# Relazione – Laboratorio su PowerShell

Durante questo laboratorio ho avuto modo di usare PowerShell. L'obiettivo principale era quello di esplorare alcuni comandi base, imparare a raccogliere informazioni sul sistema e vedere come si possono salvare dei dati utili.

Ho avviato PowerShell e ho usato il comando `Get-Process` per vedere direttamente tutti i processi, con tanto di ID, uso di CPU e memoria. Alcuni processi noti come `explorer`, `msedge`, `svchost` sono risultati attivi.

Con il comando `Get-Service` ho esplorato i servizi attivi e non attivi del sistema. È stato interessante vedere quante cose "girano" dietro le quinte anche se non ce ne accorgiamo.

Usando `Get-ComputerInfo`, ho raccolto tante informazioni sulla configurazione della macchina. Ho visto che si trattava di un Windows 10 Pro N installato su VirtualBox, con dettagli anche sul BIOS e altro.

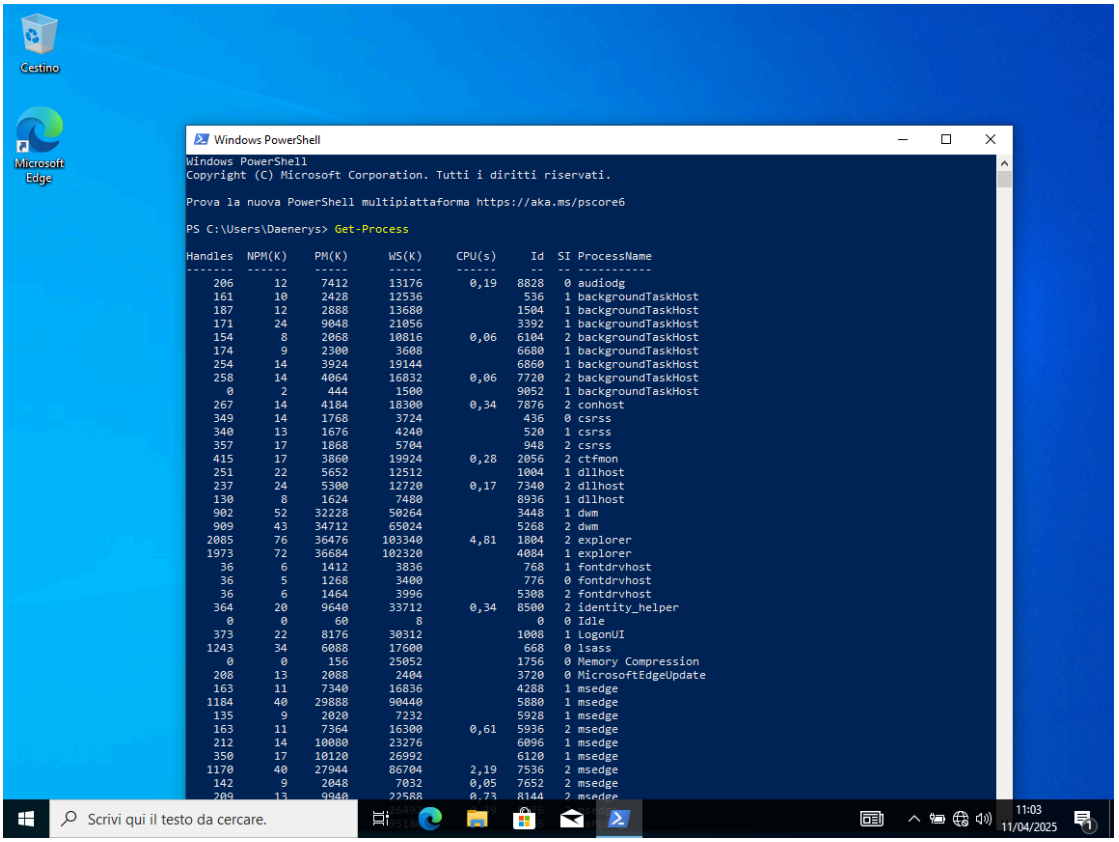
Ho eseguito `Get-Net TCP Connection` per vedere le porte di rete in ascolto e gli indirizzi IP. In quel momento c'erano diverse porte aperte e alcune connessioni in stato "TimeWait".

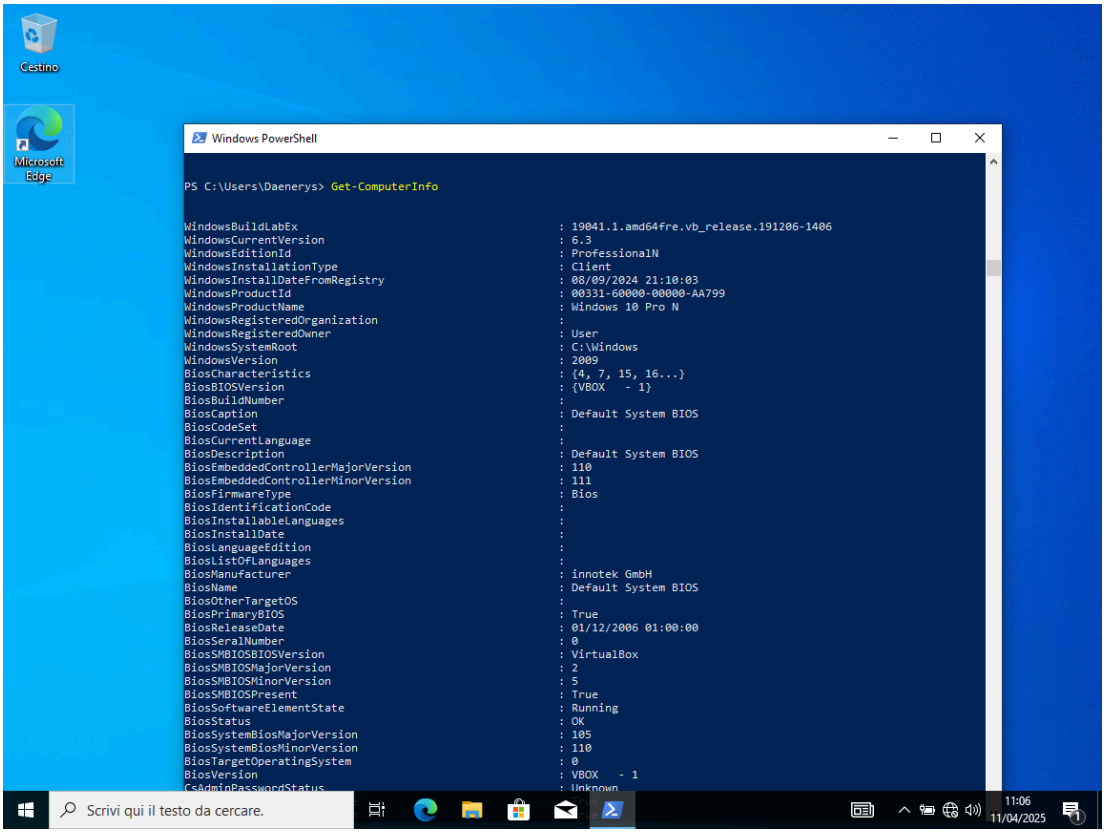
Successivamente con `Get-Process | Out-File C:\Users\Public\processi.txt` ho salvato l'elenco dei processi attivi in un file di testo. Poi ho controllato che il file fosse stato creato nella cartella indicata.

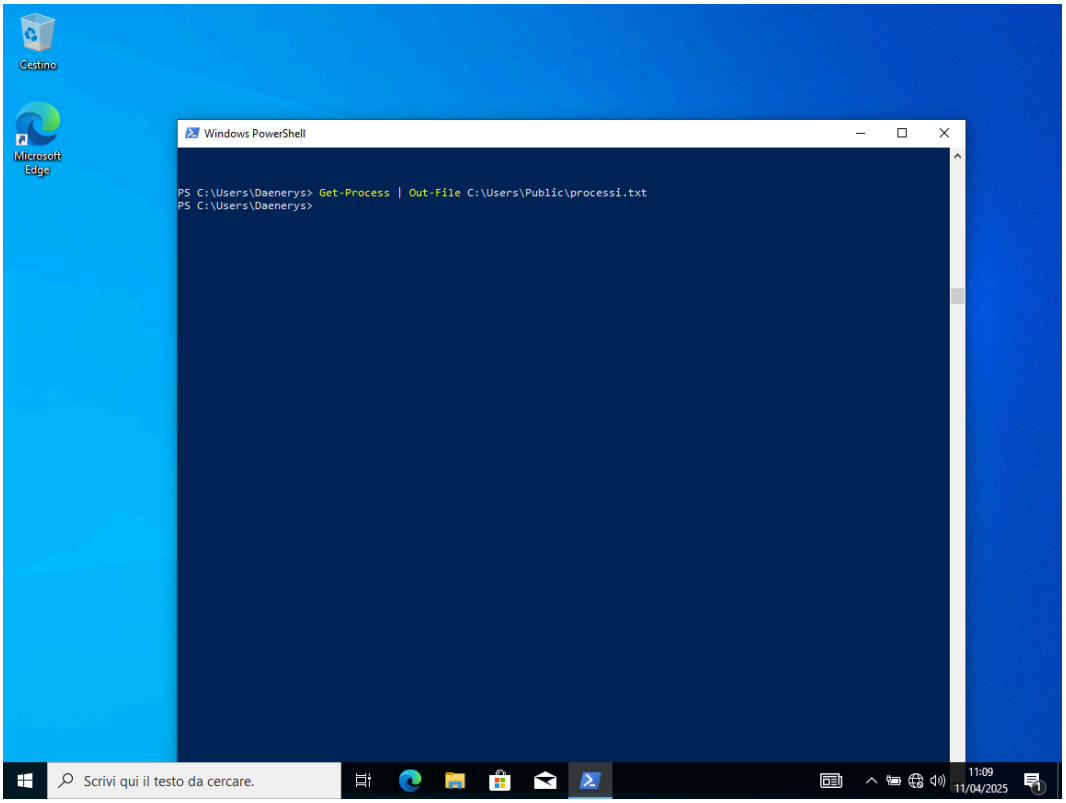
Poi ho provato il comando `netstat` e anche `ipconfig` per vedere l'indirizzo IP e la configurazione della rete. L'indirizzo IPv4 del sistema era `192.168.50.4`.

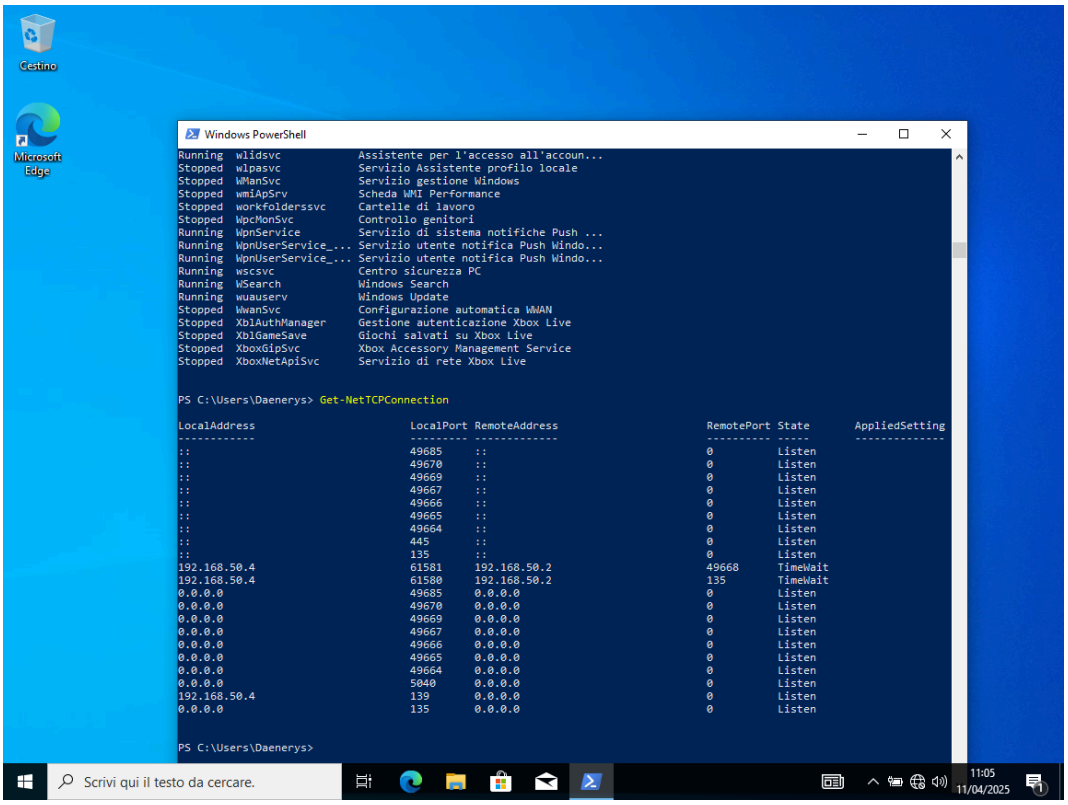
Ho testato anche comandi come `ping` (che mostra l'uso della rete per verificare la raggiungibilità di un host) e `Get-Command`, per vedere tutti i comandi disponibili su PowerShell.

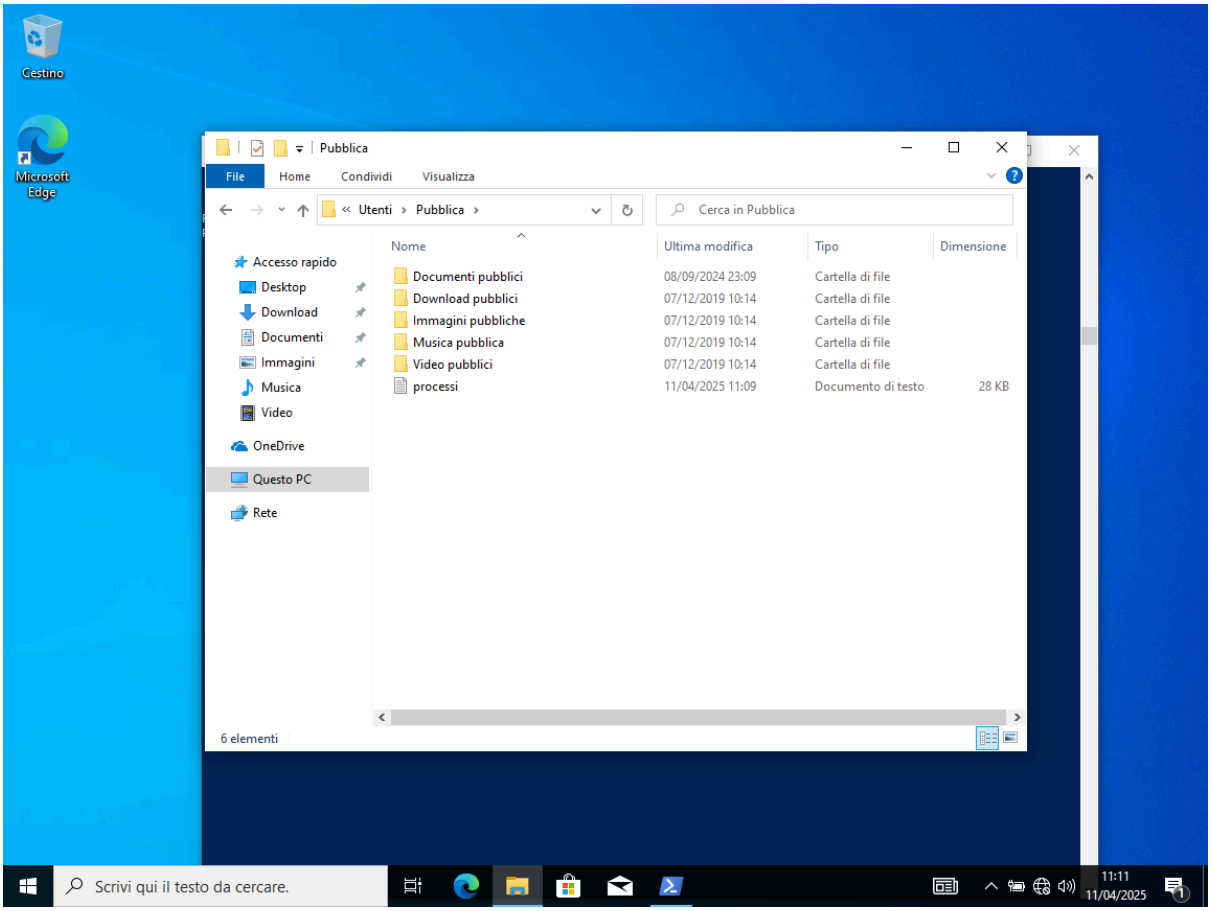
## Screenshot

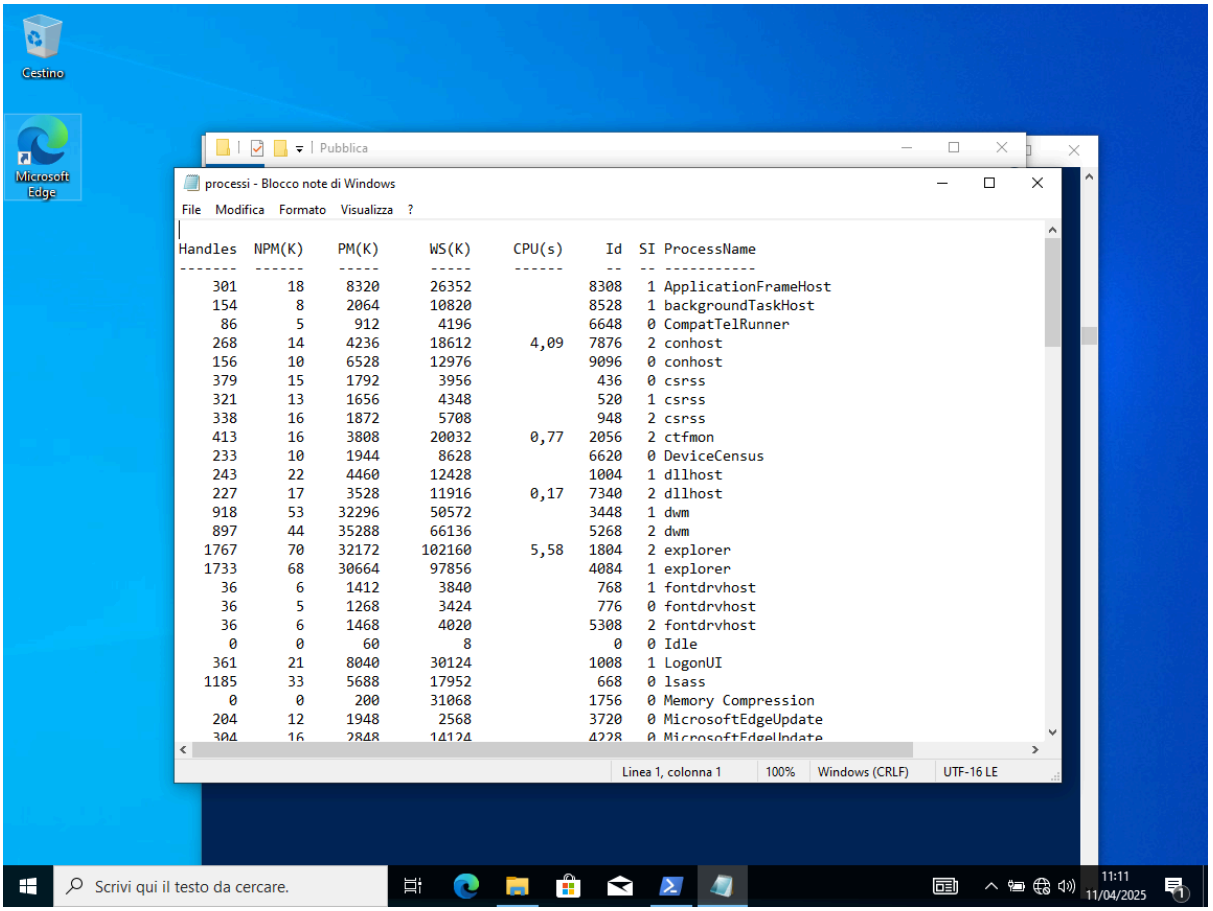

Cestino
Microsoft Edge
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.
Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6
PS C:\Users\Daenerys> Get-Process
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
206 12 7412 13176 0,19 8828 0 audiodg
161 10 2428 12536 536 1 backgroundTaskHost
187 12 2888 13680 1504 1 backgroundTaskHost
171 24 9048 21056 3392 1 backgroundTaskHost
154 8 2068 10816 0,06 6104 2 backgroundTaskHost
174 9 2300 3600 6680 1 backgroundTaskHost
254 14 3924 19144 6860 1 backgroundTaskHost
258 14 4064 16832 0,06 7720 2 backgroundTaskHost
0 2 444 1500 9052 1 backgroundTaskHost
267 14 4184 18300 0,34 7876 2 conhost
349 14 1768 3724 436 0 csrss
340 13 1676 4240 520 1 csrss
357 17 1868 5704 948 2 csrss
415 17 3860 19924 0,28 2056 2 ctfmon
251 22 5652 12512 1004 1 dllhost
237 24 5300 12720 0,17 7340 2 dllhost
130 8 1624 7480 8936 1 dllhost
902 52 32228 50264 3448 1 dwm
909 43 34712 65024 5268 2 dwm
2085 76 36476 103340 4,81 1804 2 explorer
1973 72 36684 102320 4084 1 explorer
36 6 1412 3836 768 1 fontdrvhost
36 5 1268 3400 776 0 fontdrvhost
36 6 1464 3996 5308 2 fontdrvhost
364 20 9640 33712 0,34 8500 2 identity_helper
0 0 60 8 0 0 Idle
373 22 8176 30312 1008 1 LogonUI
1243 34 6088 17600 668 0 lsass
0 0 156 25052 1756 0 Memory Compression
208 13 2088 2404 3720 0 MicrosoftEdgeUpdate
163 11 7340 16836 4288 1 msedge
1184 40 29888 90440 5880 1 msedge
135 9 2020 7232 5928 1 msedge
163 11 7364 16300 0,61 5936 2 msedge
212 14 10080 23276 6096 1 msedge
350 17 10120 26992 6120 1 msedge
1170 40 27944 86704 2,19 7536 2 msedge
142 9 2048 7032 0,05 7652 2 msedge
Scrivi qui il testo da cercare.
11:03
11/04/2025

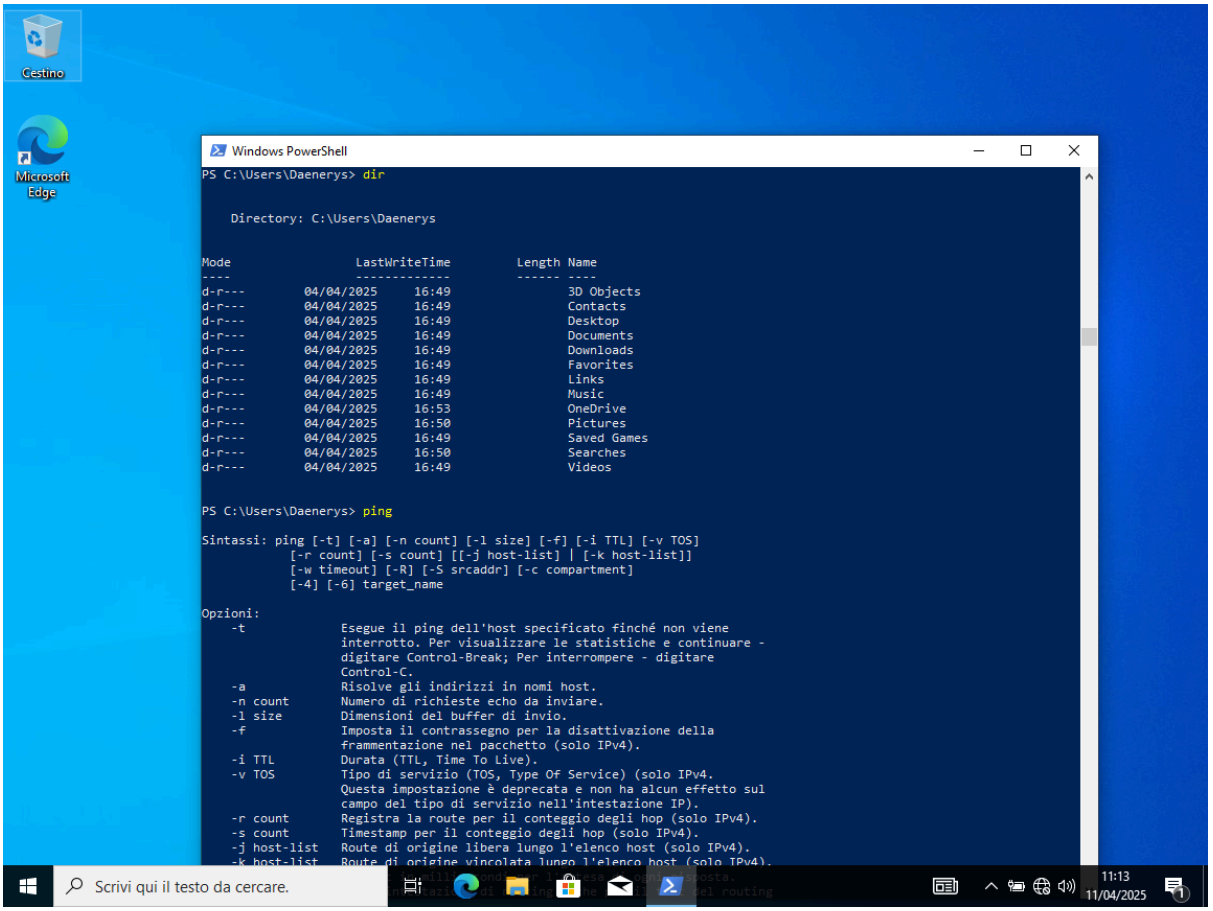

Cestino
Microsoft Edge
Windows PowerShell
PS C:\Users\Daenerys> Get-ComputerInfo
WindowsBuildLabEx : 19041.1.amd64fre.vb_release.191206-1406
WindowsCurrentVersion : 6.3
WindowsEditionId : ProfessionalN
WindowsInstallationType : Client
WindowsInstallDateFromRegistry : 08/09/2024 21:10:03
WindowsProductId : 00331-60000-00000-AA799
WindowsProductName : Windows 10 Pro N
WindowsRegisteredOrganization :
WindowsRegisteredOwner : User
WindowsSystemRoot : C:\Windows
WindowsVersion : 2009
BiosCharacteristics : {4, 7, 15, 16...}
BiosBIOSVersion : {VBOX - 1}
BiosBuildNumber :
BiosCaption : Default System BIOS
BiosCodeSet :
BiosCurrentLanguage :
BiosDescription : Default System BIOS
BiosEmbeddedControllerMajorVersion : 110
BiosEmbeddedControllerMinorVersion : 111
BiosFirmwareType : Bios
BiosIdentificationCode :
BiosInstallableLanguages :
BiosInstallDate :
BiosLanguageEdition :
BiosListOfLanguages :
BiosManufacturer : innotek GmbH
BiosName : Default System BIOS
BiosOtherTargetOS :
BiosPrimaryBIOS : True
BiosReleaseDate : 01/12/2006 01:00:00
BiosSeralNumber : 0
BiosSMBIOSBIOSVersion : VirtualBox
BiosSMBIOSMajorVersion : 2
BiosSMBIOSMinorVersion : 5
BiosSMBIOSPresent : True
BiosSoftwareElementState : Running
BiosStatus : OK
BiosSystemBiosMajorVersion : 105
BiosSystemBiosMinorVersion : 110
BiosTargetOperatingSystem : 0
BiosVersion : VBOX - 1
CsAdminPasswordStatus : Unknown
Scrivi qui il testo da cercare.
11:06
11/04/2025

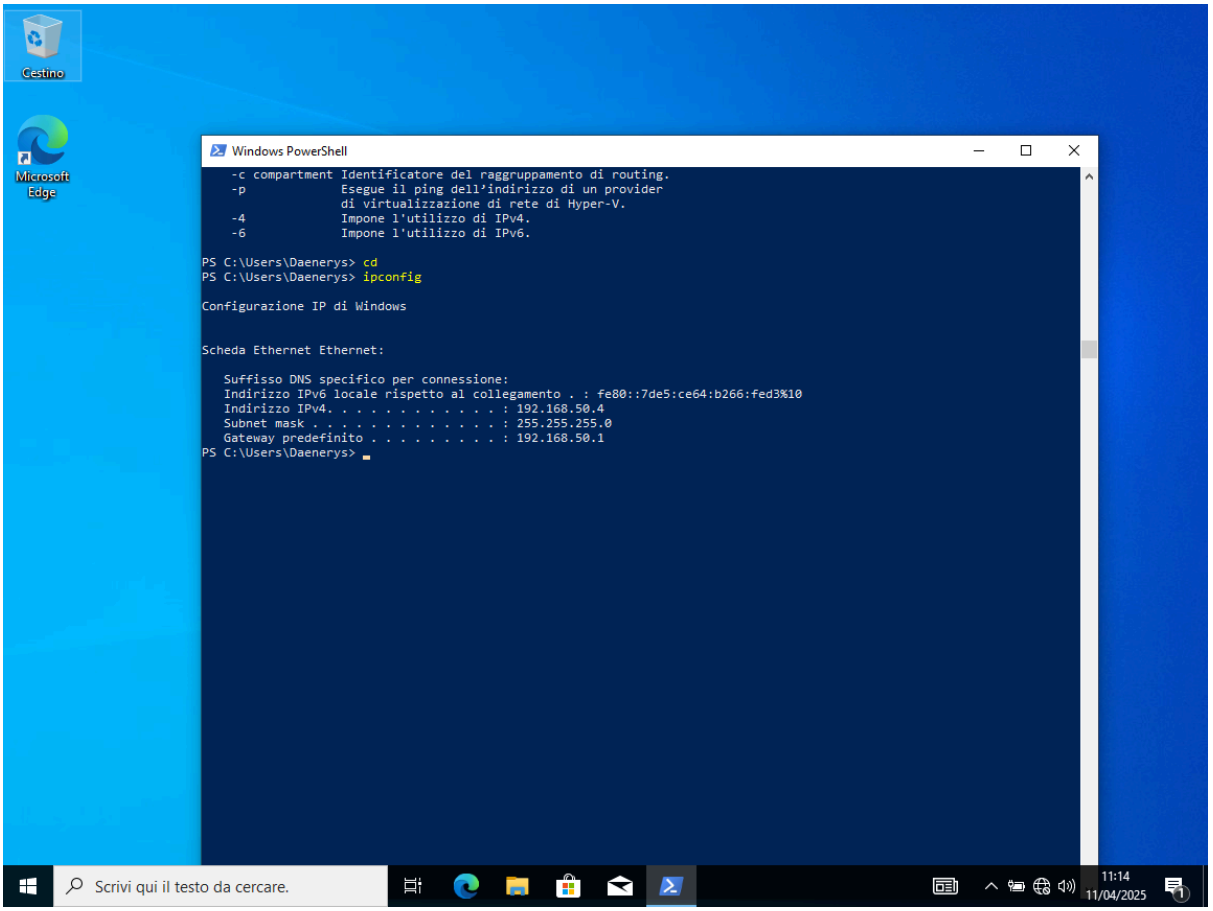

Cestino
Microsoft Edge
Windows PowerShell
PS C:\Users\Daenerys> Get-Process | Out-File C:\Users\Public\processi.txt
PS C:\Users\Daenerys>
Scrivi qui il testo da cercare.
11:09
11/04/2025

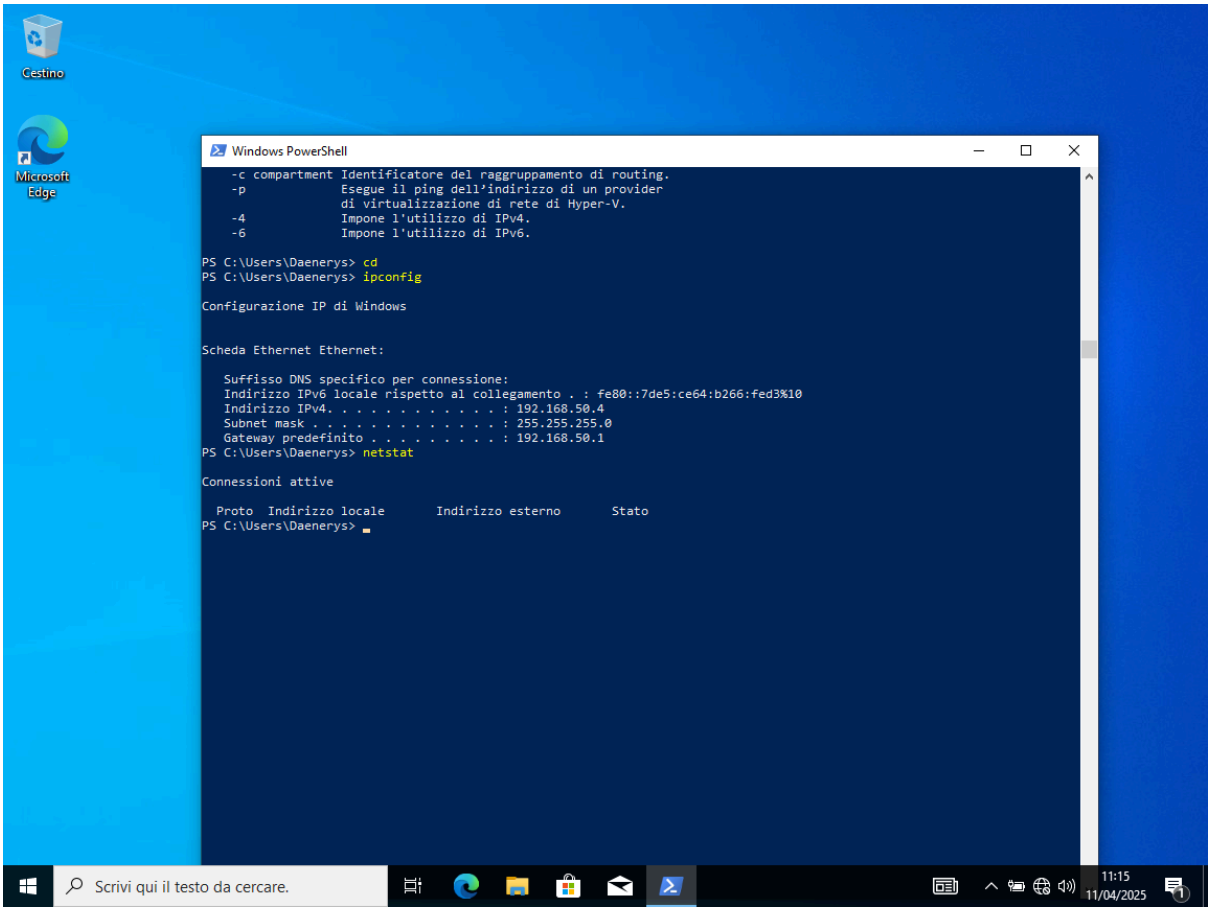

Cestino
Microsoft Edge
Windows PowerShell
Running wlidsvc Assistente per l'accesso all'accoun...
Stopped wlpasvc Servizio Assistente profilo locale
Stopped WManSvc Servizio gestione Windows
Stopped wmiApSrv Scheda WMI Performance
Stopped workfolderssvc Cartelle di lavoro
Stopped WpcMonSvc Controllo genitori
Running WpnService Servizio di sistema notifiche Push ...
Running WpnUserService_... Servizio utente notifica Push Windo...
Running WpnUserService_... Servizio utente notifica Push Windo...
Running wscsvc Centro sicurezza PC
Running WSearch Windows Search
Running wuauserv Windows Update
Stopped WwanSvc Configurazione automatica WWAN
Stopped XblAuthManager Gestione autenticazione Xbox Live
Stopped XblGameSave Giochi salvati su Xbox Live
Stopped XboxGipSvc Xbox Accessory Management Service
Stopped XboxNetApiSvc Servizio di rete Xbox Live
PS C:\Users\Daenerys> Get-NetTCPConnection
LocalAddress LocalPort RemoteAddress RemotePort State AppliedSetting
:: 49685 :: 0 Listen
:: 49670 :: 0 Listen
:: 49669 :: 0 Listen
:: 49667 :: 0 Listen
:: 49666 :: 0 Listen
:: 49665 :: 0 Listen
:: 49664 :: 0 Listen
:: 445 :: 0 Listen
:: 135 :: 0 Listen
192.168.50.4 61581 192.168.50.2 49668 TimeWait
192.168.50.4 61580 192.168.50.2 135 TimeWait
0.0.0.0 49685 0.0.0.0 0 Listen
0.0.0.0 49670 0.0.0.0 0 Listen
0.0.0.0 49669 0.0.0.0 0 Listen
0.0.0.0 49667 0.0.0.0 0 Listen
0.0.0.0 49666 0.0.0.0 0 Listen
0.0.0.0 49665 0.0.0.0 0 Listen
0.0.0.0 49664 0.0.0.0 0 Listen
0.0.0.0 5040 0.0.0.0 0 Listen
192.168.50.4 139 0.0.0.0 0 Listen
0.0.0.0 135 0.0.0.0 0 Listen
PS C:\Users\Daenerys>
Scrivi qui il testo da cercare.
11:05
11/04/2025

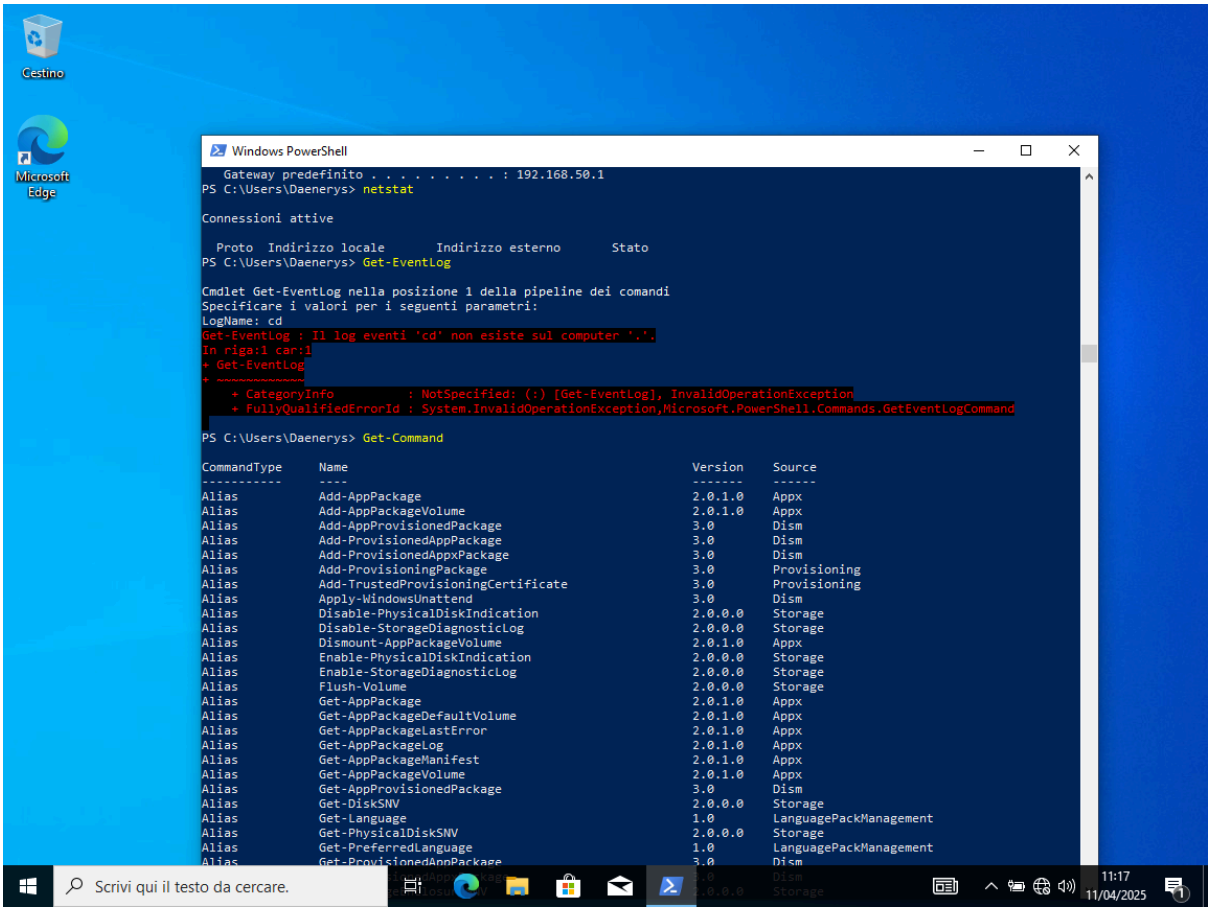

Cestino
Microsoft Edge
Pubblica
File
Home
Condividi
Visualizza
Utenti › Pubblica ›
Cerca in Pubblica
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
Video
OneDrive
Questo PC
Rete
Nome
Ultima modifica
Tipo
Dimensione
Documenti pubblici 08/09/2024 23:09 Cartella di file
Download pubblici 07/12/2019 10:14 Cartella di file
Immagini pubbliche 07/12/2019 10:14 Cartella di file
Musica pubblica 07/12/2019 10:14 Cartella di file
Video pubblici 07/12/2019 10:14 Cartella di file
processi 11/04/2025 11:09 Documento di testo 28 KB
6 elementi
Scrivi qui il testo da cercare.
11:11
11/04/2025


Cestino
Microsoft Edge
Pubblica
processi - Blocco note di Windows
File Modifica Formato Visualizza ?
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
301 18 8320 26352 8308 1 ApplicationFrameHost
154 8 2064 10820 8528 1 backgroundTaskHost
86 5 912 4196 6648 0 CompatTelRunner
268 14 4236 18612 4,09 7876 2 conhost
156 10 6528 12976 9096 0 conhost
379 15 1792 3956 436 0 csrss
321 13 1656 4348 520 1 csrss
338 16 1872 5708 948 2 csrss
413 16 3808 20032 0,77 2056 2 ctfmon
233 10 1944 8628 6620 0 DeviceCensus
243 22 4460 12428 1004 1 dllhost
227 17 3528 11916 0,17 7340 2 dllhost
918 53 32296 50572 3448 1 dwm
897 44 35288 66136 5268 2 dwm
1767 70 32172 102160 5,58 1804 2 explorer
1733 68 30664 97856 4084 1 explorer
36 6 1412 3840 768 1 fontdrvhost
36 5 1268 3424 776 0 fontdrvhost
36 6 1468 4020 5308 2 fontdrvhost
0 0 60 8 0 0 Idle
361 21 8040 30124 1008 1 LogonUI
1185 33 5688 17952 668 0 lsass
0 0 200 31068 1756 0 Memory Compression
204 12 1948 2568 3720 0 MicrosoftEdgeUpdate
Linea 1, colonna 1
100%
Windows (CRLF)
UTF-16 LE
Scrivi qui il testo da cercare.
11:11
11/04/2025


Cestino
Microsoft Edge
Windows PowerShell
PS C:\Users\Daenerys> dir
Directory: C:\Users\Daenerys
Mode LastWriteTime Length Name
d-r--- 04/04/2025 16:49 3D Objects
d-r--- 04/04/2025 16:49 Contacts
d-r--- 04/04/2025 16:49 Desktop
d-r--- 04/04/2025 16:49 Documents
d-r--- 04/04/2025 16:49 Downloads
d-r--- 04/04/2025 16:49 Favorites
d-r--- 04/04/2025 16:49 Links
d-r--- 04/04/2025 16:49 Music
d-r--- 04/04/2025 16:53 OneDrive
d-r--- 04/04/2025 16:50 Pictures
d-r--- 04/04/2025 16:49 Saved Games
d-r--- 04/04/2025 16:50 Searches
d-r--- 04/04/2025 16:49 Videos
PS C:\Users\Daenerys> ping
Sintassi: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment]
[-4] [-6] target_name
Opzioni:
-t Esegue il ping dell'host specificato finché non viene
interrotto. Per visualizzare le statistiche e continuare -
digitare Control-Break; Per interrompere - digitare
Control-C.
-a Risolve gli indirizzi in nomi host.
-n count Numero di richieste echo da inviare.
-l size Dimensioni del buffer di invio.
-f Imposta il contrassegno per la disattivazione della
frammentazione nel pacchetto (solo IPv4).
-i TTL Durata (TTL, Time To Live).
-v TOS Tipo di servizio (TOS, Type Of Service) (solo IPv4.
Questa impostazione è deprecata e non ha alcun effetto sul
campo del tipo di servizio nell'intestazione IP).
-r count Registra la route per il conteggio degli hop (solo IPv4).
-s count Timestamp per il conteggio degli hop (solo IPv4).
-j host-list Route di origine libera lungo l'elenco host (solo IPv4).
-k host-list Route di origine vincolata lungo l'elenco host (solo IPv4).
Scrivi qui il testo da cercare.
11:13
11/04/2025


Cestino
Microsoft Edge
Windows PowerShell
-c compartment Identificatore del raggruppamento di routing.
-p Esegue il ping dell'indirizzo di un provider
di virtualizzazione di rete di Hyper-V.
-4 Impone l'utilizzo di IPv4.
-6 Impone l'utilizzo di IPv6.
PS C:\Users\Daenerys> cd
PS C:\Users\Daenerys> ipconfig
Configurazione IP di Windows
Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%10
Indirizzo IPv4. . . . . : 192.168.50.4
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
PS C:\Users\Daenerys>
Scrivi qui il testo da cercare.
11:14
11/04/2025


Cestino
Microsoft Edge
Windows PowerShell
-c compartment Identificatore del raggruppamento di routing.
-p Esegue il ping dell'indirizzo di un provider
di virtualizzazione di rete di Hyper-V.
-4 Impone l'utilizzo di IPv4.
-6 Impone l'utilizzo di IPv6.
PS C:\Users\Daenerys> cd
PS C:\Users\Daenerys> ipconfig
Configurazione IP di Windows
Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%10
Indirizzo IPv4. . . . . : 192.168.50.4
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
PS C:\Users\Daenerys> netstat
Connessioni attive
Proto Indirizzo locale Indirizzo esterno Stato
PS C:\Users\Daenerys>
Scrivi qui il testo da cercare.
11:15
11/04/2025


Cestino
Microsoft Edge
Windows PowerShell
Gateway predefinito . . . . . : 192.168.50.1
PS C:\Users\Daenerys> netstat
Connessioni attive
Proto Indirizzo locale Indirizzo esterno Stato
PS C:\Users\Daenerys> Get-EventLog
Cmdlet Get-EventLog nella posizione 1 della pipeline dei comandi
Specificare i valori per i seguenti parametri:
LogName: cd
Get-EventLog : Il log eventi 'cd' non esiste sul computer '.'.
In riga:1 car:1
+ Get-EventLog
+ ~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (:) [Get-EventLog], InvalidOperationException
+ FullyQualifiedErrorId : System.InvalidOperationException,Microsoft.PowerShell.Commands.GetEventLogCommand
PS C:\Users\Daenerys> 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
Scrivi qui il testo da cercare.
11:17
11/04/2025

## Conclusione:

PowerShell permette di gestire il sistema, raccogliere dati, monitorare connessioni, e persino salvare tutto in file da consultare dopo. E’ importante perché permette di raccogliere le informazioni giuste al momento giusto, anche solo con un semplice comando.