

S11 L5

Utilizzo CMD e Powershell

Esercizio 1

- Parte 1 Accedere alla console PowerShell.

Abbiamo aperto la console Powershell e il prompt dei comandi utilizzando lo shortcut Windows + r e scrivendo "CMD" e "powershell"

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

Il comando dir equivale al comando ls su linux, ci mostra le directory presenti

```
C:\Users\eris>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 76FF-0D4F

Directory di C:\Users\eris

20/02/2026  14:32    <DIR>          .
20/02/2026  14:32    <DIR>          ..
13/02/2026  12:53    <DIR>          3D Objects
13/02/2026  12:53    <DIR>          Contacts
13/02/2026  12:53    <DIR>          Desktop
13/02/2026  12:53    <DIR>          Documents
13/02/2026  12:53    <DIR>          Downloads
13/02/2026  12:53    <DIR>          Favorites
13/02/2026  12:53    <DIR>          Links
13/02/2026  12:53    <DIR>          Music
13/02/2026  12:55    <DIR>          OneDrive
13/02/2026  12:53    <DIR>          Pictures
13/02/2026  12:53    <DIR>          Saved Games
13/02/2026  12:53    <DIR>          Searches
13/02/2026  12:53    <DIR>          Videos
               0 File               0 byte
            15 Directory  55.787.085.824 byte disponibili
```

```
PS C:\Users\eris> dir
```

```
Directory: C:\Users\eris
```

Mode	LastWriteTime	Length	Name
d-r---	13/02/2026 12:53		3D Objects
d-r---	13/02/2026 12:53		Contacts
d-r---	13/02/2026 12:53		Desktop
d-r---	13/02/2026 12:53		Documents
d-r---	13/02/2026 12:53		Downloads
d-r---	13/02/2026 12:53		Favorites
d-r---	13/02/2026 12:53		Links
d-r---	13/02/2026 12:53		Music
d-r---	13/02/2026 12:55		OneDrive
d-r---	13/02/2026 12:53		Pictures
d-r---	13/02/2026 12:53		Saved Games
d-r---	13/02/2026 12:53		Searches
d-r---	13/02/2026 12:53		Videos

Di seguito le immagini per i comandi “ping”, “cd” e “ipconfig”, che svolgono le seguenti funzioni:

1. ping: invia un ping a un determinato ip per vedere se la macchina e il target comunicano

```
C:\Users\eris>ping localhost
```

```
Esecuzione di Ping Pc1.Mushoku.local [::1] con 32 byte di dati:  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms
```

```
Statistiche Ping per ::1:
```

```
Pacchetti: Trasmessi = 4, Ricevuti = 4,  
Persi = 0 (0% persi),
```

```
Tempo approssimativo percorsi andata/ritorno in millisecondi:
```

```
Minimo = 0ms, Massimo = 0ms, Medio = 0ms
```

```
PS C:\Users\eris> ping localhost
```

```
Esecuzione di Ping Pc1.Mushoku.local [::1] con 32 byte di dati:  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms  
Risposta da ::1: durata<1ms
```

```
Statistiche Ping per ::1:
```

```
Pacchetti: Trasmessi = 4, Ricevuti = 4,  
Persi = 0 (0% persi),
```

```
Tempo approssimativo percorsi andata/ritorno in millisecondi:
```

```
Minimo = 0ms, Massimo = 0ms, Medio = 0ms
```

2. cd: il comando change directory, serve a cambiare directory attiva

```
C:\Users\eris>cd
C:\Users\eris

C:\Users\eris>cd Desktop
C:\Users\eris\Desktop>

PS C:\Users\eris> cd
PS C:\Users\eris> cd .\Desktop\
PS C:\Users\eris\Desktop>
```

3. ipconfig: permette di controllare l'indirizzo IP, il gateway predefinito e i server DNS, oltre a risolvere problemi di connessione tramite il rinnovo IP e la pulizia della cache DNS.

```
C:\Users\eris\Desktop>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fd17:625c:f037:2:7899:5949:534:2173
    Indirizzo IPv6 temporaneo. . . . . : fd17:625c:f037:2:f51b:4a5a:7e0e:9509
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%10
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::2%10
                                10.0.2.2
```

```
PS C:\Users\eris> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fd17:625c:f037:2:7899:5949:534:2173
    Indirizzo IPv6 temporaneo. . . . . : fd17:625c:f037:2:f51b:4a5a:7e0e:9509
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%10
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::2%10
                                10.0.2.2
```

Possiamo notare che i comandi svolgono la stessa funzione su entrambi i terminali

- Parte 3 Esplorare i cmdlet.

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

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

Il comando per dir per powershell è Get-ChildItem

I cmdlet eseguono un'azione e in genere restituiscono un oggetto Microsoft .NET al comando successivo nella pipeline. Un cmdlet è un singolo comando che partecipa alla semantica della pipeline di PowerShell. Sono inclusi cmdlet binari (C#), funzioni di script avanzate, CDXML e flussi di lavoro.

Di seguito degli esempi di cmdlet più usati

1. General Discovery and Help Commands

These cmdlets help you explore PowerShell's capabilities and obtain assistance.

1. Get-Command

Lists all available cmdlets, functions, workflows, aliases, and scripts.

Example: `Get-Command`

2. Get-Help

Displays detailed help information for a specified cmdlet or concept.

Example: `Get-Help Get-Process -Full`

3. Update-Help

Downloads and installs the latest help files for installed modules.

Example: `Update-Help`

2. Service Management Commands

These commands allow you to view and control Windows services.

4. Get-Service

Retrieves the status of services on a local or remote machine.

Example: `Get-Service`

5. Start-Service

Starts a specified service (e.g., the Windows Update service).

Example: `Start-Service -Name "wuauserv"`

6. Stop-Service

Stops a specified service.

Example: `Stop-Service -Name "wuauserv"`

7. Restart-Service

Restarts a specified service quickly.

Example: `Restart-Service -Name "wuauserv"`

3. Process Management Commands

Use these cmdlets to manage running processes.

8. Get-Process

Lists all currently running processes.

Example: `Get-Process`

9. Stop-Process

Terminates a process by its name or process ID.

Example: `Stop-Process -Name "notepad"`

10. Start-Process

Launches a new process or application.

Example: `Start-Process -FilePath "notepad.exe"`

4. Event Log Commands

Access and review event logs for troubleshooting.

11. Get-EventLog

Retrieves recent entries from a specified event log (such as the Application log).

Example: `Get-EventLog -LogName Application -Newest 10`

- Parte 4 Esplorare il comando netstat usando PowerShell.

```
PS C:\Users\eris> 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'eseguibile 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'eseguibile
  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
  visualizzata 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 omesso, netstat stamperà il
  informazioni di configurazione una volta.
```

Abbiamo usato il comando netstat -h, il flag -h (help) mostra i flag aggiuntivi che è possibile usare per il comando

```

PS C:\Users\eris> netstat -r
=====
Elenco interfacce
10...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           255.255.255.255  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
  10      281  ::/0      fe80::2
  1       331  ::1/128   On-link
  10      281  fd17:625c:f037:2::/64  On-link
  10      281  fd17:625c:f037:2:7899:5949:534:2173/128  On-link
  10      281  fd17:625c:f037:2:f51b:4a5a:7e0e:9509/128  On-link
  10      281  fe80::/64  On-link
  10      281  fe80::7de5:ce64:b266:fed3/128  On-link
  1       331  ff00::/8  On-link
  10      281  ff00::/8  On-link
=====
Route permanenti:
  Nessuna
PS C:\Users\eris>

```

Usando il comando netstat -r è possibile vedere le tabelle di routing

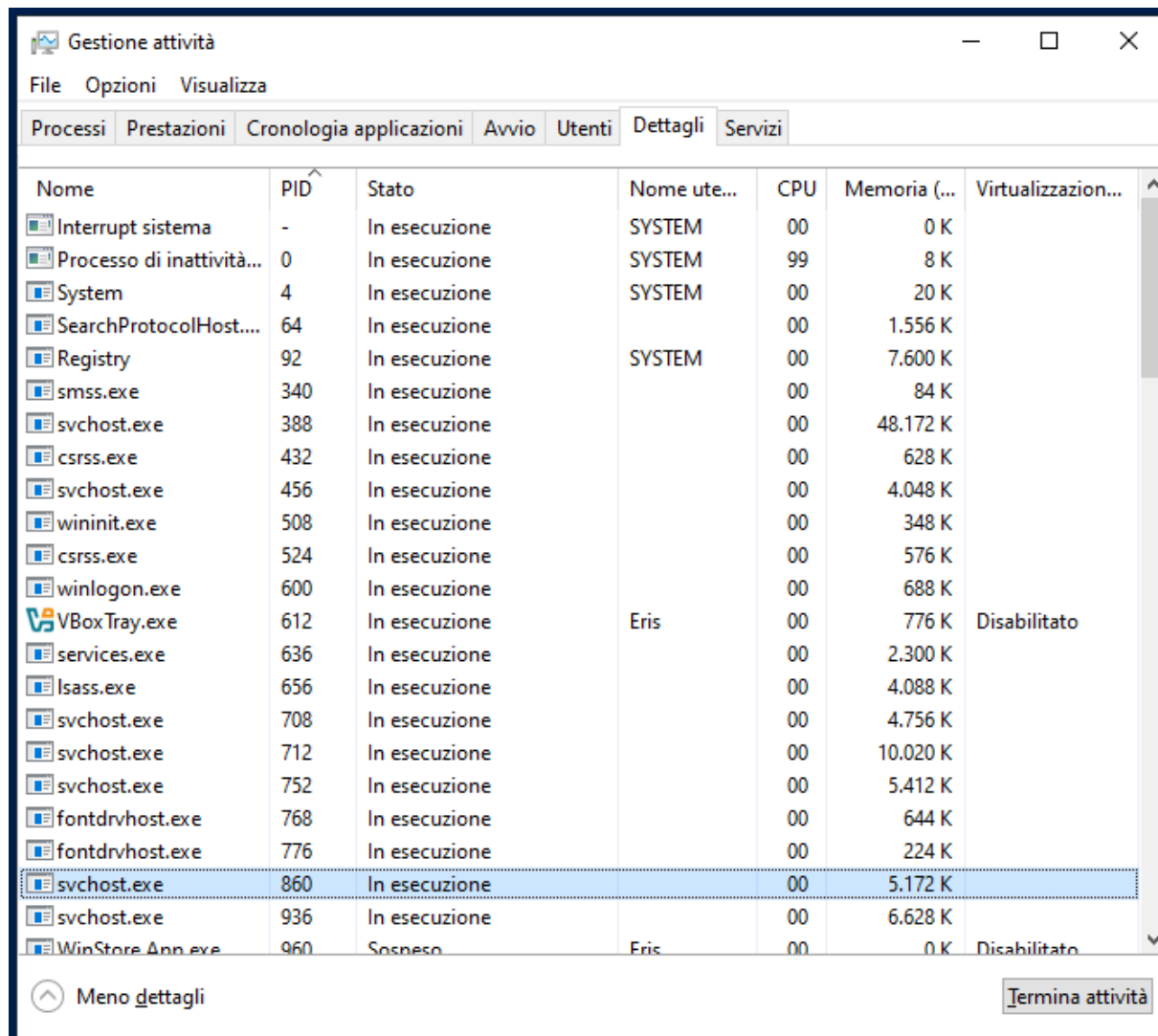
Il gateway in questo caso è 10.0.2.2

```
PS C:\Windows\system32> netstat -abno

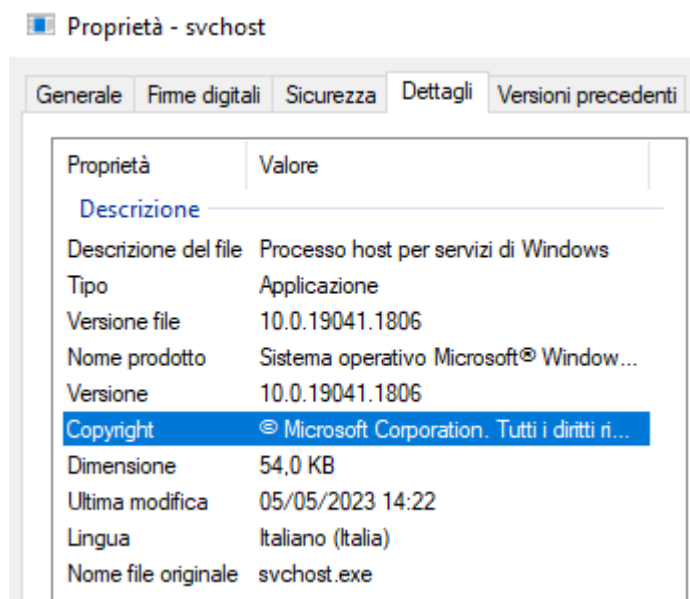
Connessioni attive

  Proto Indirizzo locale      Indirizzo esterno    Stato      PID
  ---
TCP     0.0.0.0:135             0.0.0.0:0           LISTENING  860
RpcSs
[svchost.exe]
TCP     0.0.0.0:445             0.0.0.0:0           LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP     0.0.0.0:5040            0.0.0.0:0           LISTENING  708
CDPSvc
[svchost.exe]
TCP     0.0.0.0:5357            0.0.0.0:0           LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP     0.0.0.0:49664           0.0.0.0:0           LISTENING  656
[lsass.exe]
TCP     0.0.0.0:49665           0.0.0.0:0           LISTENING  508
Impossibile ottenere informazioni sulla proprietà
TCP     0.0.0.0:49666           0.0.0.0:0           LISTENING  712
EventLog
[svchost.exe]
TCP     0.0.0.0:49667           0.0.0.0:0           LISTENING  388
Schedule
[svchost.exe]
TCP     0.0.0.0:49668           0.0.0.0:0           LISTENING  1960
[spoolsv.exe]
TCP     0.0.0.0:49669           0.0.0.0:0           LISTENING  656
[lsass.exe]
TCP     0.0.0.0:49670           0.0.0.0:0           LISTENING  636
Impossibile ottenere informazioni sulla proprietà
TCP     10.0.2.15:139           0.0.0.0:0           LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP     10.0.2.15:59449         4.207.247.138:443   ESTABLISHED 388
BITS
[svchost.exe]
TCP     10.0.2.15:59638         4.207.247.138:443   ESTABLISHED 388
BITS
```

Usiamo il comando netstat -abno per vedere processi associati alle connessioni tcp attive



Apriamo il task manager e cerchiamo il PID 860



Dalla scheda dettagli possiamo vedere varie info relative al processo in esecuzione, come riportato in immagine

- Parte 5 Svuotare il cestino usando PowerShell.

Partiamo aggiungendo 2 txt nel cestino

```
PS C:\Users\eris> 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"): T  
PS C:\Users\eris>
```

Eseguiamo questo comando. in seguito apriamo nuovamente il cestino e notiamo che i file sono stati eliminati