

S11 L5 - Analisi avanzate: Un approccio pratico - Lab 1

3.3.11 Lab – Utilizzo di Windows PowerShell (Risposte)

L'obiettivo del laboratorio:

- **Parte 1:** accedere alla console di PowerShell.
- **Parte 2:** Esplora i comandi del prompt dei comandi e di PowerShell.
- **Parte 3:** Esplora i cmdlet.
- **Parte 4:** Esplora il comando netstat utilizzando PowerShell.
- **Parte 5:** Svuotare il cestino tramite PowerShell.

Parte 1: accedere alla console di PowerShell.

- a. Fare clic su **Start** . Cerca e seleziona **PowerShell** .
- b. Fare clic su **Start** . Cerca e seleziona **prompt dei comandi** .

Parte 2: Esplora i comandi del prompt dei comandi e di PowerShell.

- a. Immettere **dir** al prompt in entrambe le finestre.

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

Directory: C:\Users\Brbsm

Mode                LastWriteTime         Length Name
----                -
d-----          28/11/2024    20:42             .idlerc
d-----          05/11/2024    20:07             .ms-ad
d-----          29/01/2025    18:38             .VirtualBox
d-----          15/11/2024    11:56             .vscode
d-----          27/11/2024    23:42             .zenmap
d-r-----        27/11/2024    11:46          3D Objects
d-----          07/12/2024    01:39 Cisco Packet Tracer 8.2.2
d-r-----        10/10/2024    19:02          Contacts
d-r-----        31/01/2025    10:42          Desktop
d-r-----        24/01/2025    01:47          Documents
d-r-----        30/01/2025    22:13          Downloads
d-r-----        10/10/2024    19:02          Favorites
d-----        12/10/2024    18:53             GNS3
d-r-----        10/10/2024    19:02             Links
d-r-----        10/10/2024    19:02             Music
dar--l          31/01/2025    08:45          OneDrive
d-r-----        05/11/2024    17:03          Pictures
d-r-----        10/10/2024    19:02          Saved Games
d-r-----        24/01/2025    01:47          Searches
d-r-----        12/10/2024    17:15          Videos
d-----        28/01/2025    11:33 VirtualBox VMs
-a-----        04/11/2024    17:52           195 .gitconfig
-a-----        07/12/2024    01:30          212 .packettracer
-a-----        02/01/2025    12:11           0 Get-ItemProperty
```

```
Prompt dei comandi
C:\Users\Brbsm>dir
Il volume nell'unità C è Windows
Numero di serie del volume: E535-4FA0

Directory di C:\Users\Brbsm

31/01/2025 08:45 <DIR> .
02/01/2025 13:08 <DIR> ..
04/11/2024 17:52             195 .gitconfig
28/11/2024 20:42 <DIR> .idlerc
05/11/2024 20:07 <DIR> .ms-ad
07/12/2024 01:30             212 .packettracer
29/01/2025 18:38 <DIR> .VirtualBox
15/11/2024 11:56 <DIR> .vscode
27/11/2024 23:42 <DIR> .zenmap
27/11/2024 11:46 <DIR> 3D Objects
07/12/2024 01:39 <DIR> Cisco Packet Tracer 8.2.2
10/10/2024 18:02 <DIR> Contacts
31/01/2025 10:42 <DIR> Desktop
24/01/2025 01:47 <DIR> Documents
30/01/2025 22:13 <DIR> Downloads
10/10/2024 19:02 <DIR> Favorites
12/10/2024 17:15 <DIR> GNS3
10/10/2024 19:02 <DIR> Links
10/10/2024 19:02 <DIR> Music
04/11/2024 17:52 <DIR> OneDrive
05/11/2024 17:03 <DIR> Pictures
10/10/2024 18:02 <DIR> Saved Games
24/01/2025 01:47 <DIR> Searches
12/10/2024 16:15 <DIR> Videos
28/01/2025 11:33 <DIR> VirtualBox VMs
3 File(s)          407 byte(s)

disponibili
```

Quali sono gli output del **dir** comando?

Entrambe le finestre forniscono un elenco di sottodirectory e file, e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell, vengono mostrati anche gli attributi/modalità.

Inserendo i seguenti comandi: ping, cd e ipconfig riceviamo lo stesso input.

Parte 3: Esplora i cmdlet.

Qual è il comando PowerShell per **dir** ?

```
PS C:\Users\Brbsm> get-alias dir

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

Utilizzando il prompt dei comandi invece il comando non è riconosciuto:

```
C:\Users\Brbsm>get-alias dir
"get-alias" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.
```

Parte 4: Esplora il comando netstat utilizzando PowerShell.

Al prompt di PowerShell, premere Invio **netstat -h** per visualizzare le opzioni disponibili per il **netstat** comando.

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

Visualizza statistiche relative ai protocolli e alle connessioni di rete TCP/IP correnti.

NETSTAT[-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a          Visualizza tutte le connessioni e le porte di ascolto.
-b          Visualizza il file eseguibile utilizzato per la creazione di ogni connessione o
            porta di ascolto. Alcuni file eseguibili conosciuti includono
```

Per visualizzare la tabella di routing con i percorsi attivi, digitare **netstat -r** al prompt.

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

=====
Elenco interfacce
.....Realtek PCIe GbE Family Controller
.....VirtualBox Host-Only Ethernet Adapter
.....Microsoft Wi-Fi Direct Virtual Adapter
.....Microsoft Wi-Fi Direct Virtual Adapter #2
.....Realtek RTL8821CE 802.11ac PCIe Adapter
.....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway      Interfaccia Metrica
0.0.0.0             0.0.0.0
```

Qual' è gateway IPv4?

Il gateway è `***.***.***.1` in questo esempio.

Esecuzione di una PowerShell con privilegi elevati.

Il comando `netstat` può anche visualizzare i processi associati alle connessioni TCP attive. Digitare al `netstat -abno` prompt.

```
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  1276
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  6616
CDPSvc
[svchost.exe]
```

Apri Task Manager. Vai alla scheda Dettagli . Fai clic sull'intestazione PID in modo che i PID siano in ordine.

Individuare il PID selezionato nel Task Manager. Fare clic con il pulsante destro del mouse sul PID selezionato nel Task Manager per aprire la finestra di dialogo Proprietà per ulteriori informazioni.






Nome	PID [^]	Stato	Nome utente	CPU	Memoria (...)	Architet...	Descriz
IntelCpHeciSvc.exe	2408	In esecuzione	SYSTEM	00	1.156 K	x64	IntelCp
wmlhost.exe	2496	In esecuzione	Brbsm	00	209.336 K	x64	Webex
svchost.exe	2516	In esecuzione	SERVIZIO DI RETE	00	4.524 K	x64	Process
svchost.exe	2528	In esecuzione	SYSTEM	00	1.340 K	x64	Process

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

Il PID 2516 è associato al processo `svchost.exe`. L'utente per questo processo è `SERVIZIO DI RETE` e sta utilizzando 4524K di memoria.

Parte 5: Svuotare il cestino tramite PowerShell.

Apri il Cestino. Verifica che ci siano elementi che possono essere eliminati in modo permanente dal tuo PC.

	1	C:\Users\Brbsm\Desktop\S11 L3
	2	C:\Users\Brbsm\Desktop\S11 L3
	3	C:\Users\Brbsm\Desktop\S11 L2
	4	C:\Users\Brbsm\Desktop\S11 L2
	5	C:\Users\Brbsm\Desktop\S11 L2

In una console di PowerShell, immettere `clear-recyclebin` al prompt.

```
PS C:\Users\Brbsm> 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"): s
PS C:\Users\Brbsm> |
```

Che fine hanno fatto i file nel Cestino?

I file vengono eliminati.

	Data di eliminazione	Dimensione	Tipo elemento	Ultima mo
La cartella è vuota.				

Domanda di riflessione

PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Utilizzando Internet, cerca i comandi che potresti usare per semplificare i tuoi compiti come analista della sicurezza.

PowerShell è uno strumento potente per gli analisti della sicurezza, consentendo l'automazione delle attività quotidiane e la gestione della configurazione. Ecco alcuni comandi utili:

- **Get-ExecutionPolicy** e **Set-ExecutionPolicy** : gestire le politiche di esecuzione degli script, controllando quali script possono essere eseguiti nel sistema.
- **Get-Service**: elenca tutti i servizi attivi sul sistema, utili per identificare i servizi sospetti o non autorizzati.
- **Get-Process**: fornisce informazioni sui processi in esecuzione, permettendo di monitorare attività anomale.
- **Stop-Process**: termina un processo specificato, utile per fermare attività dannose.
- **Get-EventLog**: accedere ai registri eventi di Windows, fondamentale per l'analisi forense e la rilevazione di incidenti.
- **Get-ADUser**: recupera informazioni sugli utenti di Active Directory, utile per audit e gestione degli accessi.
- **Resolve-DnsName**: esegue ricerche DNS, utile per analizzare attività di rete sospette.