# Esercitazione del venerdi

## Introduzione

In questa esercitazione ho analizzato e testato le funzionalità di Windows PowerShell confrontandole con il tradizionale Prompt dei Comandi. L'obiettivo principale è stato dimostrare la versatilità di PowerShell non solo come semplice interprete di comandi, ma come un potente framework di automazione e scripting orientato agli oggetti, essenziale per l'amministrazione di sistema e l'analisi di sicurezza.

## Strumenti Utilizzati

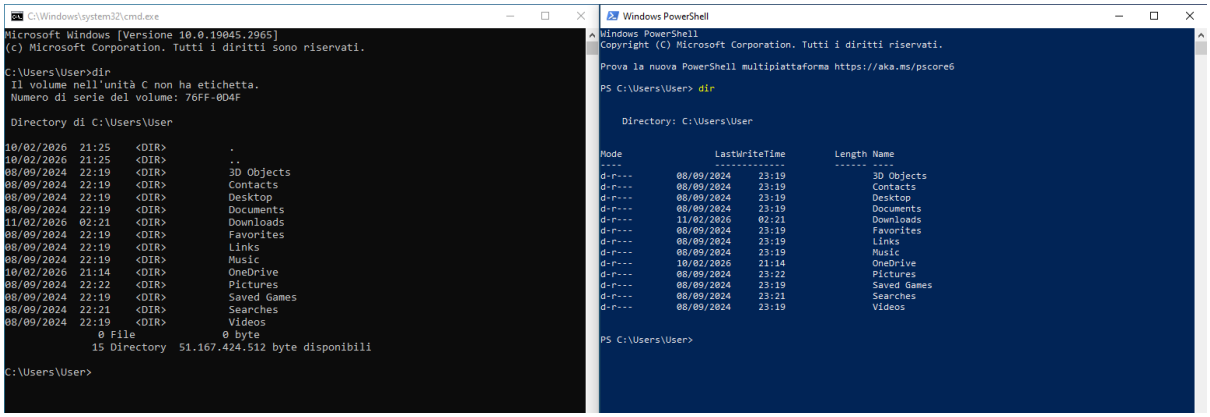
- **Sistema Operativo:** Windows (macchina virtuale).
- **Interfacce a riga di comando:** Windows PowerShell, Prompt dei Comandi (CMD).
- **Strumenti di monitoraggio:** Gestione Attività (Task Manager) di Windows.

## Svolgimento

### Parte 1 e 2: Accesso e confronto tra Prompt dei Comandi e PowerShell

Come primo passo ho avviato entrambe le console dal menu Start. Visivamente, PowerShell si distingue per il tipico sfondo blu e per il prefisso PS nel prompt che indica chiaramente l'ambiente in cui mi trovo.

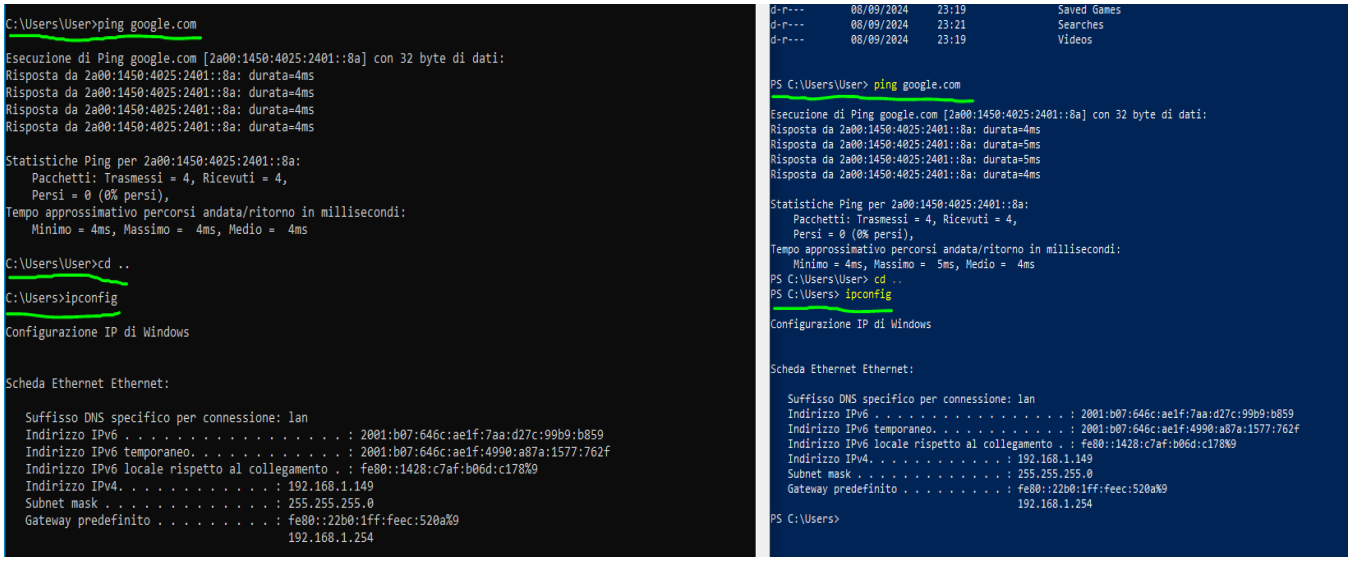
Ho iniziato eseguendo il comando dir in entrambe le finestre.




## Quali sono gli output del comando dir?

A prima vista gli output sembrano quasi identici, entrambi mostrano la lista dei file e delle directory presenti nella cartella corrente. Tuttavia c'è una profonda differenza, nel Prompt dei comandi dir è un comando nativo che restituisce semplice testo. In PowerShell dir funziona solo per retrocompatibilità ed è in realtà un Alias a un cmdlet specifico e non restituisce stringhe di testo ma oggetti manipolabili.

In seguito ho eseguito comandi di rete e di sistema standard:

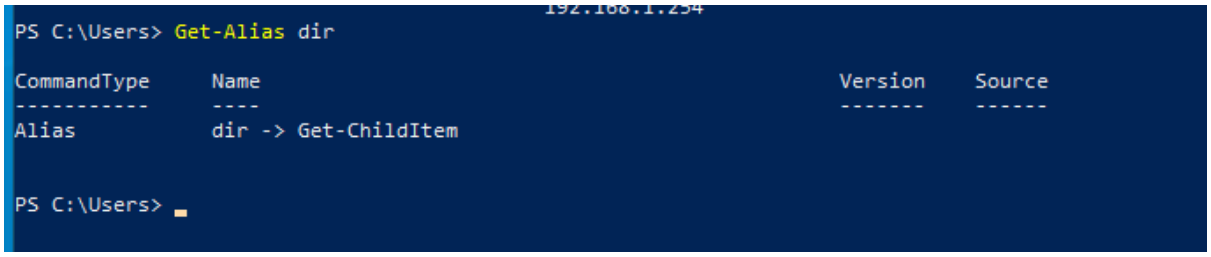



## Quali sono i risultati?

I comandi sono stati eseguiti correttamente producendo lo stesso risultato. Questo dimostra che PowerShell è in grado di invocare eseguibili standard di Windows (come ping.exe o ipconfig.exe) in modo trasparente.

## Parte 3: Esplorare i cmdlet

Ho interrogato il sistema sugli alias usando la sintassi Verbo-Nome tipica di PowerShell:

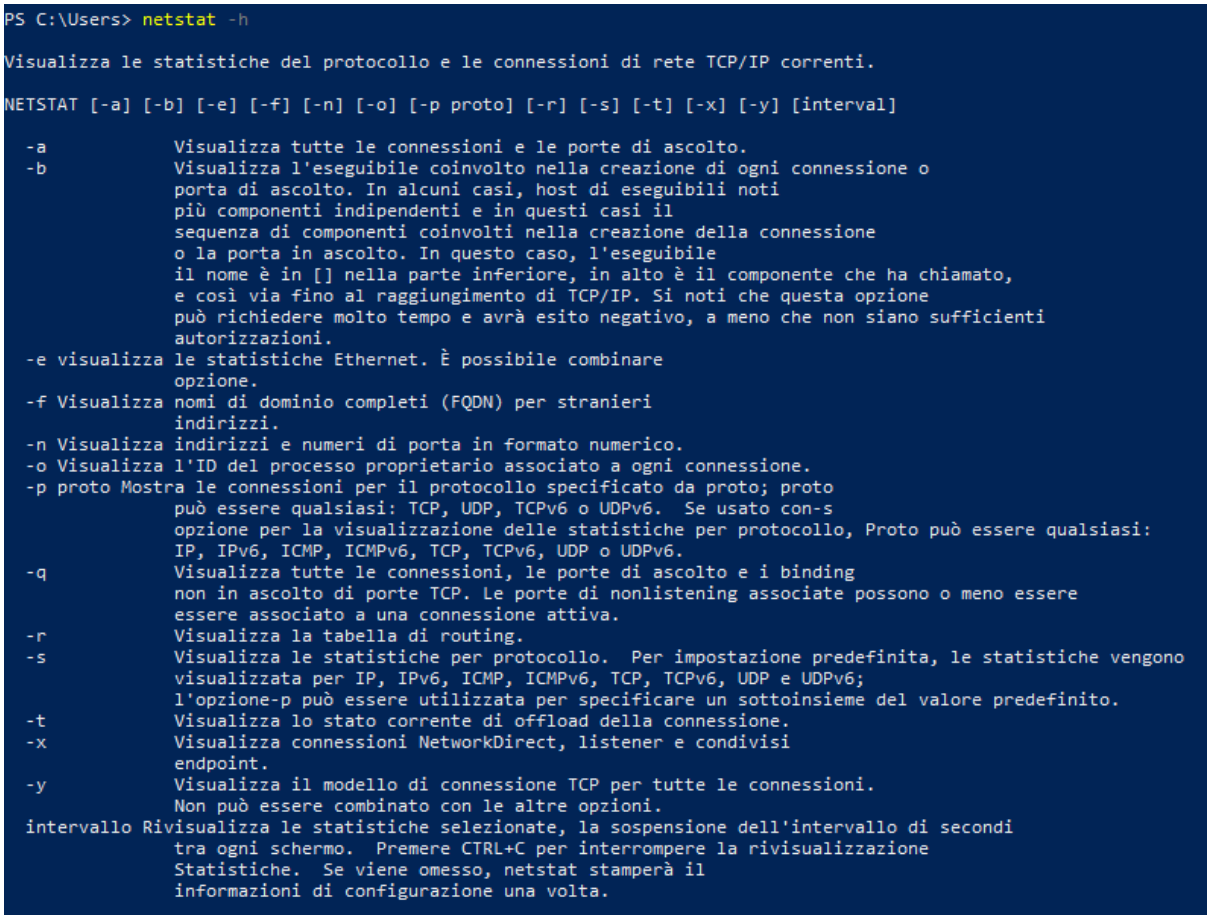



### Qual è il comando PowerShell per dir?

L'output del comando ha confermato che dir è semplicemente un alias per il cmdlet Get-ChildItem. Questo è un dettaglio cruciale, PowerShell usa alias per non disorientare gli utenti Linux (supporta anche ls) e gli utenti DOS (dir), ma il motore sottostante elabora sempre il comando Get-ChildItem.

## Parte 4: Esplorare il comando netstat

A questo punto ho chiuso il CMD per concentrarmi sull'analisi di rete tramite PowerShell. Ho esplorato la documentazione del comando netstat eseguendo netstat –h :



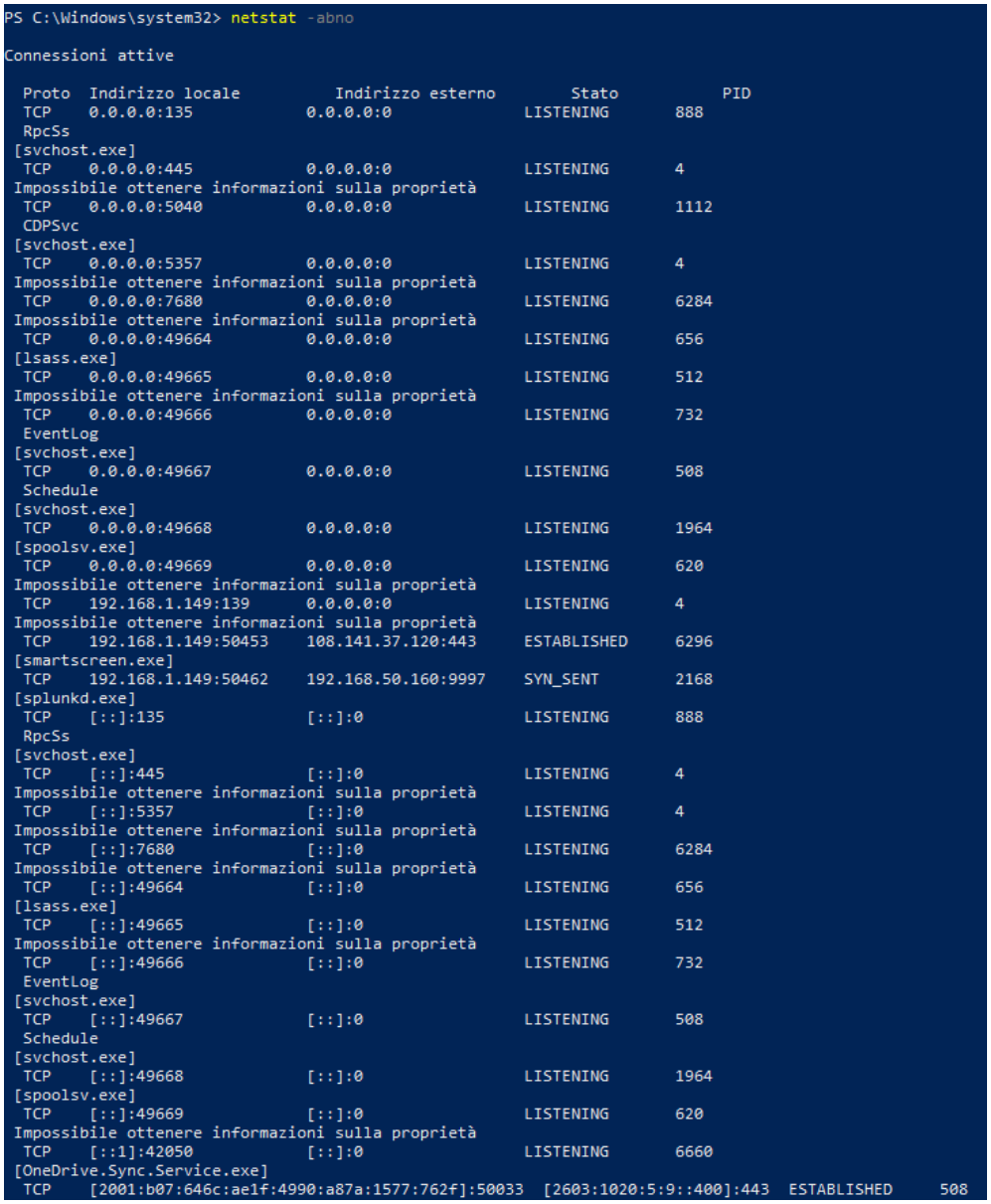

Successivamente, per analizzare la tabella di routing locale ho eseguito:

```
PS C:\Users> netstat -r
===========================================================================
Elenco interfacce
  9...08 00 27 5e df b8 ......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    192.168.1.254    192.168.1.149     25
        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
      192.168.1.0    255.255.255.0         On-link     192.168.1.149    281
    192.168.1.149  255.255.255.255         On-link     192.168.1.149    281
    192.168.1.255  255.255.255.255         On-link     192.168.1.149    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     192.168.1.149    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     192.168.1.149    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  9    281 ::/0                     fe80::22b0:1ff:feec:520a
  1    331 ::1/128                  On-link
  9    281 2001:b07:646c:ae1f::/64  On-link
  9    281 2001:b07:646c:ae1f::/64  fe80::22b0:1ff:feec:520a
  9    281 2001:b07:646c:ae1f:7aa:d27c:99b9:b859/128
                                    On-link
  9    281 2001:b07:646c:ae1f:4990:a87a:1577:762f/128
                                    On-link
  9    281 fe80::/64                On-link
  9    281 fe80::1428:c7af:b06d:c178/128
                                    On-link
  1    331 ff00::/8                 On-link
  9    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

## Qual è il gateway IPv4?

Analizzando l'output sotto la sezione "IPv4 Tabella route" ho cercato la riga dove l'Indirizzo di rete è 0.0.0.0 (la route di default). Il valore corrispondente nella colonna "Gateway" rappresenta l'indirizzo IP del mio router (essendo in Scheda con bridge il gateway e quello del mio router).

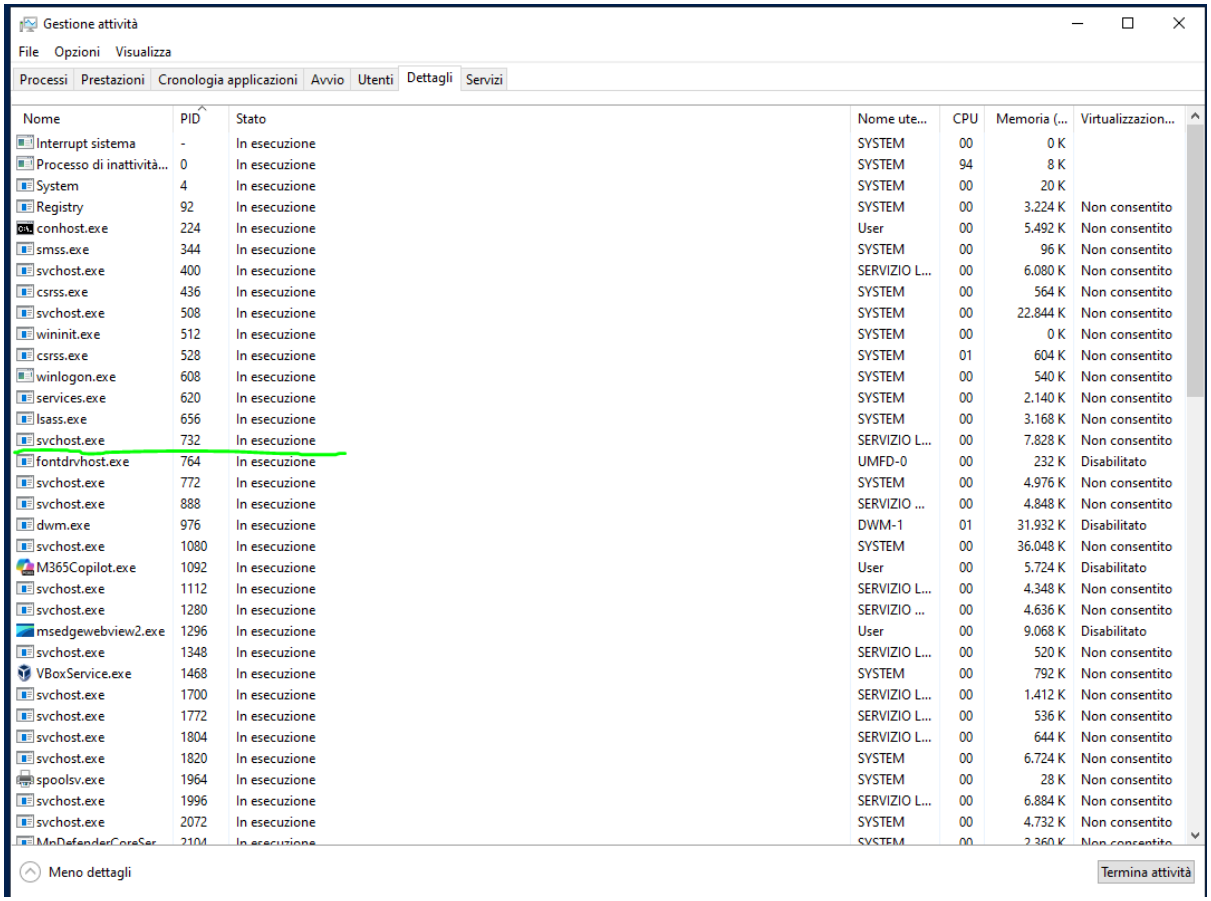
Per un'analisi di sicurezza più profonda ho dovuto elevare i privilegi. Ho riaperto PowerShell come **Amministratore** ed eseguito un comando che mappa le porte aperte ai rispettivi eseguibili e Process ID (PID):



```
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       888
  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       1112
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       6284
 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       512
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       732
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       508
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1964
 [spoolsv.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       620
 Impossibile ottenere informazioni sulla proprietà
  TCP    192.168.1.149:139      0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    192.168.1.149:50453    108.141.37.120:443     ESTABLISHED     6296
 [smartscreen.exe]
  TCP    192.168.1.149:50462    192.168.50.160:9997    SYN_SENT        2168
 [splunkd.exe]
  TCP    [::]:135               [::]:0                 LISTENING       888
  RpcSs
 [svchost.exe]
  TCP    [::]:445               [::]:0                 LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    [::]:5357              [::]:0                 LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    [::]:7680              [::]:0                 LISTENING       6284
 Impossibile ottenere informazioni sulla proprietà
  TCP    [::]:49664             [::]:0                 LISTENING       656
 [lsass.exe]
  TCP    [::]:49665             [::]:0                 LISTENING       512
 Impossibile ottenere informazioni sulla proprietà
  TCP    [::]:49666             [::]:0                 LISTENING       732
  EventLog
 [svchost.exe]
  TCP    [::]:49667             [::]:0                 LISTENING       508
  Schedule
 [svchost.exe]
  TCP    [::]:49668             [::]:0                 LISTENING       1964
 [spoolsv.exe]
  TCP    [::]:49669             [::]:0                 LISTENING       620
 Impossibile ottenere informazioni sulla proprietà
  TCP    [::1]:42050            [::]:0                 LISTENING       6660
 [OneDrive.Sync.Service.exe]
  TCP    [2001:b07:646c:ae1f:4990:a87a:1577:762f]:50033  [2603:1020:5:9::400]:443  ESTABLISHED     508
```

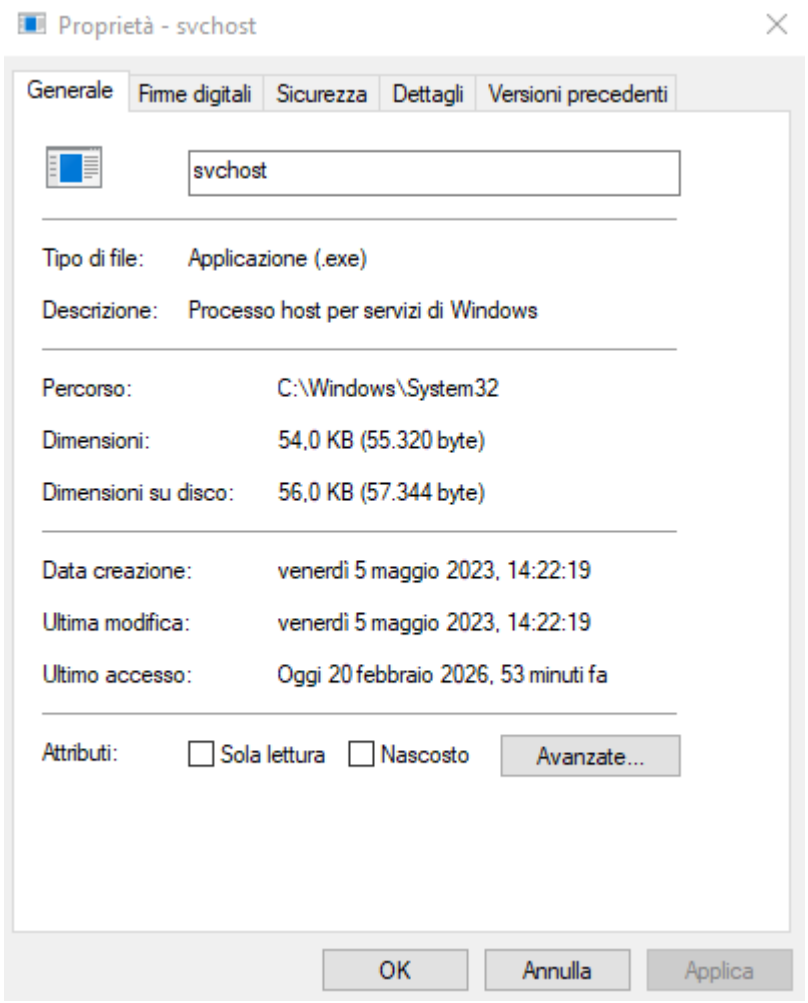
i flag usati sono fondamentali: -a mostra tutte le connessioni, -b mostra l'eseguibile coinvolto, -n evita la risoluzione DNS lenta mostrando IP numerici, e -o espone il PID

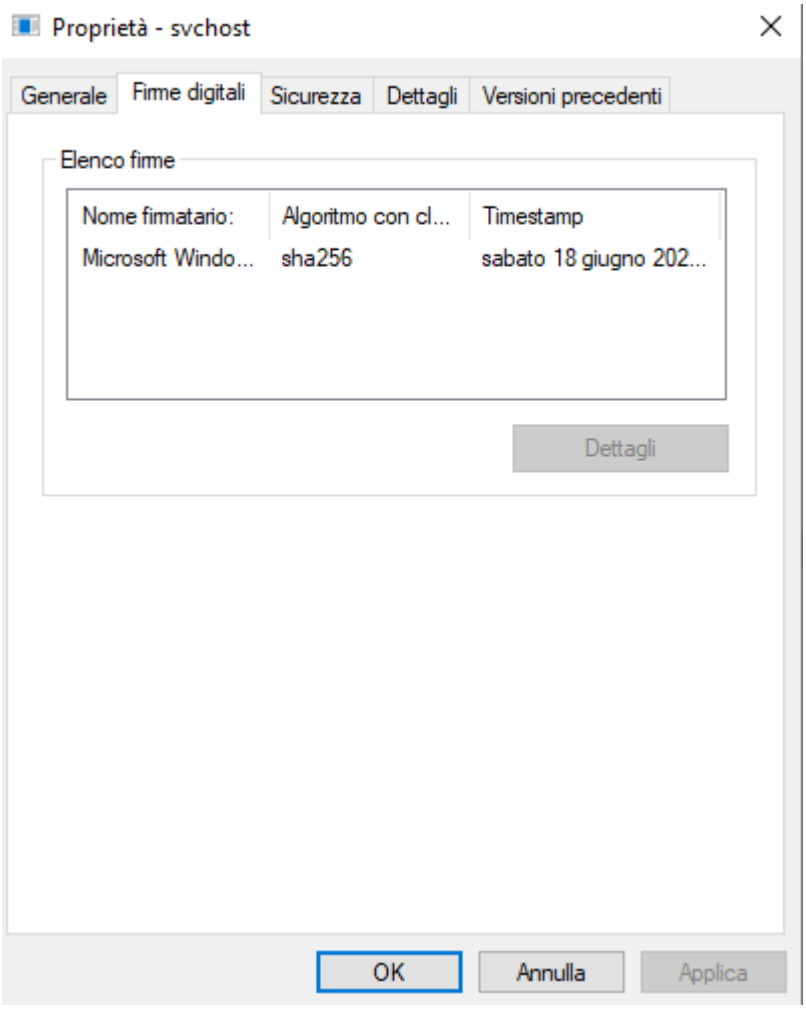
Ho selezionato un PID associato a uno stato "LISTENING" (PID 732) e ho aperto il Task Manager (Gestione Attività) spostandomi sulla scheda Dettagli per indagare.




## Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato?

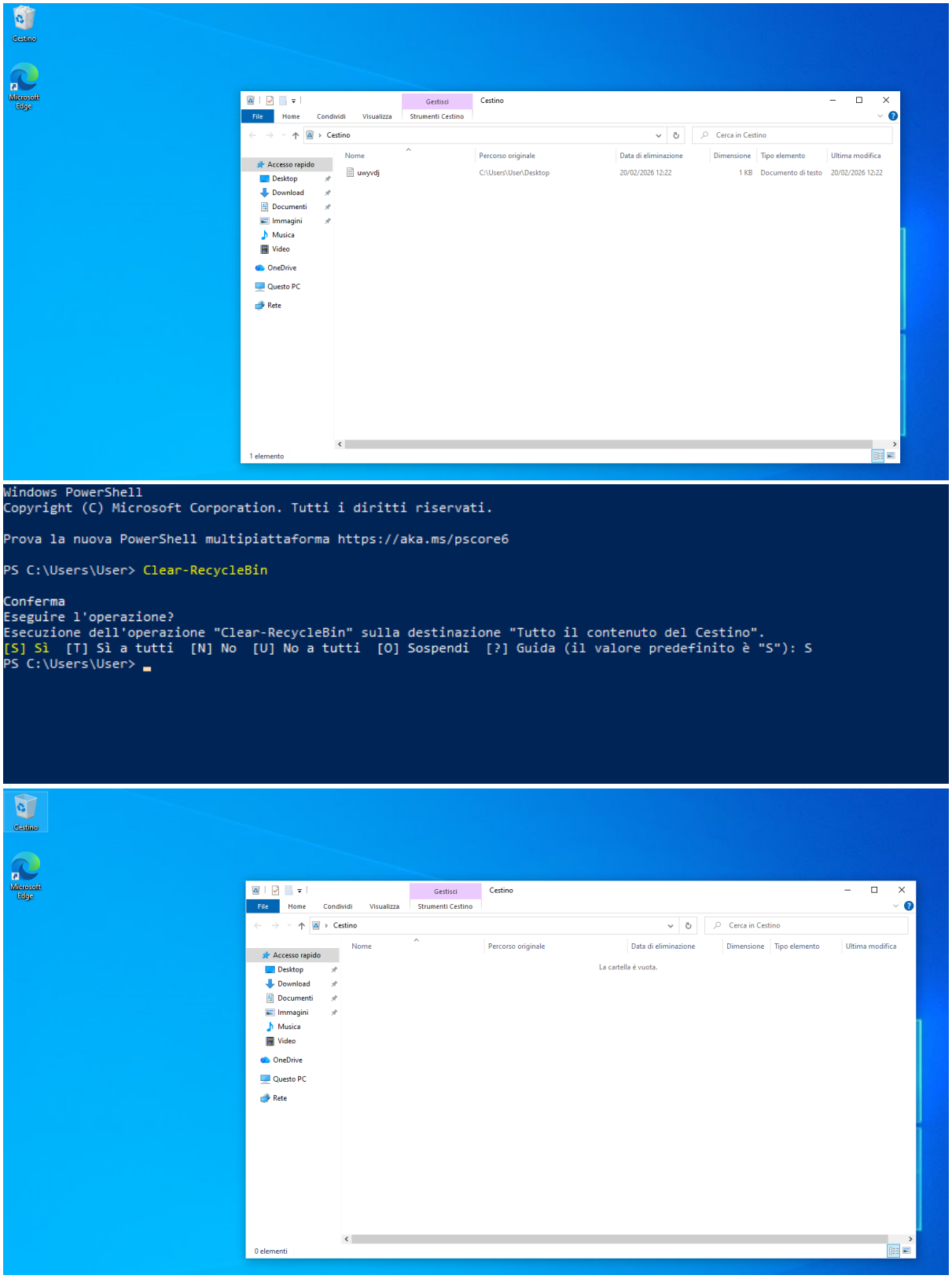
La scheda Dettagli mi fornisce un'istantanea operativa: posso vedere il nome esatto dell'eseguibile (svchost.exe), chi lo sta eseguendo (Servizio Locale), quanta CPU e memoria sta consumando. Facendo clic destro e andando in Proprietà le informazioni diventano cruciali per l'analisi forense e di sicurezza. Posso verificare il percorso fisico del file su disco (per assicurarmi che non sia un malware nascosto in una cartella temporanea), le firme digitali (per confermare che il file sia effettivamente prodotto da Microsoft o da un vendor fidato), la versione del file e le date di creazione/modifica.


Proprietà - svchost
Generale
Firme digitali
Sicurezza
Dettagli
Versioni precedenti
svchost
Tipo di file: Applicazione (.exe)
Descrizione: Processo host per servizi di Windows
Percorso: C:\Windows\System32
Dimensioni: 54,0 KB (55.320 byte)
Dimensioni su disco: 56,0 KB (57.344 byte)
Data creazione: venerdì 5 maggio 2023, 14:22:19
Ultima modifica: venerdì 5 maggio 2023, 14:22:19
Ultimo accesso: Oggi 20 febbraio 2026, 53 minuti fa
Attributi: Sola lettura Nascosto Avanzate...
OK
Annulla
Applica




## Parte 5: Svuotare il cestino tramite automazione

L'ultimo test ha riguardato la manipolazione del file system. Ho creato un file di testo sul desktop e l'ho spostato nel Cestino. Invece di usare l'interfaccia grafica ho svuotato il cestino da terminale:




## Cosa è successo ai file nel Cestino?

I file sono stati eliminati definitivamente. Questo comando è estremamente utile se integrato in uno script di manutenzione

programmata per liberare spazio sui server di una rete aziendale senza alcun intervento manuale da parte dell'amministratore.

### Domanda di Riflessione: PowerShell per un Analista di Sicurezza

Essendo PowerShell un framework così profondo, è l'arma definitiva per un analista di sicurezza. Ricercando online ho identificato tre cmdlet fondamentali che potrei usare quotidianamente nel mio lavoro per semplificare le indagini:

1. **Get-FileHash**: Estremamente utile per l'analisi dei malware. Permette di calcolare l'hash (es. SHA256) di un file sospetto per poi confrontarlo con database di threat intelligence come VirusTotal.
    a. Esempio: Get-FileHash -Path C:\sospetto.exe -Algorithm SHA256
2. **Get-WinEvent** (o il più vecchio Get-EventLog): Sostituisce la consultazione del Visualizzatore Eventi grafico. Permette di filtrare rapidamente migliaia di log di sicurezza alla ricerca di ID specifici (es. tentativi di login falliti - Event ID 4625).
3. **Get-NetTCPConnection**: L'alternativa nativa orientata agli oggetti a netstat. Essendo a oggetti permette di filtrare i risultati molto più facilmente, ad esempio mostrando solo le connessioni stabilite su determinate porte.

## Conclusione

Questo laboratorio pratico in ambiente VirtualBox ha evidenziato in modo inequivocabile la superiorità di PowerShell rispetto al classico Prompt dei comandi. Mentre CMD è utile per compiti basilari e rapidi, PowerShell rappresenta un ambiente di scripting robusto, capace di dialogare direttamente con il core del sistema operativo Windows, il Registro di sistema e le interfacce di rete. La sua struttura basata su oggetti (e non su testo) e l'adozione del paradigma Verbo-Nome lo rendono uno strumento imprescindibile per chiunque voglia fare seriamente System Administration, Incident Response o Threat Hunting nel mondo moderno.