<https://os.cybbh.io/public/os/latest/002_powershell/pwsh_fg.html#_1_basic_powershell_concepts>

get-process

cd C:\Users\andy.dwyer\Desktop

Get-ChildItem

#this is same as ls command

New-Item .\content.txt

#create file

Set-Content .\content.txt -value "This is the way"

#write to content

Get-Content .\content.txt

#read content

Get-Variable

Get-Verb

###

Start-Transcript | Out-Null

Start-Process Notepad.exe

stop-process -name notepad

#return the single property of name of every process

(get-process).name

#display the get-process properties of name, ID, path for every process

get-process | select-object name, ID, path

#get cmdlets and display them in order

get-command -type cmdlet | sort-object -property noun | format-table

#check out how to format’

get-help format-table

get-help format-list

#get commands in a module

get-command -module Microsoft.Powershell.Security, Microsoft.Powershell.Utility -GroupBy Noun

###

#start transcript keep track of all your commands that have been run

start-transcript C:\MyWork.txt

get-service

stop-transcript

###

#1.2 Powershell help

Get-Help Get-Process

#view history

history

#or

Get-History

#pwd alias

dir

Get-Location

Get-Alias

Get-Alias dir

Get-Alias ls

#HOMEWORK: find the reverse alias from cmdlet to powershell and reverse ?

#SOLUTION: get-alias -Definition <verb-noun>

###

get-process | Get-Member

Get-Alias -Definition get-member

Get-Process | Select-Object Name, ID, path | Where-Object {$\_.ID -lt '1000'}

(Get-Process | Select-Object Name, ID, path | Where-Object {$\_.ID -lt '1000'}).count

get-service | where-object {$\_.Status -eq "Stopped"}

get-service | where Status -eq "Stopped"

Get-Process | where-object -Property Handles -GE -value 1000

Get-Process | select -first 10

<#MULTI-

LINE

COMMENT

#>

#1.7 CIM Classes

get-cimclass \*

#Think of CIM class as place holder and CIM instance as an actual event.

#METHODS and PROPERTIES

#Methods- what u can do to it

#Properties- what you know about it

Get-CimInstance -namespace root\securitycenter2 -ClassName antispywareproduct

Get-CimInstance -Namespace win32\_LogicalDisk -Filter "DriveType=3"

#CIM and WMI

#CIM instances have unique methods and what they control

#WMI is organized in namespaces, which are like folders that correlate to specific products or technology.

Get-CimInstance -class Win32\_BIOS # Queries Win32\_Bios

Get-WmiObject -Class Win32\_BIOS # same output but deprecated command

#Variables

Get-Variable

$MyVariable = 1,2,3,"dig"

Clear-Variable -Name MyVariable

remove-variable -name MyVariable

#command into variable

$process =Get-Process

$process

$Today = (Get-Date).DateTime

$Today

**Start and End process:**

Start-Process chrome

(get-process chrome\*).kill()

How many properties are available for the get-process cmdlet?

(get-process | get-member | where MemberType -eq Property).count

What command would give you information about the system's processor?

Get-WmiObject -Class Win32\_Processor

What PowerShell command (without using a method) will stop the Chrome process?

stop-process -name chrome

Compare 2 Objects;

compare-object (get-content one.txt) (get-content two.txt)

Count the number of times, case-insensitive, gaab is listed in words.txt in the CTF folder on the CTF user's desktop.

$FileContent = get-content "words.txt"

$Matches = select-string -InputObject $FileContent -Pattern "gaab" -AllMatches

$Matches.Matches.count

Count the number of unique words in words.txt, found on the CTF user's desktop, in the CTF folder.

PS C:\Users\CTF\Desktop\CTF> (get-content words.txt | sort -unique).count

Use a PowerShell loop to unzip the Omega file 1,000 times and read what is inside.

Note: Make sure you back up the .zip file to a different directory before attempting this challenge.

**copy-item** -path "C:\Users\CTF\Documents\Omega1000.zip" -Destination "C:\Users\CTF\Desktop\CTF"

On the CTF user's desktop, count the number of words in words.txt that meet the following criteria:

* *a* appears at least twice consecutively
* and is followed immediately by any of the letters *a* through *g*

(type words.txt | select-string aa[a-g]).count

What registry subkey runs a single time, then deletes its value once the machine reboots? The flag is the full path, using PowerShell.

HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE