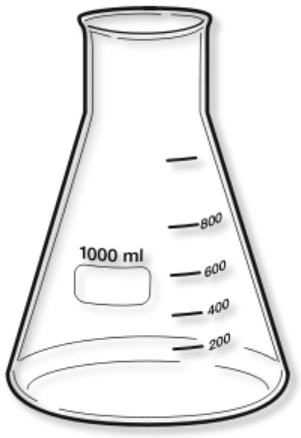
SecureSet Academy



{LAB} PowerShell

Created by ajay Menendez @paladin63

OBJECTIVE:

Today's lab objective is to be able to open powershell and run some commands to interact with the PowerShell interface.

TASKS:

1) **Get all the processes that are running on the local computer and save it to a file in a .CSV file.**
2) **Get all the log sources from Windows and export to .CSV file.**
3) **Get all the log sources from Windows and export to .CSV file.**
4) **Get a Hash from a text file, modify the text file and see the hash change.**

PLEASE NOTE!

ALL TYPED OUT COMMANDS to type are in RED, things will the need for special attention will be in Yellow Highlighter.

Save all files to your desktop so that it will be **easier** to find.

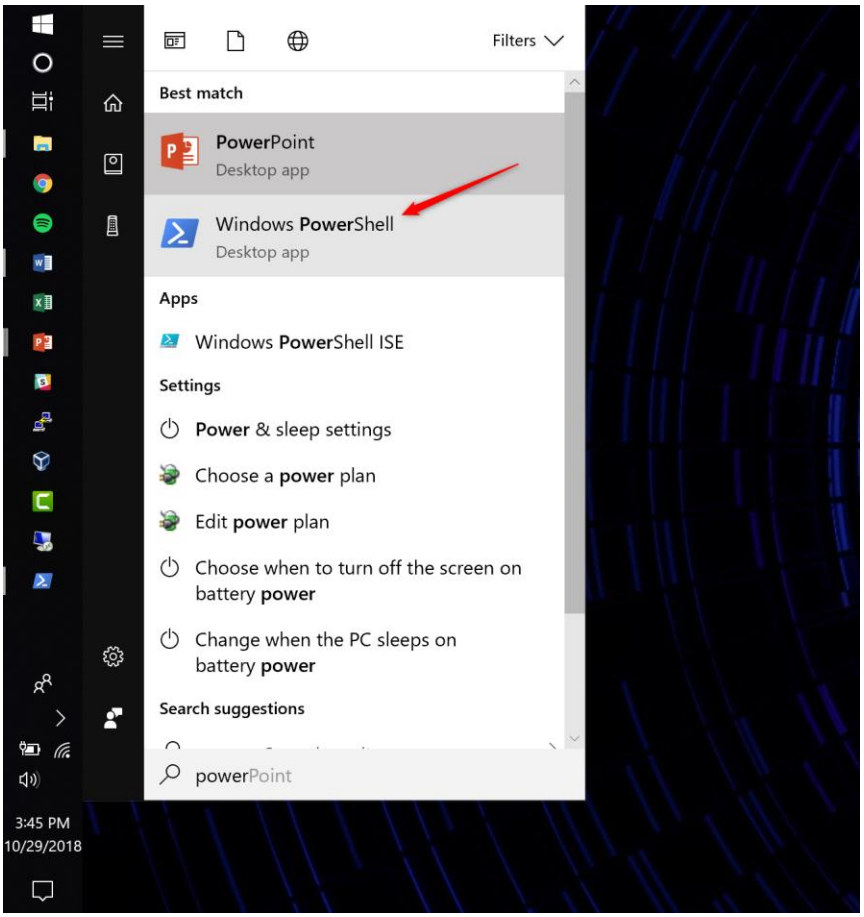
If you have never used the Windows Command Line, it would be best if you reviewed these helpful webpages before you start:

https://www.digitalcitizen.life/command-prompt-how-use-basic-commands

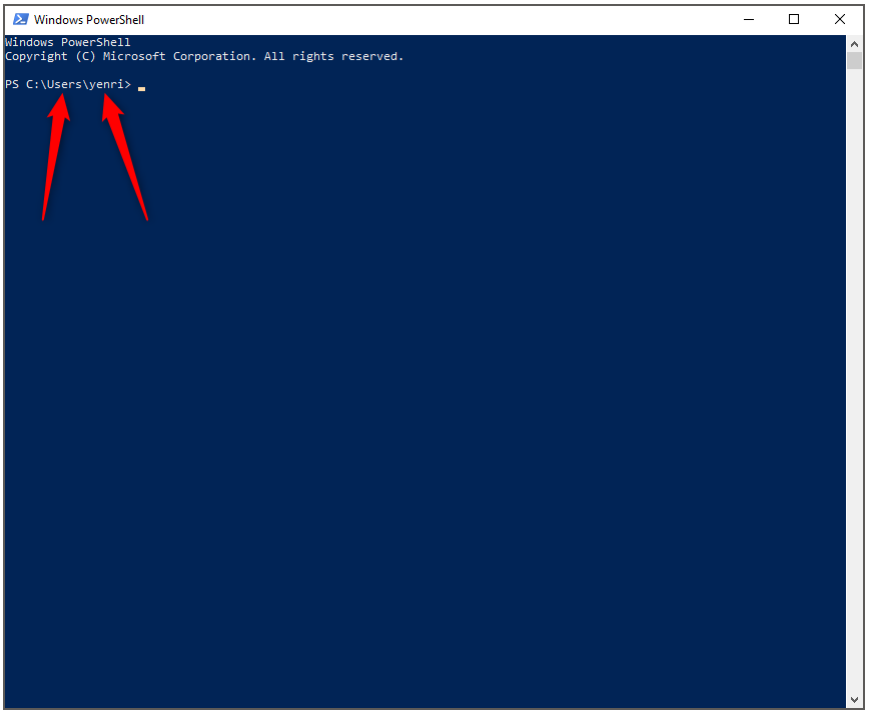
https://www.computerhope.com/issues/chusedos.htm

LAB START:

Open PowerShell by clicking start and typing in powers the automatic search function will find PowerShell, click on it and a blue window will start up.



Please notice the file path to the user folder. You'll need then when running your commands. If you started in C:\Windows\System32> you will want to cd .. several times to get to the root of the C drive, which looks like. C:\



1. Get all the processes that are running on the local computer and save it to a file as a .CSV file.

get-process | Out-File -LiteralPath C:\Users\<your_username>\Desktop\process.csv

EXAMPLE: get-process | Out-File -LiteralPath C:\Users\tom\Desktop\process.csv

2. Get all the log sources from Windows and export to .CSV file on the Desktop.

Get-EventLog -Log "Application" | Export-Csv C:\Users\<your_username>\Desktop\applog.csv

Get-EventLog -Log "system" | Export-Csv C:\Users\<your_username>\Desktop\syslog.csv

Get-EventLog -Log "security" | Export-Csv C:\Users\<your_username>\Desktop\seclog.csv

3. Get all services and export to file on Desktop.

Get-Service | Export-CSV c:\Users\<your_username>\Desktop\service.csv

4. Create a text file by opening the notepad.exe application

In PowerShell change directory to your Documents folder.

```
PS C:\> cd users
PS C:\users> cd yenri
PS C:\users\yenri> cd .\Documents\
PS C:\users\yenri\Documents>
```

Create some text in the notepad application. Save it to your Documents Folder

Save the text file

type ld or dir to show the contents of the directory.

Hash the file by using the command get-fi then click on the TAB button to autocomplete the cmdlet.

This is what the full command should look like:

Get-FileHash -algorithm md5 <name_of_your_text_file.txt>

```
    Directory: C:\users\yenri\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/29/2018   3:47 PM             13 FILEforHASHING.txt


PS C:\users\yenri\Documents> Get-FileHash -Algorithm md5 .\FILEforHASHING.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             3A88306ED45E4901B5B4CD5EBB42B2C7                                       C:\users\yenri\Documents\FILE...


PS C:\users\yenri\Documents>
```

Reopen your text file (if you closed it) and modify the text file.

Re-run the previous command

Notice the hash (or fingerprint) has changed. (Even a single space or character will change the output file hash) This is why File Hashes are used in cybersecurity forensics.

```
PS C:\users\yenri\Documents> Get-FileHash -Algorithm md5 .\FILEforHASHING.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             3A88306ED45E4901B5B4CD5EBB42B2C7                                       C:\users\yenri\Documents\FILE...

PS C:\users\yenri\Documents> Get-FileHash -Algorithm md5 .\FILEforHASHING.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             BCCA074F22CFA03A0B1E2C2167449796                                       C:\users\yenri\Documents\FILE...

PS C:\users\yenri\Documents>
```

Changed

CSI Cyber! Actually, no, let's not bring that up. (sorry) =)

FIN!