UDP    127.0.0.1:1900               *:0                        LISTENING  1604
SSDPSSRV
[svchost.exe]
UDP    127.0.0.1:49664             *:0                        LISTENING  400
iphlpvc
[svchost.exe]
UDP    127.0.0.1:49666             *:0                        LISTENING  1604
SSDPSSRV
[svchost.exe]
UDP    [::]:1900                   *:0                        LISTENING  1604
SSDPSSRV
```

Aprendo il Task manager seleziono la parte dettagli e metto in ordine i vari PID e possiamo notare sul PID n. 688 è associato il processo lsass.exe che ha come nome utente SYSTEM e utilizza una memoria pari a 4.220k.

Gestione attività

File Opzioni Visualizza

Processi	Prestazioni	Cronologia applicazioni	Avvio	Utenti	Dettagli	Servizi
Nome	PID	Stato	Nome utente	CPU	Memoria (...)	Virtualizzazion...
smss.exe	344	In esecuzione	SYSTEM	00	104 K	Non consentito
svchost.exe	400	In esecuzione	SYSTEM	00	66.260 K	Non consentito
svchost.exe	404	In esecuzione	SYSTEM	00	15.400 K	Non consentito
csrss.exe	448	In esecuzione	SYSTEM	00	680 K	Non consentito
wininit.exe	524	In esecuzione	SYSTEM	00	456 K	Non consentito
csrss.exe	536	In esecuzione	SYSTEM	03	680 K	Non consentito
winlogon.exe	620	In esecuzione	SYSTEM	00	804 K	Non consentito
services.exe	664	In esecuzione	SYSTEM	00	3.172 K	Non consentito
sihost.exe	676	In esecuzione	User	03	3.348 K	Disabilitato
lsass.exe	688	In esecuzione	SYSTEM	00	4.220 K	Non consentito
svchost.exe	700	In esecuzione	SYSTEM	00	38.136 K	Non consentito
svchost.exe	744	In esecuzione	SERVIZIO LOCALE	00	6.132 K	Non consentito
svchost.exe	788	In esecuzione	SYSTEM	00	5.880 K	Non consentito
fontdrvhost.exe	796	In esecuzione	UMFD-0	00	316 K	Disabilitato
svchost.exe	844	In esecuzione	SERVIZIO LOCALE	00	11.204 K	Non consentito
RuntimeBroker.exe	852	In esecuzione	User	00	1.276 K	Disabilitato

5) Svuotiamo ora il cestino tramite il comando clear-recyclebin dal prompt PowerShell per svuotare il cestino.

```
PS C:\Windows\system32> 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:\Windows\system32>
```