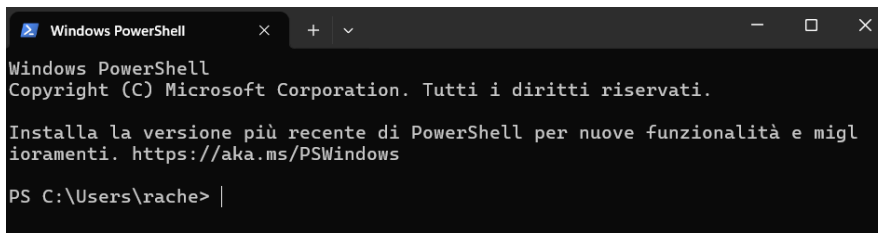


Utilizzo di Windows PowerShell

Obiettivo: Esplorare alcune funzioni di PowerShell per comprenderne il funzionamento e le potenzialità nell'ambito della gestione e dell'automazione del sistema operativo Windows.

Parte 1: Accesso alla Console di PowerShell

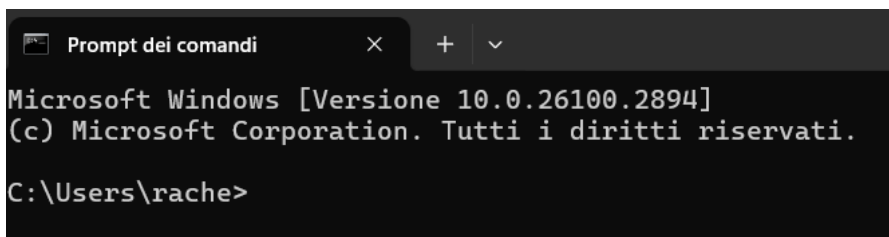
1. Aprire PowerShell tramite Start.
2. Aprire il prompt dei comandi tramite Start.



```
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\rache> |
```



```
Prompt dei comandi

Microsoft Windows [Versione 10.0.26100.2894]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\rache>
```

Parte 2: Esplorazione del Prompt dei Comandi e dei Comandi di PowerShell

1. Eseguire il comando `dir` in entrambi gli ambienti:
 - Output: elenco di file e cartelle con dettagli su tipo, dimensione, data e attributi.
2. Eseguire comandi comuni come `ping`, `cd`, `ipconfig`.
 - Output simile in entrambi gli ambienti.

Parte 3: Esplorazione dei Cmdlet di PowerShell

1. Identificare l'alias del comando `dir` con `Get-Alias dir`.
 - Output: `Get-ChildItem`.
2. Ricerca online per approfondire i cmdlet di PowerShell.
3. Chiudere la finestra del prompt dei comandi.

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

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

PS C:\Users\rache> |
```

Parte 4: Uso di Netstat in PowerShell

1. Visualizzare le opzioni del comando `netstat -h`.
2. Mostrare la tabella di routing con `netstat -r`.
 - Identificare il gateway IPv4 (es. 192.168.1.1).
3. Aprire PowerShell con privilegi elevati (amministratore).
4. Visualizzare i processi associati alle connessioni TCP con `netstat -abno`.
 - Identificare un PID e verificarlo in Task Manager.
 - Esempio: PID 756 associato a `svchost.exe`, utente "SERVIZIO DI RETE", utilizzo memoria 4132K.

```
PS C:\Users\rache> netstat -h

Socket Handle Count

    PID      Count  Closing Count
    ----      -
    2836         4          0
    21268        2          0
    7200         4          0
    25376        4          0
    4388         1          0
    20260        1          0
    2092         2          0
    11060        6          0
    31540        2          0
    1088         4          0
    4420         4          0
    2888         4          0
    11088        4          0
    20308        7          0
    1880         1          0
    4444         3          0
    1888         6          0
    1124         4          0
    11620       23          0
    18560        3          0
    12428        2          0
    7056         9          0
    7568        15          1
    12180        1          0
    1436         11         0
    20380        4          0
    12704        1          0
    17056        2          0
    4264         4          0
    18856       33          0
    24744        4          0
    17580        1          0
    17844        4          0
    10424        1          0
    20672        4          1
```

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

=====
Elenco interfacce
3...0a 00 27 00 00 03 .....VirtualBox Host-Only Ethernet Adapter
7...00 ff 48 20 20 29 .....TAP-Windows Adapter V9
10...2e 98 11 15 4d 51 .....Microsoft Wi-Fi Direct Virtual Adapter
14...22 98 11 15 4d 51 .....Microsoft Wi-Fi Direct Virtual Adapter #2
11...2c 98 11 15 4d 51 .....Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
    Indirizzo rete      Mask      Gateway      Interfaccia  Metrica
    -----
    0.0.0.0             0.0.0.0    192.168.94.57 192.168.94.136  55
    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
    192.168.94.0        255.255.255.0   On-link       192.168.94.136  311
    192.168.94.136     255.255.255.255  On-link       192.168.94.136  311
    192.168.94.255     255.255.255.255  On-link       192.168.94.136  311
    192.168.211.0       255.255.255.0   On-link       192.168.211.1   281
    192.168.211.1       255.255.255.255  On-link       192.168.211.1   281
    192.168.211.255     255.255.255.255  On-link       192.168.211.1   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       192.168.211.1   281
    224.0.0.0           240.0.0.0     On-link       192.168.94.136  311
    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       192.168.211.1   281
    255.255.255.255     255.255.255.255  On-link       192.168.94.136  311
=====
Route permanenti:
    Nessuna

IPv6 Tabella route
=====
```

Parte 5: Svuotamento del Cestino con PowerShell

1. Verificare la presenza di file nel Cestino.
2. Se vuoto, creare file e inserirli nel Cestino.
3. Utilizzare il comando `clear-recyclebin`.
 - Conferma richiesta.
 - Output: eliminazione definitiva dei file nel 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"):
```

PowerShell offre strumenti avanzati per la gestione del sistema operativo e l'automazione delle operazioni, risultando particolarmente utile per gli analisti della sicurezza informatica.