**S11L5**

**Laboratorio - Utilizzo di Windows PowerShell In questo laboratorio, esploreremo alcune delle funzioni di PowerShell .**

[**https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html**](https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html)

**Introduzione**

Questo report documenta l'esecuzione del laboratorio "Utilizzo di Windows PowerShell", suddiviso in cinque parti principali. Lo scopo dell'attività è esplorare i comandi del Prompt dei comandi e di PowerShell, esaminare i cmdlet, utilizzare il comando netstat e gestire il Cestino tramite PowerShell.

**Parte 1: Accesso alla console di PowerShell**

1. Aperta la console di PowerShell tramite il menu Start.
2. Aperta la console di Prompt dei comandi (cmd) sempre tramite il menu Start.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Entrambe le console sono state avviate con successo.

**Parte 2: Esplorazione dei comandi del Prompt dei comandi e di PowerShell**

**Obiettivo**

Confrontare i comandi dir, cd, ipconfig tra Prompt dei comandi e PowerShell.

**Procedura**

1. Eseguito dir in entrambi gli ambienti.
2. Provati comandi comuni (cd .., ipconfig).
3. Osservato che alcuni comandi funzionano in entrambi gli ambienti, mentre PowerShell offre funzioni avanzate.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer program

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.



A screen shot of a computer program

AI-generated content may be incorrect.



A screen shot of a computer

AI-generated content may be incorrect.



Il gateway trovato è il gateway della vpn a cui sono connesso, nascosto per privacy

**Parte 3: Esplorazione dei cmdlet**

**Obiettivo**

Esaminare i cmdlet di PowerShell e il loro utilizzo.

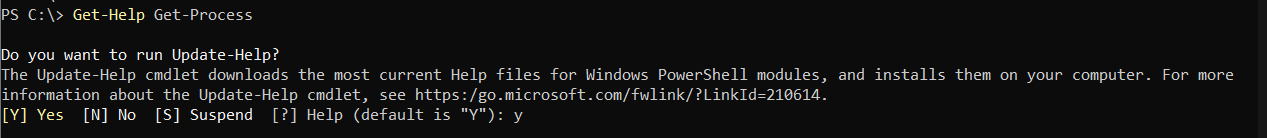
**Procedura**

1. Scoperto l'alias di dir usando Get-Alias dir.
2. Eseguito Get-ChildItem come alternativa a dir.
3. Utilizzato Get-Command per visualizzare l'elenco dei cmdlet disponibili.
4. Eseguito Get-Help Get-Process per visualizzare informazioni su un cmdlet specifico.

PowerShell fornisce una serie di cmdlet con funzionalità avanzate rispetto al Prompt dei comandi.

A screenshot of a computer program

AI-generated content may be incorrect.



A screenshot of a computer program

AI-generated content may be incorrect.

* dir: fornisce un output simile in entrambi gli ambienti.
* ipconfig: funziona correttamente in PowerShell e cmd.
* Alcuni comandi hanno alias in PowerShell.

**Parte 4: Esplorazione del comando netstat utilizzando PowerShell**

**Obiettivo**

Utilizzare netstat per monitorare le connessioni di rete.

**Procedura**

1. Eseguito netstat -h per elencare le opzioni disponibili.
2. Eseguito netstat -r per visualizzare la tabella di routing.
3. Avviata PowerShell come amministratore e eseguito netstat -abno.
4. Identificato un processo tramite il PID in **Gestione attività**.

**Risultati**

L'uso di netstat ha permesso di monitorare le connessioni e identificare i processi in ascolto sulla rete.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A computer screen shot of a route

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Parte 5: Svuotamento del Cestino utilizzando PowerShell**

**Obiettivo**

Svuotare il Cestino tramite PowerShell.

**Procedura**

1. Verificato il contenuto del Cestino.
2. Eseguito il comando Clear-RecycleBin.
3. Confermata l'operazione digitando Y.

Il Cestino può essere svuotato con successo tramite PowerShell.

A screen shot of a computer

AI-generated content may be incorrect.

Esercizio 2

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.

<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

L'analisi del file sospetto **Jvczfhe.exe** ha rivelato la creazione e l'interazione con diversi processi ed eseguibili nel sistema. Ecco un dettaglio specifico:

**Processi ed eseguibili:**

1. **Processo principale:**
   * **Nome:** Jvczfhe.exe.bin.exe
   * **Percorso:** C:\Users\admin\AppData\Local\Temp\Jvczfhe.exe.bin.exe
   * **PID:** 6496
   * **Descrizione:** Questo è il processo eseguibile principale avviato dall'utente. Si spaccia per "Microsoft Edge" con una versione dichiarata di 126.0.2592.113, ma opera da una directory temporanea, il che è atipico per applicazioni legittime.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Processi secondari avviati:**
   * **cmd.exe**
     + **Comando:** "cmd" /c timeout 21 & exit
     + **Percorso:** C:\Windows\SysWOW64\cmd.exe
     + **PID:** 6680
     + **Descrizione:** Il processo principale avvia il prompt dei comandi per eseguire il comando timeout, indicando una possibile tecnica di evasione o sincronizzazione temporale.

A screenshot of a computer

AI-generated content may be incorrect.

* + **conhost.exe**
    - **Comando:** \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
    - **Percorso:** C:\Windows\System32\conhost.exe
    - **PID:** 6708
    - **Descrizione:** Associato a cmd.exe, gestisce le finestre della console per le applicazioni della riga di comando.
  + **timeout.exe**
    - **Comando:** timeout 21
    - **Percorso:** C:\Windows\SysWOW64\timeout.exe
    - **PID:** 6752
    - **Descrizione:** Utilizzato per introdurre un ritardo di 21 secondi nell'esecuzione, spesso impiegato per sincronizzare attività o ritardare l'esecuzione di ulteriori comandi.

**Esecuzione da percorso non standard:** Il processo principale viene eseguito da una directory temporanea (AppData\Local\Temp), il che è insolito per applicazioni legittime come Microsoft Edge.

**Uso di comandi della riga di comando:** L'avvio di cmd.exe e l'esecuzione di timeout.exe suggeriscono tentativi di evasione o sincronizzazione, comuni nei comportamenti malevoli.

**Falsificazione delle informazioni del file:** Il processo principale dichiara di essere "Microsoft Edge" con dettagli come versione e descrizione corrispondenti, ma l'esecuzione da una directory temporanea e il nome del file sono sospetti.

Questi comportamenti indicano che **Jvczfhe.exe** potrebbe essere un eseguibile malevolo progettato per mascherarsi come un'applicazione legittima, eseguendo comandi di sistema per potenziali attività dannose.