

Report Analitico - Esercizio 1: Usare Windows PowerShell

Studente: Nicola Cassandra

Data: 20/02/2026

Obiettivo: Imparare ad utilizzare Windows PowerShell

Parte 1 e 2: Esplorare i comandi del Prompt dei Comandi e di PowerShell

In questa fase iniziale abbiamo confrontato il comportamento dei due ambienti a riga di comando di Windows eseguendo comandi di base.

- **Quali sono gli output del comando `dir`?** Come si evince dall'immagine, l'output è differente nei due terminali. Nel Prompt dei Comandi classico, `dir` restituisce un semplice elenco testuale che mostra data, ora, la dicitura <DIR> o la dimensione in byte, e il nome del file. In PowerShell, invece, l'output è strutturato sotto forma di *oggetti* e viene presentato in una tabella con colonne ben definite: `Mode` (i permessi e gli attributi), `LastWriteTime`, `Length` e `Name`.

The screenshot shows two windows side-by-side. The left window is titled 'Windows PowerShell' and shows the output of the 'dir' command in PowerShell. It displays a table with columns: Mode, LastWriteTime, Length, and Name. The table lists various directory entries like 'Objects', 'Contacts', 'Desktop', etc., with their respective creation times and sizes. The right window is titled 'Prompt dei comandi' and shows the output of the 'dir' command in the classic Command Prompt. It displays a plain text list where each entry consists of a date and time followed by '<DIR>' or a file size, and then the directory name. Both outputs show the same set of directories and files.

- **Quali sono i risultati di comandi come `ping`, `cd` e `ipconfig`?** Guardando l'immagine che segue questa risposta (che mostra l'esecuzione di `ipconfig`), notiamo che i risultati sono **identici** in entrambe le finestre. PowerShell è infatti progettato per essere retrocompatibile e riconosce gli eseguibili standard di Windows (come `ipconfig.exe` o `ping.exe`), restituendo lo stesso identico output di rete.

```

PS C:\Users\User> ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione: homenet.telecomitalia.it
Indirizzo IPv6 . . . . . : fd17:625c:f037:2:aibe:fe77:4521:fb9d
Indirizzo IPv6 temporaneo . . . . . : fd17:625c:f037:2:aibe:fe77:4521:fb9d
Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%5
Indirizzo IP4 . . . . . : 10.0.2.15
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::2%5
                                10.0.2.2
PS C:\Users\User>

C:\Users\User> ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione: homenet.telecomitalia.it
Indirizzo IPv6 . . . . . : fd17:625c:f037:2:aibe:fe77:4521:fb9d
Indirizzo IPv6 temporaneo . . . . . : fd17:625c:f037:2:aibe:fe77:4521:fb9d
Indirizzo IPv4 . . . . . : 10.0.2.15
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::2%5
                                10.0.2.2

PS C:\Users\User> netstat
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno      Stato
TCP  10.0.2.15:49759        4.207.247.139:https ESTABLISHED
TCP  10.0.2.15:49805        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49806        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49809        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49811        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49813        a2-16-70-4:http  ESTABLISHED
TCP  10.0.2.15:49819        a2-20-242-17:https CLOSE_WAIT
TCP  10.0.2.15:49822        4.207.247.139:https ESTABLISHED
TCP  10.0.2.15:49824        172.184.231.71:https TIME_WAIT
TCP  10.0.2.15:49825        a23-55-48-58:https TIME_WAIT
TCP  10.0.2.15:49826        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49827        172.184.231.71:https TIME_WAIT
TCP  10.0.2.15:49828        a23-55-48-58:https TIME_WAIT
TCP  10.0.2.15:49829        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49830        128.85.113.134:https TIME_WAIT
TCP  10.0.2.15:49831        109.61.38.38:https TIME_WAIT
TCP  10.0.2.15:49832        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49834        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49835        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49836        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49839        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49843        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49844        72.146.92.132:http  TIME_WAIT
TCP  10.0.2.15:49846        72.146.92.132:http  TIME_WAIT
TCP  10.0.2.15:49849        40.126.53.6:https ESTABLISHED

C:\Users\User> netstat
Connessioni attive

Proto Indirizzo locale      Indirizzo esterno      Stato
TCP  10.0.2.15:49759        4.207.247.139:https ESTABLISHED
TCP  10.0.2.15:49805        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49806        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49809        199.232.214.172:http TIME_WAIT
TCP  10.0.2.15:49811        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49813        a2-16-70-4:http  ESTABLISHED
TCP  10.0.2.15:49819        a2-20-242-17:https CLOSE_WAIT
TCP  10.0.2.15:49822        4.207.247.139:https ESTABLISHED
TCP  10.0.2.15:49826        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49827        172.184.231.71:https TIME_WAIT
TCP  10.0.2.15:49828        a23-55-48-58:https TIME_WAIT
TCP  10.0.2.15:49829        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49830        128.85.113.134:https TIME_WAIT
TCP  10.0.2.15:49831        109.61.38.38:https TIME_WAIT
TCP  10.0.2.15:49832        135.232.92.97:https TIME_WAIT
TCP  10.0.2.15:49834        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49835        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49836        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49839        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49843        a2-20-114-43:https ESTABLISHED
TCP  10.0.2.15:49844        72.146.92.132:http  TIME_WAIT
TCP  10.0.2.15:49846        72.146.92.132:http  TIME_WAIT
TCP  10.0.2.15:49849        40.126.53.6:https ESTABLISHED

```

Parte 3: Esplorare i cmdlet

PowerShell utilizza una struttura "Verbo-Nome" per i suoi comandi nativi (i *cmdlet*), ma permette l'uso di comandi legacy tramite un sistema di alias.

- **Qual è il comando PowerShell per `dir`?** Eseguendo il comando `Get-Alias dir`, scopriamo che la riga di comando ci restituisce la mappatura esatta: il vero cmdlet eseguito dietro le quinte da PowerShell quando digitiamo `dir` è `Get-ChildItem`.

```

Windows PowerShell

PS C:\Users\User> Get-Alias dir
 CommandType      Name          Version      Source
-----          ----          -----      -----
 Alias           dir -> Get-ChildItem

```

Parte 4: Esplorare il comando `netstat` usando PowerShell

Questa sezione del laboratorio si è concentrata sull'analisi delle connessioni di rete e delle tabelle di routing.

- **Qual è il gateway IPv4?** Osservando l'output del comando `netstat -r` (Tabella di routing) nell'immagine al di sotto, possiamo identificare la rotta predefinita (quella con Indirizzo rete `0.0.0.0` e Mask `0.0.0.0`). Il Gateway IPv4 associato a questa rotta

sulla tua macchina virtuale è **10.0.2.2**.

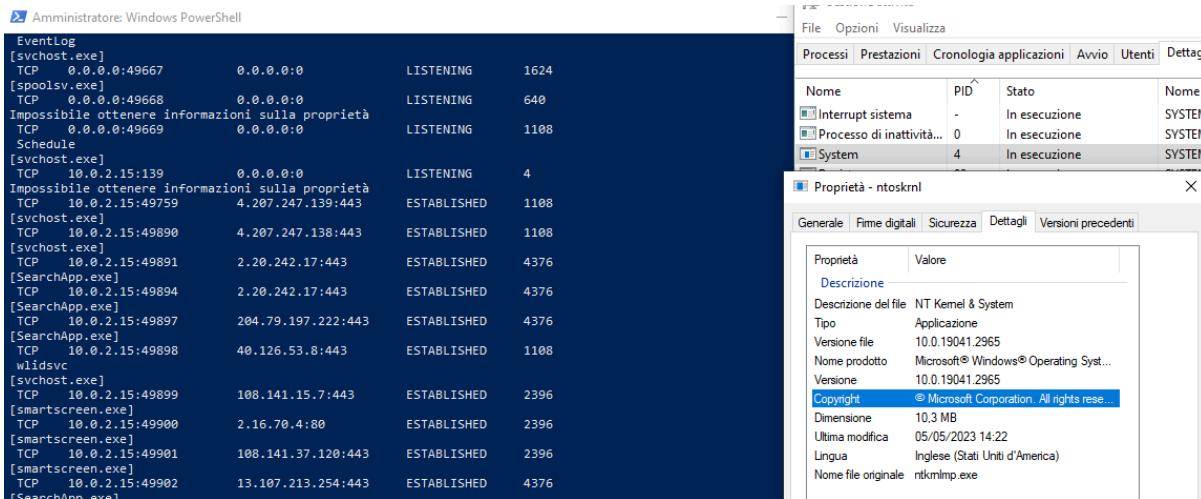
```
PS C:\Users\User> netstat -r
=====
Elenco interfacce
 5...08 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
 1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask       Gateway   Interfaccia Metrica
    0.0.0.0        0.0.0.0   10.0.2.2   10.0.2.15     25
    10.0.2.0      255.255.255.0 On-link    10.0.2.15     281
    10.0.2.15     255.255.255.255 On-link    10.0.2.15     281
    10.0.2.255    255.255.255.255 On-link    10.0.2.15     281
    127.0.0.0      255.0.0.0   On-link    127.0.0.1      331
    127.0.0.1      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
    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    10.0.2.15     281
  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    10.0.2.15     281
=====
Route permanenti:
  Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
    5    281 ::/0                      fe80::2
    1    331 ::1/128                  On-link
    5    281 fd17:625c:f037:2::/64    On-link
    5    281 fd17:625c:f037:2:7899:5949:534:2173/128
                                         On-link
    5    281 fd17:625c:f037:2:a1be:fe77:4521:f9d/128
                                         On-link
    5    281 fe80::/64                On-link
    5    281 fe80::7de5:ce64:b266:fed3/128
                                         On-link
    1    331 ff00::/8                On-link
    5    281 ff00::/8                On-link
=====
Route permanenti:
  Nessuna
```

- Quali informazioni puoi ottenere dalla scheda **Dettagli** e dalla finestra di dialogo **Proprietà per il PID selezionato**? Nell'immagine che segue al di sotto vediamo l'uso di PowerShell come Amministratore e l'apertura del Task Manager per indagare su un processo specifico. Dalla scheda *Dettagli* otteniamo informazioni sullo stato dell'esecuzione, l'utente che lo ha lanciato (es. SYSTEM), l'utilizzo di CPU e memoria. Aprendo le *Proprietà* (in questo caso per **ntoskrnl.exe**), otteniamo dati cruciali per l'analisi forense e di sicurezza:
 - Descrizione del file (NT Kernel & System)
 - Versione del file e del prodotto
 - Copyright (che aiuta a confermare se il file è legittimo, es. Microsoft Corporation)
 - Dimensione e data di ultima modifica

- Il nome originale del file (`ntkrnlmp.exe`).



Parte 5: Svuotare il cestino usando PowerShell

L'automazione tramite PowerShell permette di eseguire rapidamente task di sistema che richiederebbero più clic nell'interfaccia grafica.

The screenshot shows the Windows Recycle Bin interface. It has tabs for Gestisci (Manage) and Cestino (Trash). Below these are buttons for Condividi (Share), Visualizza (View), and Strumenti Cestino (Trash Tools). The main area displays a list of files in the trash, with columns for Nome (Name) and Percorso originale (Original Path). Two files are listed: 'sdvcsdvsdsvs' and 'zcvsfvfvsvs', both located at C:\Users\User\Desktop.

- Cosa è successo ai file nel Cestino?** Come documentato nelle immagini che seguono la risposta, dopo aver eseguito il comando `clear-recyclebin` e aver confermato premendo **S** (Sì), i file sono stati **eliminati in modo permanente** dal PC

e la cartella del cestino risulta completamente vuota.

