Esercizio_S10_L5_ PowerShell

Consegna

L'obiettivo del laboratorio è esplorare alcune delle funzioni di PowerShell.

- Parte 1 Accedere alla console PowerShell.
- Parte 2 Esplorare i comandi del Prompt dei Comandi e di PowerShell.
- Parte 3 Esplorare i cmdlet.
- Parte 4 Esplorare il comando netstat usando PowerShell.
- Parte 5 Svuotare il cestino usando PowerShell.

Contesto / Scenario

PowerShell è un potente strumento di automazione. È sia una console di comando che un linguaggio di scripting. In questo laboratorio, userai la console per eseguire alcuni dei comandi disponibili sia nel prompt dei comandi che in PowerShell.
PowerShell ha anche funzioni che possono creare script per automatizzare compiti e lavorare insieme al Sistema Operativo Windows.

Risorse Richieste: 1 PC Windows con PowerShell installato e accesso a internet

Svolgimento

Quali sono gli output del comando dir?

Il comando dir restituisce i file e le cartelle presenti all'interno della directory corrente; è l'equivalente di ls su linux.

Prova un altro comando che hai usato nel prompt dei comandi, come ping, cd e ipconfig. Quali sono i risultati?

ping Invia pacchetti ICMP a un host per verificare la connettività di rete.

cd Cambia directory corrente.

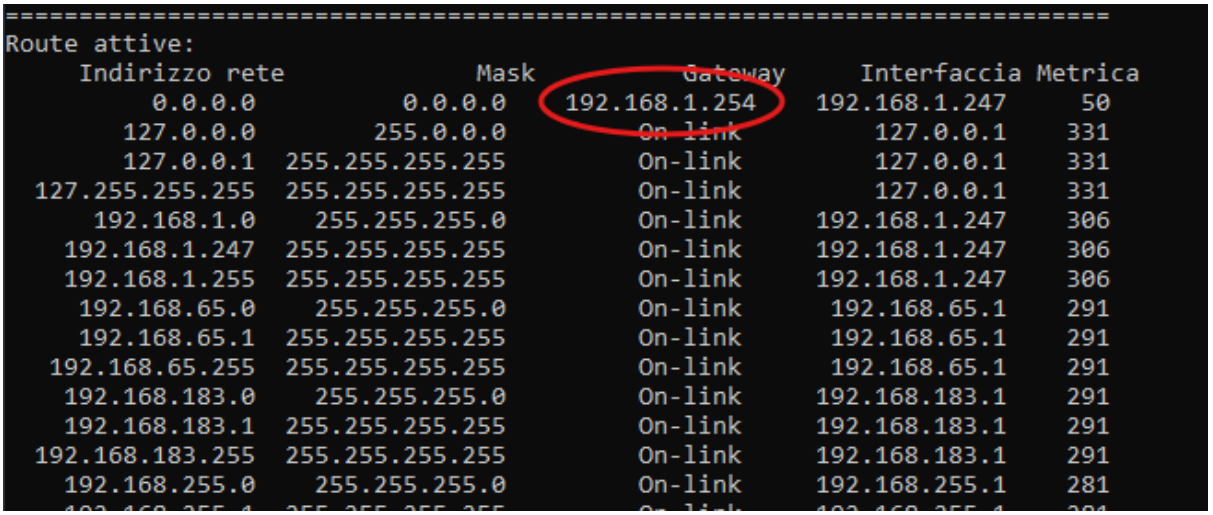
ipconfig Mostra la configurazione di rete del computer.

Qual è il comando PowerShell per dir?

Eseguendo il comando get-alias dir otteniamo come risultato che dir è l'alias di Get-ChildItem.

Inserisci netstat -r al prompt. Qual è il gateway IPv4?

Dopo aver digitato il comando netstar -r è parso chiaro che il mio indirizzo gateway IPV4 fosse 192.168.1.254.



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

La finestra proprietà permette di vedere informazioni più dettagliate sull'eseguibile e sul file che ha originato il processo:

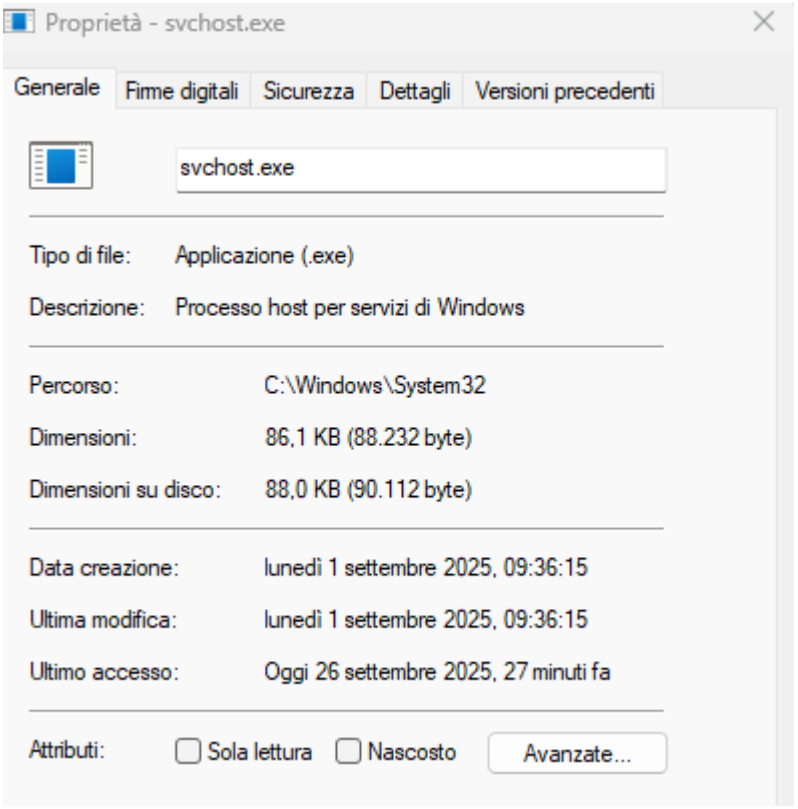
- Nella scheda generale possiamo trovare il **Percorso del file** → la directory completa in cui si trova l'eseguibile (utile per distinguere software legittimi da potenziali malware), **Dimensione e versione del file** → dettagli tecnici forniti dal produttore e altre informazioni utili quali data creazione, ultima modifica ecc.. .

- Nella scheda Firma digitale troviamo la sessione che indica se l'eseguibile è firmato ed eventualmente da chi.

- Nella scheda Sicurezza troviamo i vari permessi.

- Nella scheda Dettagli troviamo un riassunto di quanto principalmente è presente all'interno di Generale.

- Nella scheda Versioni precedenti troviamo eventuali versioni dalle quali poter effettuare il ripristino dell'applicazione ispezionata.



La scheda dettagli indica invece informazioni tecniche sui processi in esecuzione. Dal PID selezionato puoi ottenere:

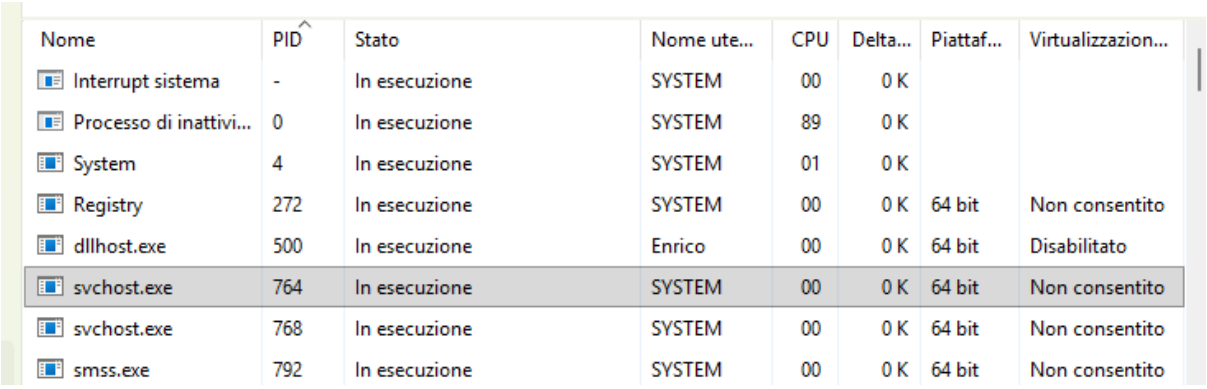
- Nome mostra il nome del file eseguibile associato al processo.
- PID (Process ID) mostra l'identificatore numerico unico del processo.
- Stato indica se il processo è in esecuzione, sospeso, ecc.
- Nome utente mostra l'account con cui gira il processo.
- CPU rappresenta quante risorse consuma il processo.
- Piattaforma Indica l'architettura con cui il processo è stato avviato (64 bit o 32 bit).
- Virtualizzazione UAC mostra se la funzionalità di User Account Control (UAC) Virtualization è attiva per quel processo. Serve a ridirigere scritture su percorsi protetti (come C:\Program Files) in cartelle alternative dell'utente, per compatibilità con vecchie applicazioni.

  Valori possibili:

  Non consentito → processo che non supporta o non ha bisogno della virtualizzazione.

  Disabilitato → supportata ma spenta (ad esempio perché il processo gira come amministratore).

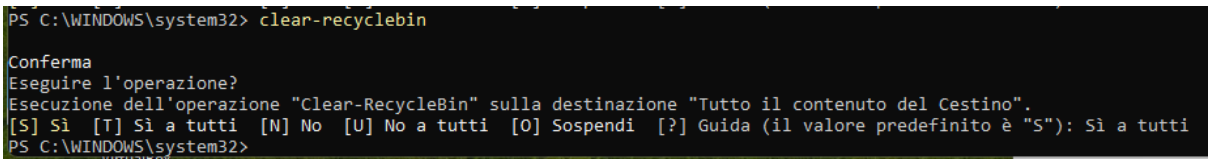
  Abilitato → la virtualizzazione è attiva.



Nome	PID	Stato	Nome ute...	CPU	Delta...	Piattaf...	Virtualizzazion...
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K		
Processo di inattivi...	0	In esecuzione	SYSTEM	89	0 K		
System	4	In esecuzione	SYSTEM	01	0 K		
Registry	272	In esecuzione	SYSTEM	00	0 K	64 bit	Non consentito
dllhost.exe	500	In esecuzione	Enrico	00	0 K	64 bit	Disabilitato
svchost.exe	764	In esecuzione	SYSTEM	00	0 K	64 bit	Non consentito
svchost.exe	768	In esecuzione	SYSTEM	00	0 K	64 bit	Non consentito
smss.exe	792	In esecuzione	SYSTEM	00	0 K	64 bit	Non consentito

Cosa è successo ai file nel Cestino?

Dopo aver utilizzato il comando clear-recyclebin ed aver confermato di voler estendere l'azione a tutti gli elementi del cestino, il cestino viene ovviamente svuotato.



Domanda di Riflessione: PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

Per l'analisi degli eventi parto da Get-WinEvent, perché filtra in modo nativo e quindi è rapido anche su macchine rumorose: ad esempio Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625; StartTime=(Get-Date).AddDays(-1)} isola i logon falliti delle ultime 24 ore; lo uso quando devo validare un sospetto brute force. Per capire subito cosa "brucia" la macchina in termini di risorse passo a Get-Process e ordino per CPU o memoria: Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 mi evidenzia i candidati anomali; è utile nel triage di persistenze rumorose o miner.

Sul fronte rete, Get-NetTCPConnection mostra le sessioni con IP/porte/stato: con Get-NetTCPConnection -State Established | Sort-Object RemoteAddress,RemotePort ottengo una fotografia delle connessioni attive e riconosco endpoint insoliti. Per test puntuali di raggiungibilità e porte uso Test-NetConnection: Test-NetConnection -ComputerName example.com -Port 443 -InformationLevel Detailed, mentre per il "ping" scriptabile ad alta fedeltà sfrutto Test-Connection. Quando devo validare indicatori DNS si può utilizzare Resolve-DnsName: Resolve-DnsName malware.test -Server 8.8.8.8 -Type A mi dà record, TTL ed errori, utile per distinguere cache locale da risoluzioni autorevoli.

Il contenimento minimo lato host lo affronto con il firewall integrato: Get-NetFirewallRule -Enabled True | Select DisplayName,Direction,Action mi fa audit rapido; se serve bloccare un IOC specifico creo al volo una regola con New-NetFirewallRule -DisplayName "Contain IOC" -Direction Outbound -Action Block -RemoteAddress 1.2.3.4 -RemotePort 4444 -Protocol TCP. Per verificare integrità e alimentare confronti con feed IOC, Get-FileHash è lo standard: con Get-ChildItem C:\suspect -Recurse -File | Get-FileHash -Algorithm SHA256 | Export-Csv C:\suspect\hashes.csv -NoTypeInformation genero un inventario hash pronto da correlare. Infine, per lo stato antimalware e una scansione rapida senza uscire dalla console, Start-MpScan -ScanType QuickScan avvia la verifica e Get-MpComputerStatus | Select AMServiceEnabled,AntivirusEnabled,SignatureLastUpdated,QuickScanStartTime mi riassume la postura di Microsoft Defender.

In pratica, questi cmdlet coprono l'80% delle richieste tipiche ovvero **leggere eventi in modo mirato, individuare processi anomali, mappare e testare la rete, applicare un contenimento di base, validare file con hash e verificare l'AV**.

Cmdlet	Scopo principale	Esempio pratico	Utilità per la sicurezza
Get-WinEvent	Leggere eventi dai log di Windows	Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625; StartTime=(Get-Date).AddDays(-1)}	Identificare logon falliti o eventi critici
Get-Process	Elencare e analizzare processi attivi	Get-Process | Sort-Object CPU -Descending | Select-Object -First 10	Individuare processi anomali o ad alto consumo
Get-NetTCPConnection	Mostrare connessioni TCP attive	Get-NetTCPConnection -State Established	Scoprire connessioni sospette verso host remoti
Test-NetConnection	Test connettività e porte TCP	Test-NetConnection -ComputerName example.com -Port 443 -InformationLevel Detailed	Verificare apertura porte critiche (es. HTTPS)
Resolve-DnsName	Risolvere nomi DNS	Resolve-DnsName malware.test -Server 8.8.8.8 -Type A	Validare IoC DNS e controllare risposte dai resolver
Get-NetFirewallRule	Visualizzare regole firewall attive	Get-NetFirewallRule -Enabled True | Select DisplayName,Direction, Action	Audit delle regole di rete

New-NetFirewallRule	Creare regole firewall	New-NetFirewallRule -DisplayName "Contain IOC" -Direction Outbound -Action Block -RemoteAddress 1.2.3.4 -RemotePort 4444 -Protocol TCP	Bloccare traffico malevolo mirato
Get-FileHash	Calcolare hash di file (es. SHA256)	Get-ChildItem C:\suspect -Recurse -File | Get-FileHash -Algorithm SHA256	Confrontare file con baseline o feed IOC
Start-MpScan	Avviare scansione Microsoft Defender	Start-MpScan -ScanType QuickScan	Eseguire scansione veloce in caso di sospetto
Get-MpComputerStatus	Verificare stato di Microsoft Defender	Get-MpComputerStatus | Select AntivirusEnabled,SignatureLastUpdated	Controllare che l'antivirus sia attivo e aggiornato