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 notimao che le interfacce sono simili mostrandoti 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
                                     .VirtualBox
                     <DIR>
                                    Cisco Packet Tracer 8.2.2
21/02/2025
            19:10
                     <DIR>
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
                                     Tracing
            12:30
                     <DIR>
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.

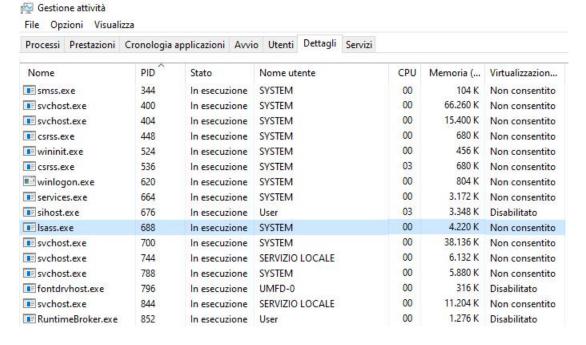
4) Netstat con Powershell. Digitiamo netstat -r e visualizziamo l' elenco interfaccia e la tabella di route lpv4 notando che il Gateway risulta 192.168.1.1

```
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
                                                     Interfaccia Metrica
                             Mask
                                          Gateway
                         0.0.0.0
                                     192.168.1.1
         0.0.0.0
                                                    192.168.1.5
                                                                   35
                                       On-link
       127.0.0.0
                       255.0.0.0
                                                      127.0.0.1
                                                                  331
                 255.255.255.255
       127.0.0.1
                                       On-link
                                                      127.0.0.1
                                                                  331
 127.255.255.255
                 255.255.255.255
                                                      127.0.0.1
                                       On-link
                                                                  331
                  255.255.255.0
     192.168.1.0
                                       On-link
                                                    192.168.1.5
                                                                  291
                                       On-link
     192.168.1.5
                 255.255.255.255
                                                    192.168.1.5
                                                                  291
                                       On-link
   192.168.1.255
                 255.255.255.255
                                                    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
                                       On-link
       224.0.0.0
                       240.0.0.0
                                                      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
                                                   127.0.0.1
192.168.253.1
 255.255.255.255
                 255.255.255.255
                                       On-link
                                                                  331
                 255.255.255.255
  255.255.255.255
                                       On-link
                                                                  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

Proto Indirizzo locale	05 5 111/		- American			
Proto Indirizzo locale	PS C:\Windows\s	ystem32> netstat				
RpcSS Esvenost.exe TCP 0.0.0.445 0.0.0.0:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0:5040 0.0.0.0:0 LISTENING 1152 CDPSvc Svchost.exe TCP 0.0.0:49664 0.0.0.0:0 LISTENING 688 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0:49665 0.0.0.0:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0:49666 0.0.0.0:0 LISTENING 844 Eventlog Svchost.exe TCP 0.0.0:49667 0.0.0:0:0 LISTENING 400 Schedule Svchost.exe TCP 0.0.0:49667 0.0.0:0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0:49669 0.0.0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0:49669 0.0.0:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):4964 (::):0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49666 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49667 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49668 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49668 (::):0 LISTENING 1860 Spoolsv.exe TCP (::):49669 (::):0 LISTENING 1860 Spoolsv.exe TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 TCP (::):49669 (::):0 LISTENING 664 TCP (::):49669 (::):0 LISTENING CEP TCP (::):49669 (::)	Connessioni attive					
RpcSs Esvenost.exe TCP 0.0.0.445 0.0.0.00 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0.0:5040 0.0.0.00 LISTENING 1152 CDPSvc Svchost.exe TCP 0.0.0.0:49664 0.0.0.00 LISTENING 688 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0.0:49665 0.0.0.00 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0.0:49666 0.0.0.00 LISTENING 844 Eventlog Svchost.exe TCP 0.0.0.0:49667 0.0.0.00 LISTENING 400 Schedule Svchost.exe TCP 0.0.0.0:49667 0.0.0.00 LISTENING 400 Schedule Svchost.exe TCP 0.0.0.0:49668 0.0.0.00 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):135 (::):0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49666 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49667 (::):0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP (::):49668 (::):0 LISTENING 844 Eventlog Svchost.exe TCP (::):49668 (::):0 LISTENING 1860 Spoolsv.exe TCP (::):49669 (::):0 LISTENING 1860 Spoolsv.exe TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 (::):0 LISTENING 664 TCP (::):49669 (::):0 LISTENING 1860 LISTENING	Proto Indiri	zzo locale	Indirizzo esterno	Stato		
[sychost.exe]	TCP 0.0.0.	0:135	0.0.0.0:0	LISTENING	908	
TCP 0.0.0.6.1445 0.0.0.0:0 LISTENING 4 Impossible ottenere informazioni sulla proprietà TCP 0.0.0.0:5940 0.0.0.0:0 LISTENING 1152 CDPSvc Esvenost.exe TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà 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 (:):1:495 [:]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP (:):1:49664 [:]:0 LISTENING 688 LISTENING CISTENING CIS						
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 524 Impossibile ottenere informazioni sulla proprietà TCP 0.0.0.0:49666 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 Schedule Svchost.exe] TCP (:]:49664 [:]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP [:]:49664 [:]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP [:]:49664 [:]:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP [:]:49666 [:]:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP [:]:49666 [:]:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP [:]:49666 [:]:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP [:]:49667 [:]:0 LISTENING 1860 Schedule Svchost.exe TCP [:]:49668 [:]:0 LISTENING 1860 Spoolsv.exe TCP [:]:49669 [:]:0 LISTENING 1860 Spoolsv.exe TCP [:]:49669 [:]:0 LISTENING 664 TCP [:]:49669 [:]:0 LISTENING 1860 Spoolsv.exe TCP [:]:49669 [:]:0 LISTENING 186	TCP 0.0.0.			LISTENING		
CDPSVC Syvinost.exe TCP 0.0.0.149664 0.0.0.0:0 LISTENING 688 Classs.exe TCP 0.0.0.0.149665 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 Esvenost.exe TCP 0.0.0.149667 0.0.0.0:0 LISTENING 400 Schedule Svinost.exe TCP 0.0.0.149668 0.0.0.0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0.149669 0.0.0.0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0.149669 0.0.0:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP (:):135 [:]:0 LISTENING 908 Rocks Svinost.exe TCP (:):1454 [:]:0 LISTENING 4 LISTENING 524 TCP (:):149664 [::]:0 LISTENING 524 TCP (:):149666 [::]:0 LISTENING 524 TCP (:):149666 [::]:0 LISTENING S44 Eventlog Svinost.exe TCP (:):149667 [::]:0 LISTENING S44 Eventlog Svinost.exe TCP (:):149667 [::]:0 LISTENING S44 Eventlog Svinost.exe TCP (:):149668 [::]:0 LISTENING S68 Spoolsv.exe TCP (:):149667 [::]:0 LISTENING S68 Spoolsv.exe TCP (:):149669 [::]:0 LISTENING S64 Spoo	Impossibile ottenere informazioni sulla proprietà				****	
Sychost.exe	CDPSvc	0:5040	0.0.0.0:0	LISTENING	1152	
	[svchost.exe]					
TCP 0.0.0.0.49665 0.0.0.00 LISTENING 524 Impossible ottenere informazioni sulla proprietà TCP 0.0.0.0:49666 0.0.0.00 LISTENING 844 EventLog [swchost.exe] TCP 0.0.0.0:49667 0.0.0.00 LISTENING 1860 [spoolsv.exe] TCP 0.0.0.0:49668 0.0.0.00 LISTENING 1860 [spoolsv.exe] TCP 0.0.0.0:49669 0.0.0.00 LISTENING 664 Impossible ottenere informazioni sulla proprietà TCP [::]:435 [::]:0 LISTENING 908 Rocss [swchost.exe] TCP [::]:446 [::]:0 LISTENING 4 Impossible ottenere informazioni sulla proprietà TCP [::]:49664 [::]:0 LISTENING 688 [lass.exe] TCP [::]:49666 [::]:0 LISTENING 888 [lass.exe] TCP [::]:49666 [::]:0 LISTENING 844 EventLog [swchost.exe] TCP [::]:49667 [::]:0 LISTENING 844 EventLog [swchost.exe] TCP [::]:49668 [::]:0 LISTENING 400 Schedule [svchost.exe] TCP [::]:49668 [::]:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà TCP [::]:49667 [::]:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà TCP [::]:49667 [::]:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà TCP [::]:49667 [::]:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà UDP 1::49669 [::]:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà UDP 0.0.0:5950 *:* UDP 127.0.0:1:1900 *:* SSDPSNV [swchost.exe] UDP 127.0.0:1:1906 *:* SSDPSNV [swchost.exe] UDP 127.0.0:1:49664 *:*		0:49664	0.0.0.0:0	LISTENING	688	
Impossibile ottenere informazioni sulla proprietà ISTENING 844 Eventlog Events Ev		a · 49665	0 0 0 0 0	LISTENING	524	
TCP 0.0.0.49666 0.0.0.0:0 LISTENING 844 Eventlog Svchost.exe TCP 0.0.0.49667 0.0.0.0:0 LISTENING 400 Schedule Svchost.exe TCP 0.0.0.49668 0.0.0.0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0.49668 0.0.0.0:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà TCP 1:1:135 Si:10 LISTENING 508 Spoolsv.exe TCP 1:1:49664 I:10 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP I:1:49664 I:10 LISTENING 688 LISTENING 524 Impossibile ottenere informazioni sulla proprietà TCP I:1:49665 I:10 LISTENING 524 LISTENING Spoolsv.exe TCP I:1:49667 I:10 LISTENING S44 Eventlog Svchost.exe TCP I:1:49667 I:10 LISTENING S44 Schedule Svchost.exe TCP I:1:49668 I:10 LISTENING Soolsv.exe TCP I:1:49669 I:10 LISTENING S64 TCP I:1:49669 I:10 LISTENING S64 TCP I:1:49669 I:10 LISTENING S64 TCP TC	Impossibile ot	tenere informazi	oni sulla proprietà	LIDILINI		
Svchost_exe	TCP 0.0.0.			LISTENING	844	
TCP 0.0.0.0.049667 0.0.0.0:0 LISTENING 400 Schedule [svchost.exe] TCP 0.0.0.049668 0.0.0.0:0 LISTENING 1860 [spoolsv.exe] TCP 0.0.0.049668 0.0.0.0:0 LISTENING 664 Impossible ottenere informazioni sulla proprietà TCP (::):135 [::]:0 LISTENING 908 RocSs [svchost.exe] TCP (::):445 [::]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP (::):49664 [::]:0 LISTENING 524 Impossibile ottenere informazioni sulla proprietà 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 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 [::]:0 LISTENING 1860 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 [::]:0 LISTENING 1860 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 [::]:0 LISTENING 1860 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 [::]:0 LISTENING 1860 Impossibile ottenere informazioni sulla proprietà TCP (::):49669 [::]:0 LISTENING 1152 CDP 0.0.0.0:5050 *:* TCP (::):49664 TCP (::):49664 TCP (::):49664 TCP (::):49665 TCP (::):49669						
Schedule		0:49667	0.0.0.0:0	LISTENING	400	
TCP 0.0.0.49668 0.0.0.0:0 LISTENING 1860 Spoolsv.exe TCP 0.0.0.49659 0.0.0.0:0 LISTENING 664 LISTENING 665 LISTENING 666 LISTENING CISTENING CISTENIN						
[spoolsv.exe]			0.0.0.0		4000	
TCP 0.0.0.1949669 0.0.0.00 Impossibile ottenere informazioni sulla proprietà TCP [::]:435 [::]:0 LISTENING 908 RpcSs Rpc		0:49668	0.0.0.0:0	LISTENING	1800	
TCP [::]:135 [::]:0 LISTENING 908 RpcSs [svchost.exe] TCP [::]:445 [::]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP [::]:49664 [::]:0 LISTENING 688 [lasss.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 0.0.0:5050 *:* UDP 127.0.0.1:1900 *:* SSDPSKV [svchost.exe] UDP 127.0.0.1:1900 *:* SSDPSKV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 Implayer	TCP 0.0.0.			LISTENING	664	
RpcSs					***	
[svchost.exe] TCP [::]:445 [::]:0 LISTENING 4 Impossibile ottenere informazioni sulla proprietà TCP [::]:49664 [::]:0 LISTENING 688 [lasss.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 [::]:49668 [::]:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà UDP 0.0.0:5050 *:* UDP 127.0.0.1:1900 *:* SSDPSNV [svchost.exe] UDP 127.0.0.1:1906 *:* SSDPSNV [svchost.exe] UDP 127.0.0.1:49664 *:*		35	[::]:0	LISTENING	908	
Impossibile ottenere informazioni sulla proprietà ISTENING 688	[sychost eyel					
TCP [::]:49664 [::]:0 LISTENING 688 [lasss.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 [::]:49668 [::]:0 LISTENING 1860 Impossibile ottenere informazioni sulla proprietà UDP 0.0.0:5050 *:* CDPSvc [svchost.exe] UDP 127.0.0:1:1900 *:* SSDPSRV [svchost.exe] UDP 127.0.0:1:49664 *:* 400 iphlpsvc				LISTENING		
	Impossibile of	tenere informazi 9664		LISTENING	688	
Impossibile ottenere informazioni sulla proprietà ITCP [::]:49666 [::]:0 LISTENING 844 EventLog			[].0	LISTENING	000	
TCP [::]:49666 [::]:0 LISTENING 844 Eventlog [swchost.exe] TCP [::]:49667 [::]:0 LISTENING 400 Schedule [swchost.exe] TCP [::]:49668 [::]:0 LISTENING 1860 [spoolsv.exe] TCP [::]:49668 [::]:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà UDP 0.0.0:5050 *:*	TCP [::]:4	9665		LISTENING	524	
Eventlog [Svchost.exe] TCP [::]:49667 [::]:0 LISTENING 400 Schedule [Svchost.exe] TCP [::]:49668 [::]:0 LISTENING 1860 [Spoolsv.exe] TCP [::]:49668 [::]:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà UDP 0.0.0.0:5050 *:* 1152 CDPSvc [svchost.exe] UDP 127.0.0.1:1900 *:* 1604 SSDPSRV [Svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc				LICTENTING	944	
Svchost.exe TCP [::]:49667 [::]:0	EventLog	3000	[].0	LISTENING	044	
Schedule	[sychost.exe]					
[svchost.exe] ICP [::]:49668 [::]:0 LISTENING 1860 [spoolsv.exe] ICP [::]:49669 [::]:0 LISTENING 664 IMpossable ottenere informazioni sulla proprietà UDP 0.0.0.0:5050 *:* 1152 CDPSvc [svchost.exe] UDP 127.0.0.1:1900 *:* 1604 SSDPSRV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc		9667	[::]:0	LISTENING	400	
TCP [::]:49668 [::]:0 LISTENING 1860 [spoolsv.exe] TCP [::]:49669 [::]:0 LISTENING 664 Impossibile ottenere informazioni sulla proprietà UDP 0.0.0:0556 *:* 1152 UDP 0.0.0:0556 *:* 1152 UDP 127.0.0:1:1900 *:* 1604 UDP 127.0.0:1:1900 *:* 1604 UDP 127.0.0:1:49664 *:* 400 UDP 127.0.0:1:49664 UDP 127.0.0:1:49664						
[spoolsv.exe]	TCP [::]:4		[::]:0	LISTENING	1860	
Impossibile ottenere informazioni sulla proprietà UDP 0.0.0.0:5550 *:* 1152 CDPSvc [svchost.exe] UDP 127.0.0.1:1900 *:* 1604 SSDPSRV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc 400	[spoolsv.exe]		51.0	LICTENTING	664	
UDP 0.0.0.0:5050 *:* 1152 CDPSvc CDPSvc [svchost.exe]					bb4	
[svchost.exe] UDP 127.0.0.1:1900 *:* 1604 SSDPSRV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc	UDP 0.0.0.0:5050 *:*				1152	
UDP 127.0.0.1:1900 *:* 1604 SSDPSNV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc						
SSDPSRV [svchost.exe] UDP 127.0.0.1:49664 *:* 400 iphlpsvc		0 1:1900	***		1604	
UDP 127.0.0.1:49664 *:* 400 iphlpsvc		01111100				
iphlpsvc						
		0.1:49664	*12		400	
I SVCNOST. exe	[svchost.exe]					
UDP 127.0.0.1:49666 *:* 1604	UDP 127.0.	0.1:49666			1604	
SSDPSRV						
[svchost.exe] UDP [::1]:1900 *:* 1604		1900	*;*		1604	
SSDPSRV		100000000			366275-0	

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 Isass.exe che ha come nome utente SYSTEM e utilizza una memoria pari a 4.220k.



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] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S

PS C:\Windows\system32>
```