

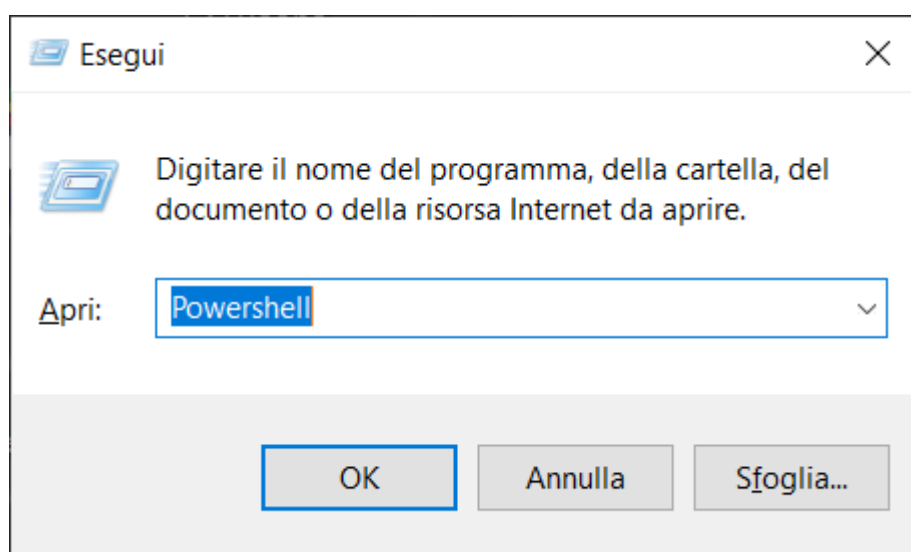
Esplorazione Windows Powershell

Laboratorio sull'uso di Windows PowerShell: Un approccio tecnico approfondito

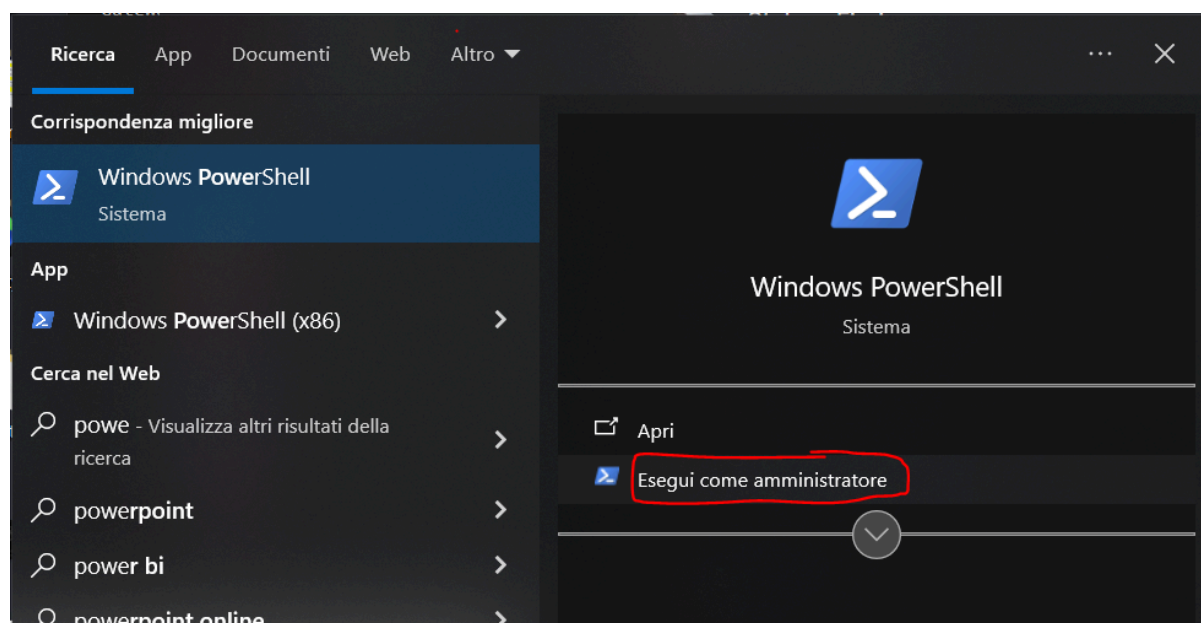
PowerShell è più di una semplice shell di comando: è un ambiente di scripting avanzato progettato per semplificare e potenziare la gestione di sistemi e applicazioni. In questo laboratorio, ti guideremo attraverso una serie di attività pratiche che metteranno in luce le sue funzionalità principali.

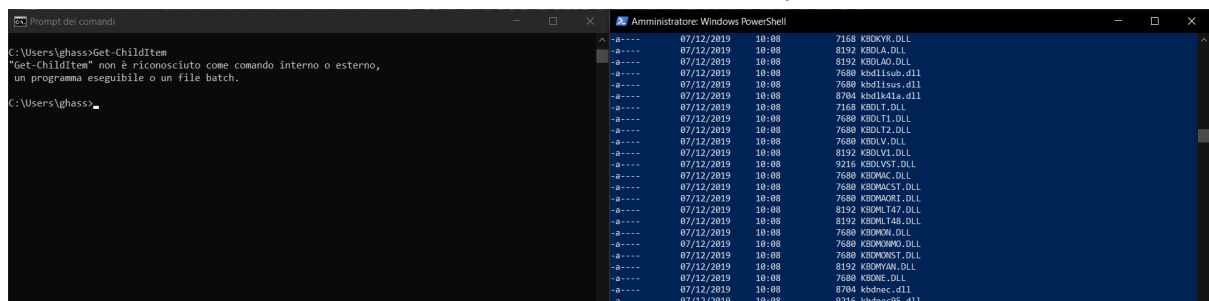
Parte 1: Accedere alla console di PowerShell

1. Avvia PowerShell:
 - Premi **Win + S**, digita PowerShell e premi Invio.



- Per compiti amministrativi, fai clic con il tasto destro su Windows PowerShell e seleziona Esegui come amministratore.





Parte 3: Esplora i cmdlet

I cmdlet sono comandi predefiniti di PowerShell progettati per eseguire operazioni specifiche in modo efficiente. Seguono una struttura standard verbo-sostantivo (es. `Get-Process`) e restituiscono oggetti anziché testo, consentendo una manipolazione avanzata dei dati.

Elenco di tutti i cmdlet disponibili:

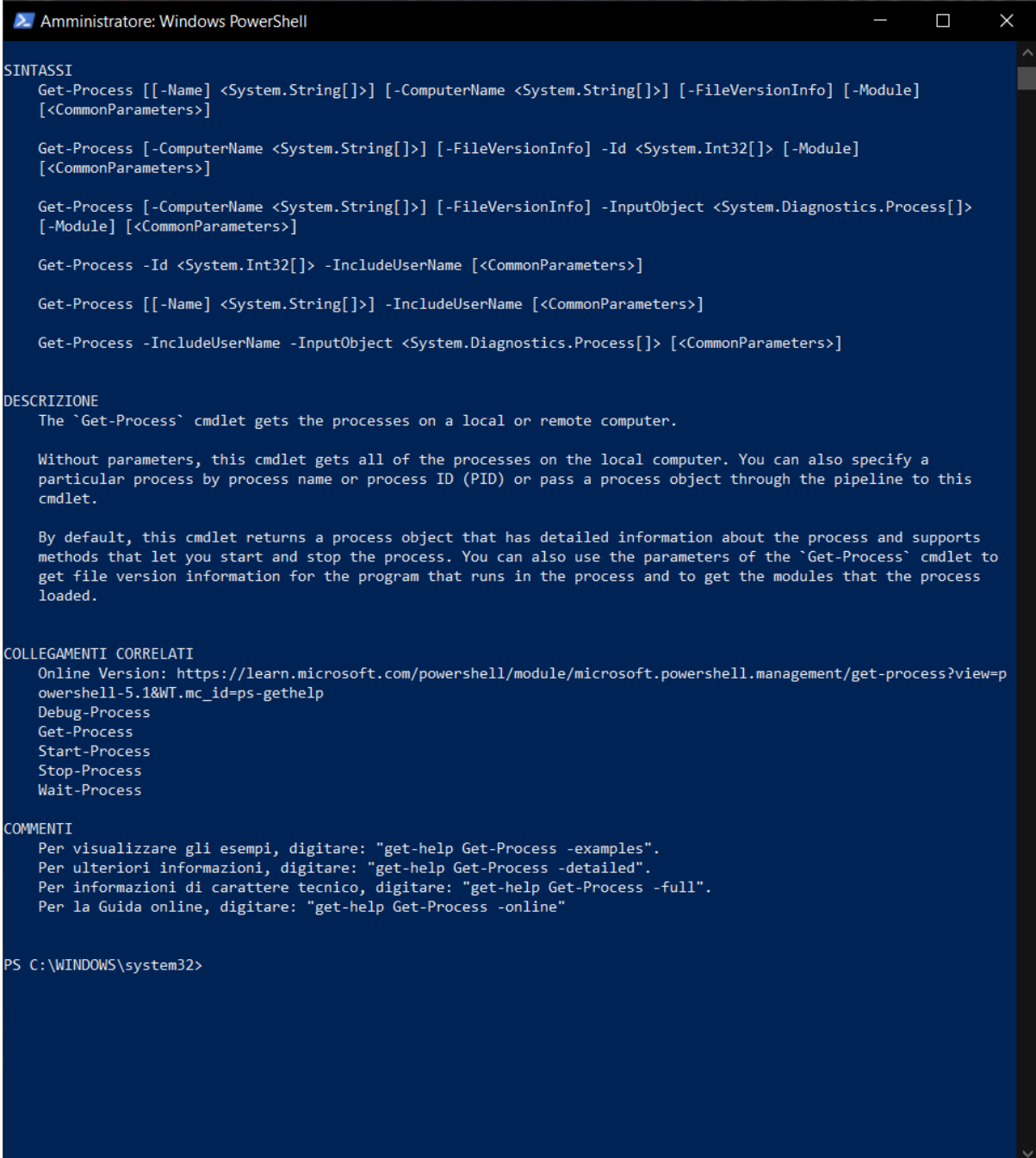
Get-Command



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-ProvisionedAppPackage	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-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Dismount-AppPackageVolume	2.0.1.0	Appx
Alias	Enable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Enable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Flush-Volume	2.0.0.0	Storage
Alias	Get-AppPackage	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-Language	1.0	LanguagePackManagement
Alias	Get-PhysicalDiskSNV	2.0.0.0	Storage
Alias	Get-PreferredLanguage	1.0	LanguagePackManagement
Alias	Get-ProvisionedAppPackage	3.0	Dism
Alias	Get-ProvisionedAppxPackage	3.0	Dism
Alias	Get-StorageEnclosureSNV	2.0.0.0	Storage
Alias	Get-SystemLanguage	1.0	LanguagePackManagement
Alias	Initialize-Volume	2.0.0.0	Storage
Alias	Mount-AppPackageVolume	2.0.1.0	Appx
Alias	Move-AppPackage	2.0.1.0	Appx
Alias	Move-SmbClient	2.0.0.0	SmbWitness
Alias	Optimize-AppProvisionedPackages	3.0	Dism
Alias	Optimize-ProvisionedAppPackages	3.0	Dism
Alias	Optimize-ProvisionedAppxPackages	3.0	Dism
Alias	Remove-AppPackage	2.0.1.0	Appx
Alias	Remove-AppPackageVolume	2.0.1.0	Appx
Alias	Remove-AppProvisionedPackage	3.0	Dism
Alias	Remove-EtwTraceSession	1.0.0.0	EventTracingManagement
Alias	Remove-ProvisionedAppPackage	3.0	Dism
Alias	Remove-ProvisionedAppxPackage	3.0	Dism
Alias	Remove-ProvisioningPackage	3.0	Provisioning
Alias	Remove-TrustedProvisioningCertificate	3.0	Provisioning
Alias	Set-AppPackageDefaultVolume	2.0.1.0	Appx
Alias	Set-AppPackageProvisionedDataFile	3.0	Dism
Alias	Set-AutoLoggerConfig	1.0.0.0	EventTracingManagement
Alias	Set-EtwTraceSession	1.0.0.0	EventTracingManagement

Ottieni informazioni su un cmdlet specifico: Ad esempio, per il cmdlet `Get-Process`:

`Get-Help Get-Process`



```
Amministratore: Windows PowerShell

SINTASSI
Get-Process [[-Name] <System.String[]>] [-ComputerName <System.String[]>] [-FileVersionInfo] [-Module]
[<CommonParameters>]

Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -Id <System.Int32[]> [-Module]
[<CommonParameters>]

Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -InputObject <System.Diagnostics.Process[]>
[-Module] [<CommonParameters>]

Get-Process -Id <System.Int32[]> -IncludeUserName [<CommonParameters>]

Get-Process [[-Name] <System.String[]>] -IncludeUserName [<CommonParameters>]

Get-Process -IncludeUserName -InputObject <System.Diagnostics.Process[]> [<CommonParameters>]

DESCRIZIONE
The 'Get-Process' cmdlet gets the processes on a local or remote computer.

Without parameters, this cmdlet gets all of the processes on the local computer. You can also specify a
particular process by process name or process ID (PID) or pass a process object through the pipeline to this
cmdlet.

By default, this cmdlet returns a process object that has detailed information about the process and supports
methods that let you start and stop the process. You can also use the parameters of the 'Get-Process' cmdlet to
get file version information for the program that runs in the process and to get the modules that the process
loaded.

COLLEGAMENTI CORRELATI
Online Version: https://learn.microsoft.com/powershell/module/microsoft.powershell.management/get-process?view=powershell-5.1&WT.mc\_id=ps-gethelp
Debug-Process
Get-Process
Start-Process
Stop-Process
Wait-Process

COMMENTI
Per visualizzare gli esempi, digitare: "get-help Get-Process -examples".
Per ulteriori informazioni, digitare: "get-help Get-Process -detailed".
Per informazioni di carattere tecnico, digitare: "get-help Get-Process -full".
Per la Guida online, digitare: "get-help Get-Process -online"

PS C:\WINDOWS\system32>
```

Esempio pratico con **Get-Process**: Visualizza tutti i processi attivi sul sistema:

Get-Process

Amministratore: Windows PowerShell

PS C:\WINDOWS\system32> Get-process

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
439	20	7948	15056	9,14	2948	0	AppHelperCap
471	27	26544	34448	0,16	19788	5	ApplicationFrameHost
208	12	7816	14164	16,48	14204	0	audiodg
578	26	55984	59368	3,30	6360	5	BlueStacksServices
272	16	21948	49396	0,19	16196	5	BlueStacksServices
797	33	58932	86024	143,44	20224	5	BlueStacksServices
286	16	14596	45308	2,91	23716	5	BlueStacksServices
515	38	46448	2416	0,17	23888	5	CalculatorApp
426	20	5576	19520	9,41	2472	5	CiscoCollabHost
724	51	135844	709364	142,28	9104	5	CiscoCollabHost
1139	147	595764	310180	2.292,88	15304	5	CiscoCollabHost
80	5	2392	4984	0,00	11048	5	cmd
144	7	1764	8804	0,02	4596	5	CompPkgSrv
108	7	6240	5636	0,02	12576	0	conhost
273	14	6996	20232	10,72	18156	5	conhost
305	14	8000	21548	0,39	18904	5	conhost
764	25	2296	2460	4,19	740	0	csrss
870	28	3400	7096	51,30	17456	5	csrss
546	17	5080	23792	5,92	7192	5	ctfmon
450	19	8632	13360	8,28	5640	0	dasHost
112	8	2052	4036	0,39	6668	0	dasHost
298	15	14588	3664	2,28	2916	0	DiagsCap
292	16	12644	79012	1,08	4348	5	Discord
645	29	143708	115168	262,00	10232	5	Discord
1603	48	115284	108332	76,61	15672	5	Discord
196	12	11028	32308	0,02	16216	5	Discord
1175	83	331332	314432	756,73	20000	5	Discord
383	19	17212	53432	19,59	21740	5	Discord
281	16	4604	14136	0,23	13192	5	dllhost
213	11	7452	5824	2,30	4928	0	DtsApo4Service
1560	55	147308	97820	2.999,44	14820	5	dwm
4806	122	368740	217596	125,56	22168	5	explorer
50	6	1560	1020	0,00	552	0	fontdrvhost
50	12	5536	8424	0,25	7940	5	fontdrvhost
813	14	6700	9960	4,78	5044	0	HPPrintScanDoctorService
95	6	1364	2056	1,14	4936	0	ibtsiva
0	0	60	8		0	0	Idle
506	31	19216	7416	2,45	4944	0	IntelAudioService
140	8	1308	1128	0,00	5108	0	jhi_service
211	11	3224	2656	0,25	3936	0	LMS
671	31	49448	53224	0,80	18852	5	LockApp
1617	30	13128	19876	505,03	916	0	lsass
0	0	1384	334840	545,64	2668	0	Memory Compression
612	41	53948	2436	0,20	11636	5	Microsoft.Media.Player
557	20	26024	28812	6,31	5692	0	MoUsoCoreWorker
274	20	22444	44924	0,27	924	5	msedge
584	35	100824	150972	27,63	928	5	msedge
825	35	111128	156204	35,84	1040	5	msedge
297	20	26536	52720	0,45	4340	5	msedge
676	61	289344	341968	96,05	4640	5	msedge
209	17	15112	29316	0,05	4716	5	msedge

Parte 4: Esplora il comando netstat utilizzando PowerShell

Il comando **netstat** (Network Statistics) è uno strumento utile per monitorare le connessioni di rete e le porte in uso sul sistema. Può essere eseguito direttamente all'interno di PowerShell per ottenere informazioni dettagliate sulla rete.

1. Visualizzare i comandi disponibili

Esegui il comando seguente in PowerShell per ottenere l'elenco completo delle opzioni di **netstat**:

netstat -h

```
PS C:\WINDOWS\system32> 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'eleggibile 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'eleggibile
            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
            visualizzate 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 omissa, netstat stamperà il
            informazioni di configurazione una volta.
```

2. Esempi pratici con netstat

Tabella di routing attiva

La tabella di routing è una struttura che indica come un sistema instrada i pacchetti di rete verso le destinazioni. Contiene righe con informazioni su:

1. Destinazione: L'indirizzo IP o la rete di destinazione.
2. Gateway: L'indirizzo del router o dispositivo attraverso cui passano i pacchetti.
3. Interfaccia: L'adattatore di rete utilizzato (es. Ethernet o Wi-Fi).
4. Metriche: Priorità del percorso, dove valori più bassi indicano percorsi preferiti.

Si visualizza con `netstat -r`

```
Amministratore: Windows PowerShell

PS C:\WINDOWS\system32> netstat -r

=====
Elenco interfacce
 4...6c 02 e0 79 01 fe .....Realtek Gaming GbE Family Controller
12...0a 00 27 00 00 0c .....VirtualBox Host-Only Ethernet Adapter
 3...08 5b d6 5d de 60 .....Microsoft Wi-Fi Direct Virtual Adapter
 7...0a 5b d6 5d de 5f .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...08 5b d6 5d de 5f .....Intel(R) Wi-Fi 6 AX201 160MHz
16...08 5b d6 5d de 63 .....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    192.168.43.1 192.168.43.40 50
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
192.168.43.0         255.255.255.0   On-link      192.168.43.40 306
192.168.43.40        255.255.255.255  On-link      192.168.43.40 306
192.168.43.255       255.255.255.255  On-link      192.168.43.40 306
192.168.56.0         255.255.255.0   On-link      192.168.56.1  281
192.168.56.1        255.255.255.255  On-link      192.168.56.1  281
192.168.56.255       255.255.255.255  On-link      192.168.56.1  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      192.168.56.1  281
224.0.0.0            240.0.0.0      On-link      192.168.43.40 306
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      192.168.56.1  281
255.255.255.255      255.255.255.255  On-link      192.168.43.40 306
=====
Route permanenti:
 Nessuna

IPv6 Tabella route
=====
Route attive:
 Interf Metrica Rete Destinazione Gateway
 1      331  ::1/128              On-link
12      281 fe80::/64             On-link
14      306 fe80::/64             On-link
12      281 fe80::651f:3774:9fb2:2e47/128
                                On-link
14      306 fe80::9108:12af:d6b:ddc7/128
                                On-link
 1      331 ff00::/8              On-link
12      281 ff00::/8              On-link
14      306 ff00::/8              On-link
=====
Route permanenti:
 Nessuna
PS C:\WINDOWS\system32>
```


Il comando **netstat -abno** fornisce informazioni dettagliate sulle connessioni di rete attive, includendo:

1. -a: Mostra tutte le connessioni e le porte in ascolto.
2. -b: Mostra il nome del processo associato a ciascuna connessione (richiede privilegi amministrativi).
3. -n: Visualizza gli indirizzi IP e le porte in formato numerico, evitando la risoluzione dei nomi.
4. -o: Aggiunge l'ID del processo (PID) associato a ciascuna connessione.

Questo comando è utile per mostrare quale processo (e il relativo nome) sta utilizzando una connessione di rete, utile per individuare applicazioni sospette o non autorizzate.

The screenshot displays three windows from a Windows system:

- Windows PowerShell (Administrator):** Shows the output of the command `netstat -abno`. The output lists active connections with columns for Protocol, Local Address, Foreign Address, State, and PID. It shows various processes like `svchost.exe`, `RuntimeBroker.exe`, and `SearchApp.exe`.
- Task Manager:** Shows the 'Processes' tab, listing running applications and their PIDs. It highlights `svchost.exe` with PID 1084.
- Properties - svchost:** A window showing the details of the `svchost.exe` process. It includes the file path `C:\Windows\System32\svchost.exe`, the description 'Process host for Windows services', and the creation/modification dates.

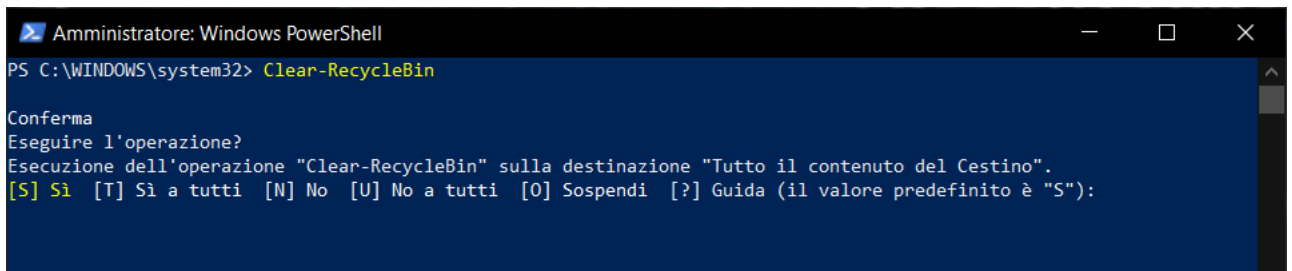
Parte 5: Svuotare il cestino utilizzando PowerShell.

Il cmdlet `Clear-RecycleBin` in PowerShell è utilizzato per svuotare il Cestino di Windows. Questo comando è utile per automatizzare la pulizia dei file eliminati, liberando spazio su disco senza dover interagire manualmente con l'interfaccia grafica.

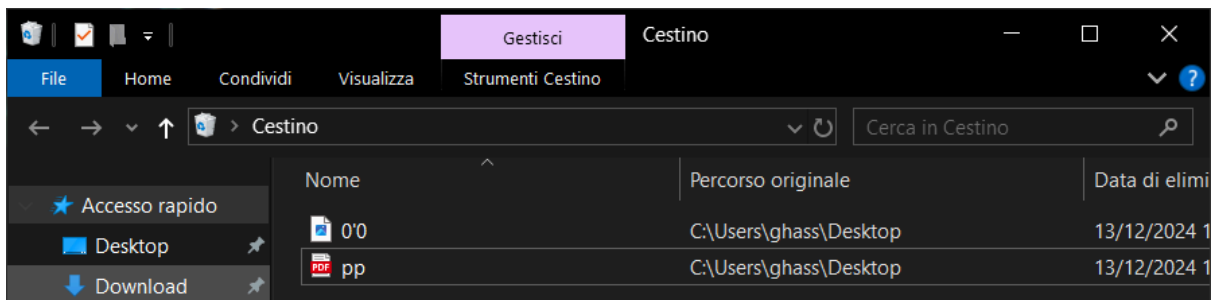
Sintassi di base:

`Clear-RecycleBin`

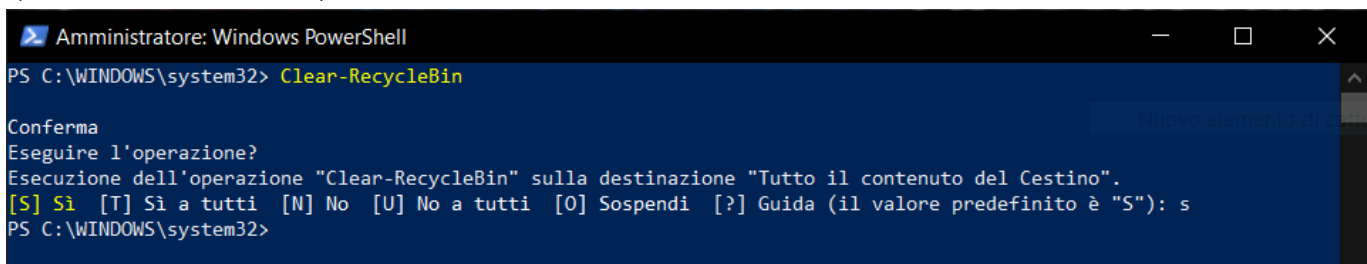
- 1) Richiesta di conferma da parte di Powershell



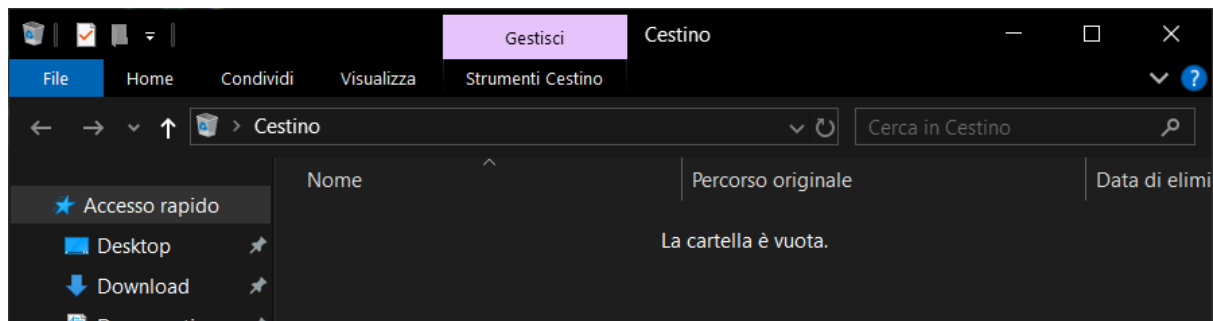
- 2) Controllo file da svuotare



- 3) Confermiamo l'operazione con s se siamo sicuri di eliminare il file



4) Verifichiamo l'eliminazione dei file



Utilizzo e vantaggi:

- Automazione: Permette di svuotare il Cestino automaticamente tramite script, utile per amministratori di sistema o per operazioni pianificate.
- Risparmio di spazio: Aiuta a liberare spazio su disco rimuovendo permanentemente i file nel Cestino.

Questo comando è particolarmente utile in ambienti aziendali o su server dove è necessario gestire regolarmente lo spazio di archiviazione senza interventi manuali.

Nota

Il cmdlet **Clear-RecycleBin** è disponibile solo su versioni più recenti di PowerShell (Windows PowerShell 5.1 o versioni superiori)

Domanda di riflessione

PowerShell offre numerosi comandi utili per semplificare le operazioni di un analista di sicurezza. Ad esempio, **Get-EventLog** permette di recuperare e analizzare i log degli eventi di sistema, utile per rilevare attività sospette. Con **Get-Process**, è possibile monitorare i processi in esecuzione e identificare quelli non autorizzati. **Get-NetTCPConnection** consente di visualizzare le connessioni di rete attive, utile per individuare traffico anomalo. **Set-ExecutionPolicy** è fondamentale per gestire le politiche di esecuzione degli script e proteggere il sistema da script dannosi. Infine, **Invoke-Command** permette di eseguire comandi su macchine remote, facilitando la gestione di più sistemi in contemporanea. Questi comandi sono essenziali per ottimizzare il monitoraggio e la gestione della sicurezza.