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

3.3.11 Lab – Utilizzo di Windows PowerShell (Risposte)

L'obiettivo del laboratorio:

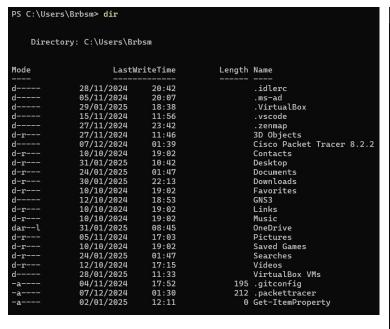
- Parte 1: accedere alla console di PowerShell.
- Parte 2: Esplora i comandi del prompt dei comandi e di PowerShell.
- Parte 3: Esplora i cmdlet.
- Parte 4: Esplora il comando netstat utilizzando PowerShell.
- Parte 5: Syuotare il cestino tramite PowerShell.

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.



Prompt dei	comandi	× +	~							
C:\Users\Brbsm>dir										
Il volume nell'unità C è Windows										
Numero di	serie del	volume:	E535-4F	-A0						
Directory	di C:\Use	rs\Brbsm								
24 /04 /2025	00 45	-DTD:								
31/01/2025	08:45	<dir></dir>								
02/01/2025	13:08	<dir></dir>	***							
04/11/2024	17:52		195	.gitconfig						
28/11/2024	20:42	<dir></dir>		.idlerc						
05/11/2024	20:07	<dir></dir>	040	.ms-ad						
07/12/2024	01:30		212	.packettrace	r					
29/01/2025	18:38	<dir></dir>		.VirtualBox						
15/11/2024		<dir></dir>		.vscode						
27/11/2024		<dir></dir>		.zenmap						
27/11/2024		<dir></dir>		3D Objects						
07/12/2024		<dir></dir>			Tracer 8.2.2					
10/10/2024		<dir></dir>		Contacts						
31/01/2025	10:42	<dir></dir>		Desktop						
24/01/2025	01:47	<dir></dir>		Documents						
30/01/2025		<dir></dir>		Downloads						
10/10/2024		<dir></dir>		Favorites						
02/01/2025	12:11		0	Get-ItemProp	erty					
12/10/2024		<dir></dir>		GNS3						
10/10/2024	18:02	<dir></dir>		Links						
10/10/2024	18:02	<dir></dir>		Music						
31/01/2025	08:45	<dir></dir>		OneDrive						
05/11/2024	17:03	<dir></dir>		Pictures						
10/10/2024		<dir></dir>		Saved Games						
24/01/2025	01:47	<dir></dir>		Searches						
12/10/2024		<dir></dir>		Videos						
28/01/2025	11:33	<dir></dir>		VirtualBox V	Ms					
	3 Eil	9	LINE	7 byte						
					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.

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
                                                 LISTENING
                                                               1276
 TCP
      0.0.0.0:135
                            0.0.0.0:0
 RpcSs
 [svchost.exe]
      0.0.0.0:445
                                                 LISTENING
                            0.0.0.0:0
 Impossibile ottenere informazioni sulla proprietà
      0.0.0.0:5040
 TCP
                           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.

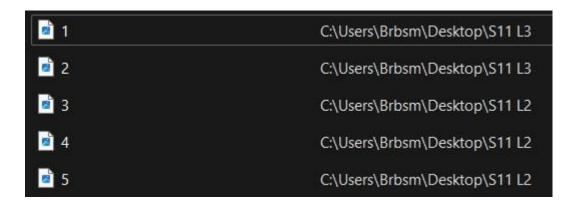
Nome	PID	Stato	Nome utente	CPU	Memoria (Architet	Descriz
■ IntelCpHeciSvc.exe	2408	In esecuzione	SYSTEM	00	1.156 K	x64	IntelCpl
wmlhost.exe	2496	In esecuzione	Brbsm	00	209.336 K	x64	Webex
svchost.exe	2516	In esecuzione	SERVIZIO DI RETE	.00	4.524 K	x64	Process
svchost.exe	2528	In esecuzione	SYSTEM	00	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: Syuotare il cestino tramite PowerShell.

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



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

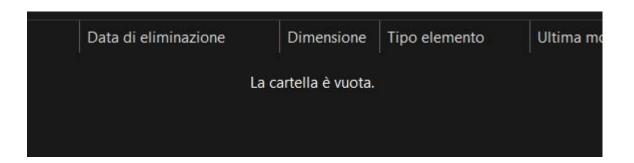
```
PS C:\Users\Brbsm> clear-recyclebin

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.



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.