************** Windows PowerShell **************

What syntax do PowerShell cmdlets follow?

- verb-noun

What PS command will list all PowerShell cmdlets?

- Get-Command

What PowerShell command will list all verbs?

- Get-Verb

BASH commands output strings. PowerShell commands output what data type?

- Objects

All PowerShell objects are comprised of what two things?

Flag format: things,things

- properties, methods

What command will list all things that make up a PowerShell object?

- Get-Member

What PowerShell command will list PowerShell aliases?

- Get-Alias

What PowerShell command lists all of the contents of a directory?

- Get-ChildItem

What is the basic cmdlet that displays help about Windows Powershell cmdlets and concepts?

- Get-Help

PowerShell "help files" don't show the entire help file with a basic command. What switch option shows the entire help file?

- -full

What PowerShell command will update the PowerShell "help files" to the latest version?

- Update-Help

What help switch will show you the "help files" on Microsoft's website, in your default browser?

- -online

What command will start the Chrome browser on your machine?

- Start-Process chrome.exe

What command using a PS Method will stop chrome?

Flag is the full command.

- (Get-Process chrome).kill()

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

- Stop-Process -name chrome

PowerShell doesn't have a native cmdlet that will give you processor information (such as get-processor or get-cpu). Knowing this information might be necessary. What command would give you information about the system's processor?

Flag is the full command

- Get-WmiObject Win32_Processor

What PowerShell command will read a text file?

- Get-Content

What PowerShell command will allow for counting lines in a file, averaging numbers, and summing numbers?

- Measure-Object

What PowerShell command searches for text patterns in a string?

- select-string

Users' files are stored in their corresponding home directory. What is the literal path to all home directories on a Windows 10 system?

- C:\users

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

Note: Property values only

- 52
- get-process | get-member -MemberType Property | measure-object

How many aliases does PowerShell have for listing the contents of a directory?

- get-help get-childitem
- 3

When requesting the help file for the get-process cmdlet, what full command is the 9th example given?

- update-help
- get-help get-process –Examples #To get the examples menu
- get-process powershell

To complete this challenge, find the description of the Lego Land service.

- Get-WmiObject -Class Win32_Service -Filter "name='legoland'" | ft description
- i_love_legos (answer)

In the CTF folder on the CTF User's Desktop, count the number of words in words2.txt.

- cd C:\Users|CTF\Desktop\CTF
- get-content -path words2.txt | measure-object
- 5254 (answe)

Count the number of files in the Videos folder in the CTF user's home directory.

- cd C:\Users\CTF\videos
- ls | measure-object
- 925

Find the only line that makes the two files in the CTF user's Downloads folder different.

Hint The flag is the string (not line number).

- cd..
- cd Downloads
- ls
- Compare-Object (Get-Content new.txt) (Get-Content old.txt)
- Popeye (answer)

The password is the 21st line from the top, in ASCII alphabetically sorted, descending order of the words.txt file.

Note: File location is CTF user's Desktop in CTF folder.

- cd..
- cd Desktop
- cd CTF
- get-content words.txt | sort-object -Descending | select -first 21
- ZzZp (answer)

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

- get-content words.txt | sort -Unique | Measure-Object
- 456976 (answer)

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

- get-process | Get-Member -MemberType Method | Measure-Object
- 19

Count the number of folders in the Music folder in the CTF user's profile.

- cd..
- cd Music
- ls | Measure-Object
- 411

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

- Get-Content words.txt | Select-String -Pattern GAAb | Measure-Object
- 1

Count the number of words, case-insensitive, with either a or z in a word, in the words.txt file on the CTF user's desktop.

Hint: There are multiple "words" on each line.

- Get-Content words.txt | Select-String -Pattern z, a | Measure-Object
- 160352

Count the number of times az appears in the words.txt file on the CTF user's desktop.

- Get-Content words.txt | Select-String -Pattern az | Measure-Object
- 2754

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.

- Get-ChildItem $Path "*Omega*" -Recurse

#FIND THE PATH TO OMEGA FILE

- Compress-Archive -LiteralPath 'C:\Users\CTF\Documents\Omega1000.zip' -DestinationPath 'C:\Users\CTF\Desktop\Omega.zip' #COPY OMEGA ZIP TO A NEW LOCATION
- Expand-Archive -LiteralPath 'C:\Users\CTF\Desktop\Omega.zip' -DestinationPath 'C:\Users\CTF\Desktop\O1000'

#UNZIP THE FIRST ITERATION - you now have a zipped folder (Omega999.zip) inside of an unzipped folder

- for($i = 0; $i -lt 1001; $i++){@(Get-ChildItem 'C:\Users\CTF\Desktop\O1000'| Sort-Object {$_.length})[0]| Expand-Archive -DestinationPath 'C:\Users\CTF\Desktop\O1000' -Force}

#UNZIP THE FILE 1000 TIMES

- Expand-Archive -LiteralPath ‘C:\Users\CTF\Desktop\O1000\Omega1.zip’ -DestinationPath ‘‘C:\Users\CTF\Desktop\O1000’

#UNZIP THE FINAL FILE (Omega1.zip)

- Get-Content C:\Users\CTF\Desktop\O1000\Omega.txt

#READ THE LAST UNZIPPED FILE

- kung-fu

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

Example: aac...aaa...

- Get-Content words.txt | Select-String -Pattern aaa,aab,aac,aad,aae,aaf,aag| Measure-Object
- 357

*********** Windows Powershell Profiles **************

Which PowerShell profile has the lowest precedence?

- Current user, Current Host

Which PowerShell profile has the highest precedence?

- All Users, All Hosts

Which PowerShell variable stores the current user’s home directory?

- $Home

Which PowerShell variable stores the installation directory for PowerShell?

- $PSHOME

Which PowerShell variable stores the path to the "Current User, Current Host" profile?

- $PROFILE

What command would you run to view the help for PowerShell Profiles?

- Get-Help about_Profiles

What command would tell you if there was a profile loaded for All Users All Hosts?

Flag is the full command syntax

- Test-Path -Path $PROFILE.AllUsersAllHosts

Malware is running in a PowerShell profile on the File-Server. Based on PowerShell profile order of precedence (what is read first), find the correct flag.

The flag is the string after the #, without the preceding space.

- #ALL PROFILES
- $PROFILE | Get-Member -Type NoteProperty -verbose

#AllUsersAllHosts - returns '# I am definitely not the malware'

- Get-Content 'C:\Windows\System32\WindowsPowerShell\v1.0\profile.ps1'

#AllUsersCurrentHost - returns cyber crest and '# I am not the malware'

- Get-Content 'C:\Windows\System32\WindowsPowerShell\v1.0\Microsoft.PowerShell_profile.ps1'

#CurrentUserAllHosts Returns '# I am the Malware'

- Get-content 'C:\Users\andy.dwyer\Documents\WindowsPowerShell\profile.ps1'

#CurrentUserCurrentHost Returns # Am I the Malware?

- Get-Content 'C:\Users\andy.dwyer\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'

*************** Windows Registry ***************

What registry hive contains all machine settings?

- HKEY_LOCAL_MACHINE

What registry hive contains all user settings?

- HKEY_USERS

What registry hive contains only the currently logged-in user's settings?

- HKEY_CURRENT_USER

The HKEY_CURRENT_USER registry hive is a symbolic link to another registry subkey. What is the subkey that it is linked to?

Flag format: HIVE\SID........................

- Get-LocalUser | select Name, SID #to find SID of andy
- HKEY_USERS\S-1-5-21-3939661428-3032410992-3449649886-1002

What PowerShell command will list all the subkeys and contents in the current directory and/or will list all the subkeys and the contents of a directory you specify?

- Get-ChildItem

What PowerShell command will list only the contents of a registry key or subkey?

- Get-Item

What registry subkey runs every time the machine reboots? The flag is the full path, using PowerShell.

Flag format: FULL\PATH\ALL\CAPS

- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

What registry subkey runs every time a user logs on? The flag is the full path, using PowerShell.

Flag format: FULL\PATH\ALL\CAPS

- HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

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

Flag format: FULL\PATH\ALL\CAPS

- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE

What registry subkey runs a single time, then deletes its value when a user logs on? The flag is the full path, using PowerShell.

Flag format: FULL\PATH\ALL\CAPS

- HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE

What is the value inside of the registry subkey from your previous challenge named registry_basics_7?

- Get-ItemProperty -Path HKLM:\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- malware.exe

What is the value inside of the registry subkey that loads every time the "Student" user logs on?

- Get-LocalUser | select Name, SID #See all the SIDs and find the one for student
- get-Item -path Registry::HKEY_USERS\S-1-5-21-2881336348-3190591231-4063445930-1003\Software\Microsoft\Windows\CurrentVersion\Run
- C:\botnet.exe

What is the value inside of the registry subkey from registry_basics_9?

- get-Item -path HKLM:\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE
- C:\virus.exe

What is the value inside of the registry subkey that loads a single time when the "student" user logs on?

- get-Item -path Registry::HKEY_USERS\S-1-5-21-2881336348-3190591231-4063445930-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE
- C:\worm.exe

Figure out the manufacturer's name of the only USB drive that was plugged into this machine.

- Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR
- SanDisk

What suspicious user profile, found in the registry, has connected to this machine?

- Get-ChildItem 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\ProfileList'
- Hacker_McHackerson

What suspicious wireless network, found in the registry, has this system connected to?

- Get-ChildItem 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles'
- Terror_cafe_network

********Windows Alternate Data Stream **********

Every file on a Windows system has attributes. What does the d attribute mean?

- directory

Every file on a Windows system has attributes. What does the h attribute mean?

- hidden

What PowerShell command will list all files in the current directory, regardless of their attributes?

- Get-Childitem -Force

What PowerShell command will give you the sha512 hash of a file?

Flag format: PS-command -argument

- Get-FileHash -Algorithm SHA512

What PowerShell command will list permissions of a file?

- Get-Acl

What Windows file maps hostnames to IP addresses?

- Hosts

Which group has ReadandExecute (RX) permissions to the file listed in the previous challenge, File_System_Basics_6?

- Get-ChildItem $Path "hosts" -Recurse   #SEARCH FOR FILENAME hosts ensure to cd... all the way back to C:\
- cd C:\Windows\System32\drivers\etc #Change directory to location of hosts
- get-acl hosts |ft -Wrap #DISPLAY PERMISIONS
- BUILTIN\Users

Find the last five characters of the MD5 hash of the hosts file.

- get-FileHash -Algorithm MD5 hosts
- 7566D

Examine the readme file somewhere in the CTF user’s home directory.

- Get-ChildItem $Path "readme" -Recurse
- cd C:\Users\CTF\Favorites
- Get-Content readme
- 123456

There is a hidden directory in the CTF user's home directory. The directory contains a file. Read the file.

- cd C:\Users\CTF
- ls -Force
- cd secretsauce
- Get-Content saucey
- ketchup

Find a file in a directory on the desktop with spaces in it.

HINT: If you like to type the full names and paths of files, you better look for a shortcut.

- cd C:\Users\CTF\Desktop
- ls -Force
- dir '.\z
- cd '.\z
- get-content .\spaces.txt
- 987654321

Find the Alternate Data Stream in the CTF user's home, and read it.

- Get-ChildItem -recurse | ForEach { Get-Item $_.FullName -stream * } | Where stream -ne ':$DATA'
- Get-Content C:\Users\CTF\Documents\nothing_here -stream Hidden
- P455W0RD

"Fortune cookies" have been left around the system so that you won't find the hidden password...

- Get-ChildItem C:\ -Recurse -Force -Include *fortune*
- C:\Windows\PLA\not_anihc
- Fortune Cookie Crumb
- "find the hidden fortune cookie.s . ."
- The Fortune Cookie

"The fortune you seek is inside The Fortune Cookie on this system."

- Get-item 'The Fortune Cookie' -stream * #NOTE STREAM IS 'NONE' BUT LENGTH IS 26
- Get-Content 'The Fortune Cookie' -stream none
- Password: fortune_cookie

There are plenty of phish in the C:\, but sometimes they're hidden in plain site.

Find the phish.

- Get-ChildItem C:\ -Recurse -Force -Include *www*

- cd C:\Users\CTF\Documents\WWW
- ls -Force
- for($i=0; $i -lt 400; $i++){get-content $i} #OR
- get-content 200   #LENGTH OF 200(30) GREATER THAN 0
- Flag: phi5hy

************* Windows Boot Process ************

What is the first process to spawn on Windows systems after the kernel loads?

- SYSTEM
-

What is the Process ID (PID) of the first Windows process?

- 4

What is the second boot process to spawn, that then spawns csrss in both user space and kernel space?

- smss

What session ID do kernel space processes operate in?

- 0

What process creates access tokens?

- lsass.exe

What is the parent process to all svchosts?

- services.exe

What process is waiting with high priority for the Secure Attention Sequence (SAS)?

- winlogon.exe

What user space process spawns explorer, then dies?

- userinit.exe

What is the name of the bootloader we are using on all of the Windows machines in this environment?

- powershell use bcedit command
- in path .exe is the name of bootloader

Based on the boot loader from Init_9, which firmware are we using (BIOS or UEFI) in our environment?

- System Info

- look for BIOS Version/Date
- BIOS

  OR

bcdedit | findstr /i winload # displays: \windows\system32\winload.exe (winload.exe means BIOS, winload.efi means UEFI)

What file saves the memory state to the hard drive when going into hibernation?

- hiberfi.sys

What bootloader is responsible for restoring the system to its original state after hibernation?

- winresume.exe

The system is booting into safe mode. Identify the flag from the command-line output.

Follow these instructions to boot the virtual image -- Click Here ---> Windows Bootkit Instructions

- after rebooting---- cmd ---bcdedit-----in description (flag is there)

- 1RF5Zgf9P
- #Launch the virtual machine on MobaXTerm
- Bcdedit
- Flag: 1RF5Zgf9P (will see in terminal)
-

The system is booting into safe mode. Correct that, and reboot into the desktop. The flag is on the desktop.

Follow these Windows Bootkit Instructions to boot the virtual image

- bcdedit /deletevalue {current} safeboot
- shutdown /r
- #once the virtual machine shuts down, it doesn't usually reboot on it's own - you will have to kill your connection and reboot it using ****qemu-system-x86_64 -m 2G Win_Bootkit.vdi
- #this will take you to your desktop, and the flag is the wallpaper
- Flag: 76Drp6hB
-

Prevent the system restart using the command line, and then identify persistence mechanisms that are reverting the OS and boot loader configurations. The flag is in the same folder as the persistence mechanism. HINT: Copy the error message in its entirety to figure out what is happening to the system. WARNING: You have 30 seconds to comply.

#You must ensure you stop playin when it comes to this problem - you only have 30 seconds

#Virtual machine will restart after last flag because of timeout, IF YOU WERE PLAYIN enter qemu-system-x86_64 -m 2G Win_Bootkit.vdi again

#Immediately open terminal and type “shutdown /a”

#This makes it so the terminal will not time out

#In terminal

```
sc query state= inactive | find “DISPLAY_NAME”
```

Flag: AlsKdJfhG

Run PowerShell... if you can. Resolve PowerShell dependencies. HINT: Search the entire file system for the PowerShell .dll and copy it back to where it needs to go. It is hidden in China. The flag is a file in the directory with the .dll

#Open File Explorer…

#Computer → Local Disk → Windows → System32 → cn-CN

#You will find the System.Management.Automation.dll (ctrl + c to cut)

#The correct path for this file is C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35

#Paste into correct folder

Flag: rfVBgtYHn

Once you fix and launch PowerShell, the console is changed to a custom layout. Figure out what file is causing this, read the file, and inspect the file that it is referencing.

#launch powershell as administrator - it will look weird because it is formatted differently

#Test-Path $profile.AllUsersAllHosts #returns True

#$cd C:\Windows\System32\WindowsPowershell\v1.0 #this takes you to all users, all hosts PSHOME file

#get-content profile.psi

#copy C:\Users\Yin\AppData\Local\Temp\7f7cfb189b822c87a02778a033f4275a.pdf

#paste into file explorer search bar

#PDF will open

#Scroll down to page 2

Flag: 8B7da4v6Y

************** Windows Process Validity************

1. **What Sysinternals tool shows malware persistence locations in tabs within its GUI?**
    a. Autoruns

2. **What Sysinternals tool is used to investigate processes**
    a. Procexp

3. **What Sysinternals tool can be used to investigate network connection attempts?**
    a. TCPView

4. **What Sysinternals tool can view permissions?**
    a. AccessChk

5. **What Sysinternals tool allows us to view and modify handles?**
    a. Handles

6. **What is the default Windows user directory for files downloaded from the internet? The flag is the folder name only.**
    a. Downloads

7. **What is the default Windows download directory that everyone has access to? The flag is the absolute path to the directory.**
    a. C:\Users\Public\Downloads

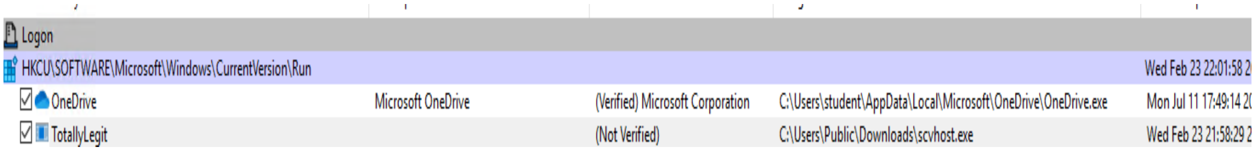
8. **What Sysinternals tool shows service load order?**
    - LoadOrd

9. **What is the service name of Windows Defender Firewall**
    a. Mpssvc

10. **What SysInternals tool reports .dlls loaded into processes?**
    a. ListDLLs

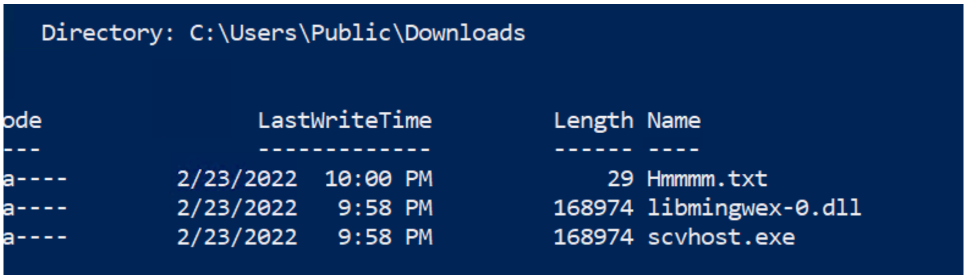
11. **There is malware on the system that is named similarly to a legitimate Windows executable. There is a .dll in the folder that the malware runs from. The flag is the name of the .dll.**

- **Open Autoruns to investigate suspicious files**



Logon				
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Wed Feb 23 22:01:58 2
☑ OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\student\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Mon Jul 11 17:49:14 2(
☑ TotallyLegit		(Not Verified)	C:\Users\Public\Downloads\scvhost.exe	Wed Feb 23 21:58:29 2

The file totally legit seems suspicious. Going to that folder path, and using the dll name is the answer:



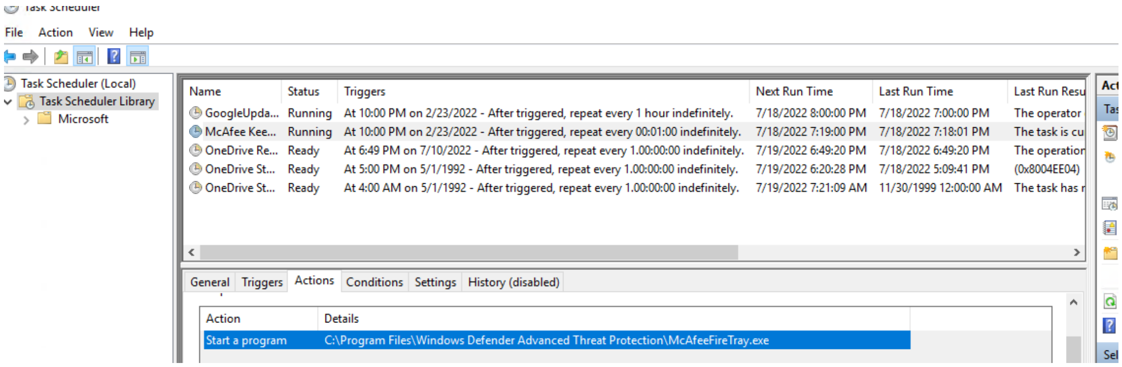
```
  Directory: C:\Users\Public\Downloads


ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
a----          2/23/2022  10:00 PM            29 Hmmmm.txt
a----          2/23/2022   9:58 PM        168974 libmingwex-0.dll
a----          2/23/2022   9:58 PM        168974 scvhost.exe
```

12. **You notice that there is an annoying pop up happening regularly. Investigate the process causing it. The flag is the name of the executable.**

- Go to Autoruns and go to scheduled task........ McAfee Keep-alive looks suscpicious
- right click and do Jump to Entry

-



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Resu
GoogleUpda...	Running	At 10:00 PM on 2/23/2022 - After triggered, repeat every 1 hour indefinitely.	7/18/2022 8:00:00 PM	7/18/2022 7:00:00 PM	The operator
McAfee Kee...	Running	At 10:00 PM on 2/23/2022 - After triggered, repeat every 00:01:00 indefinitely.	7/18/2022 7:19:00 PM	7/18/2022 7:18:01 PM	The task is cu
OneDrive Re...	Ready	At 6:49 PM on 7/10/2022 - After triggered, repeat every 1.00:00:00 indefinitely.	7/19/2022 6:49:20 PM	7/18/2022 6:49:20 PM	The operation
OneDrive St...	Ready	At 5:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	7/19/2022 6:20:28 PM	7/18/2022 5:09:41 PM	(0x8004EE04)
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	7/19/2022 7:21:09 AM	11/30/1999 12:00:00 AM	The task has r

Action	Details
Start a program	C:\Program Files\Windows Defender Advanced Threat Protection\McAfeeFireTray.exe

OR

#Open Task Scheduler, Notice task runs every 1 minute. (McAfee Keep Alive)

#Right click on McAfee Keep Alive, and view properties

#Go to “Actions” tab and double click on details

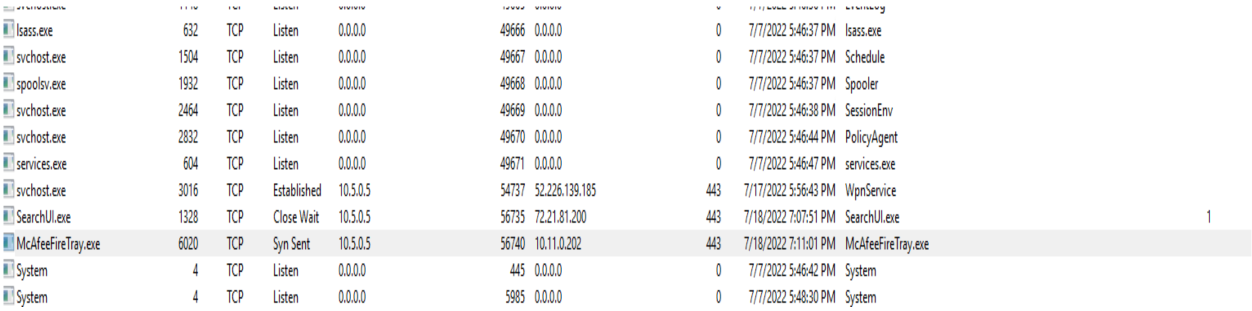
#Add arguments shows McAfeeFireTray.exe

McAfeeFireTray.exe

12. **Determine what is sending out a SYN_SENT message. The flag is the name of the executable.**

HINT: Use a Sysinternals tool.

Open TCPView. On the protocol column you can see Syn Sent



lsass.exe	632	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	7/7/2022 5:46:37 PM	lsass.exe	
svchost.exe	1504	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	7/7/2022 5:46:37 PM	Schedule	
spoolsv.exe	1932	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	7/7/2022 5:46:37 PM	Spooler	
svchost.exe	2464	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	7/7/2022 5:46:38 PM	SessionEnv	
svchost.exe	2832	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	7/7/2022 5:46:44 PM	PolicyAgent	
services.exe	604	TCP	Listen	0.0.0.0	49671	0.0.0.0	0	7/7/2022 5:46:47 PM	services.exe	
svchost.exe	3016	TCP	Established	10.5.0.5	54737	52.226.139.185	443	7/17/2022 5:56:43 PM	WpnService	
SearchUI.exe	1328	TCP	Close Wait	10.5.0.5	56735	72.21.81.200	443	7/18/2022 7:07:51 PM	SearchUI.exe	1
McAfeeFireTray.exe	6020	TCP	Syn Sent	10.5.0.5	56740	10.11.0.202	443	7/18/2022 7:11:01 PM	McAfeeFireTray.exe	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	7/7/2022 5:46:42 PM	System	
System	4	TCP	Listen	0.0.0.0	5985	0.0.0.0	0	7/7/2022 5:48:30 PM	System	

OR

Get-NetTCPConnection -State SynSent #powershell

Run TCP View

Sort by name or state

Find synsent -> answer is McAfeeFireTray.exe

13. **Malware uses names of legit processes to obfuscate itself. Give the flag located in Kerberos' registry subkey.**

    HINT: Use Sysinternals tools.

    Creds:

    Machine: Workstation1 (RDP from Admin-Station)

    login: student

    password: password

    - search for Kerberos in Autorun......... Right click and Jumpt to Entry------Click paramerts

    - flag: 76aGreX5

    OR

Open autoruns (sysinternals)

Search kerberos in search bar that says quick filter

Right click on Kerberos -> Jump to entry -> run as admin -> yes (do again if nothing happens)

Expand Kerberos folder on left-hand side -> click PARAMETERS

Flag: 76aGreX5

This is the path at the top: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kerberos\Parameters

14. **There is malware named TotallyLegit. Find its binary location and there will be a file in that directory. Read the file.**

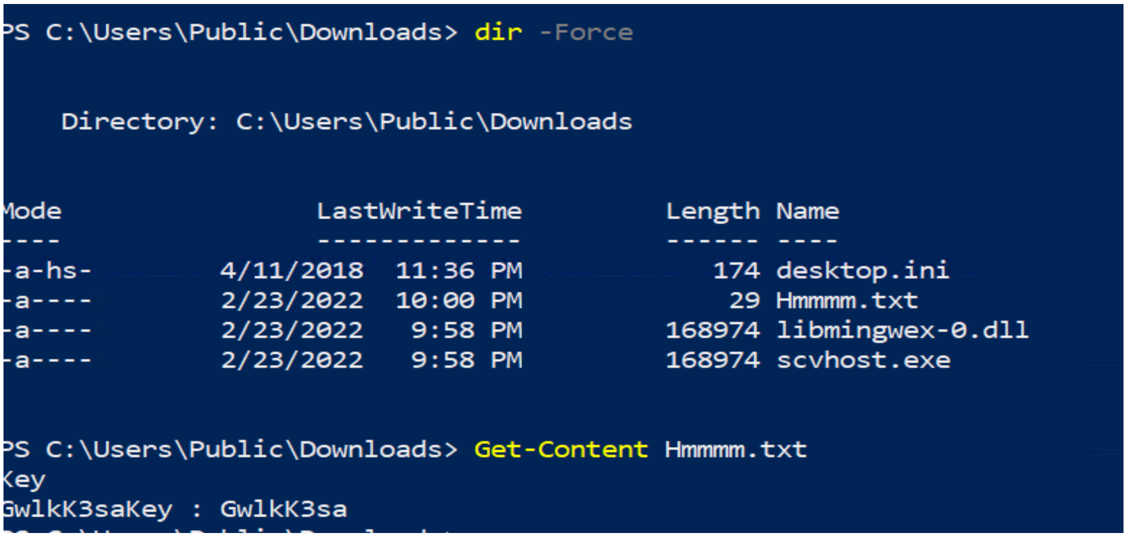
HINT: Use Sysinternals tools.

- go to AutoRuns--- search for TotallyLegit

- right click and Jump to Entry

- this gives the path----- read the Hmmm.txt file

GwlkK3sa



```
PS C:\Users\Public\Downloads> dir -Force


    Directory: C:\Users\Public\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-        4/11/2018  11:36 PM             174 desktop.ini
-a----        2/23/2022  10:00 PM              29 Hmmmm.txt
-a----        2/23/2022   9:58 PM          168974 libmingwex-0.dll
-a----        2/23/2022   9:58 PM          168974 scvhost.exe


PS C:\Users\Public\Downloads> Get-Content Hmmmm.txt
Key
GwlkK3saKey : GwlkK3sa
```

OR

strings * | findstr /i TotallyLegit

Cd HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\

ls -force | select-object name, property | where-object {$_.property -like 'tot*'}

Returns HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run {TotallyLegit, OneDrive}

get-Item HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

#Shows TotallyLegit : C:\Users\Public\Downloads\scvhost.exe

cd C:\Users\Public\Downloads\

Ls -Force

get-content Hmmmm.txt

Flag: GwlkK3sa

```
get-Item HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

cd  C:\Users\Public\Downloads\

Ls -Force

get-content Hmmmm.txt
```

Flag: GwlkK3sa

15. **Find the McAfeeFireTray.exe. There is a file in that directory. The flag is inside.HINT: Use Sysinternals tools.**

- autorun search for the file----right click jump --- this gives file path

- C:\Program Files\Windows Defender Advanced Threat Protection

- read file its' here : StrongBad

OR

strings * | findstr /i TotallyLeg

```
Get-ChildItem -Path C:\ -Include "McAfeeFireTray.exe" -File -Recurse #search for name of file

cd "C:\Program Files\Windows Defender Advanced Threat Protection"

ls

get-content '.\It''s_Here.txt'
```

Flag: StrongBad

16. What are the permissions for NT SERVICE\TrustedInstaller on spoolsv.exe? Copy the permissions from your shell.

```
Get-Process | ? { $.Path -like '*spoolsv.exe' } | % { $.Handle }
```

Handle -> different everytime

```
Get-ChildItem -Path C:\ -Include "spoolsv" -File -Recurse #search for name of file

        Directory: C:\Windows\System32\en-US

        Cd C:\Windows\System32\en-US

        (get-acl spoolsv.exe.mui).access | ft
```

Read,write

#OR

```
C:\Users\student\desktop\accesschk.exe C:\Windows\System32\spoolsv.exe
```

NT SERVICE\TrustedInstaller will show RW

#OR

Can also run:

```
icacls "C:\windows\System32\spoolsv.exe"
```

which shows (F) for Full Control

#https://www.varonis.com/blog/ntfs-permissions-vs-share Full Control = read, write and change, does not include execute

16. What is the PATH listed in the output when we find the handle for spoolsv.exe?

HINT: Use Sysinternals tools and don't forget to run as Administrator...

Open Process Explorer as administrator

Find spool in the top left search bar

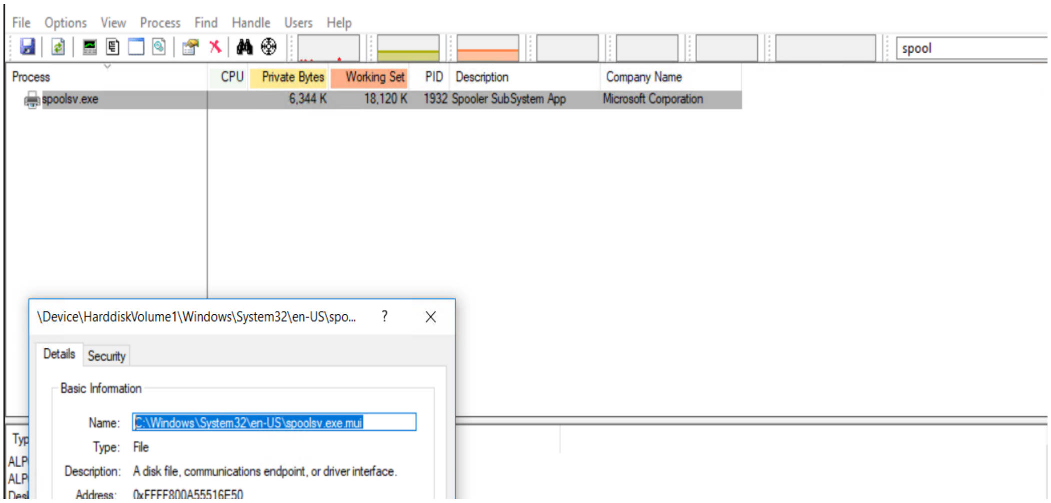
C:\Windows\System32\en-US\spoolsv.exe.mui

Go to options > lower Pane > DLL

Under lowerpane find spoolsv.exe.mui

Right click properties and see path

C:\Windows\System32\en-US\spoolsv.exe.mui



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
spoolsv.exe		6,344 K	18,120 K	1932	Spooler SubSystem App	Microsoft Corporation

\Device\HarddiskVolume1\Windows\System32\en-US\spo...

Basic Information

Name: C:\Windows\System32\en-US\spoolsv.exe.mui

Type: File

Description: A disk file, communications endpoint, or driver interface.

Address: 0xFFFF800A55516E50

OR

```
\C:\Users\student\Desktop\handle.exe | select-string ‘spools’
```

Result is C:\Windows\System32\en-US\spoolsv.exe.mui

17. In what Load Order Group is the Windows Firewall service?

HINT: Use Sysinternals tools.

#Open LoadOrd sysinternal

#I googled the driver for the Windows Firewall service, which is mps.drv

#also see under display name FirewallAPI.dll - mpssvc

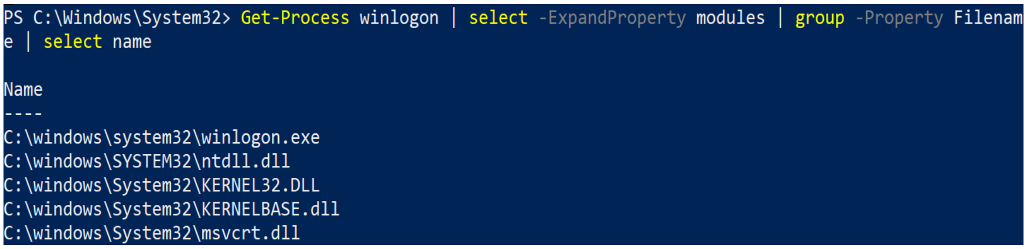
#I looked through load order and found the service in the service/device column

NetworkProvider

18. What is the first .dll associated with winlogon.exe? Provide the name of the .dll only, not the /absolute/path

HINT: Use Sysinternals tools.

PS C:\Windows\System32> Get-Process winlogon | select -ExpandProperty modules | group -Property Filename | select name   #This will list the dll in order



```
PS C:\Windows\System32> Get-Process winlogon | select -ExpandProperty modules | group -Property Filenam
e | select name

Name
----
C:\windows\system32\winlogon.exe
C:\windows\SYSTEM32\ntdll.dll
C:\windows\System32\KERNEL32.DLL
C:\windows\System32\KERNELBASE.dll
C:\windows\System32\msvcrt.dll
```

https://techexpert.tips/powershell/powershell-dll-loaded-running-process/

OR

cd Windows\System32

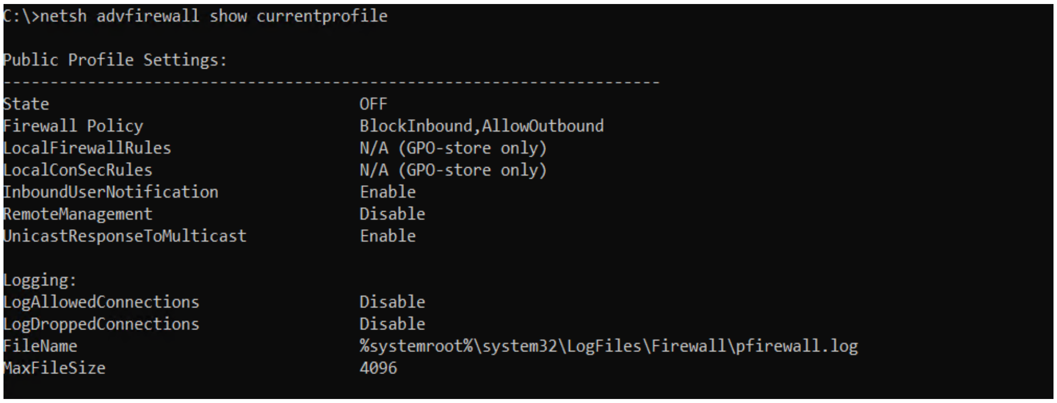
Get-Process winlogon | select -ExpandProperty modules | group -Property FileName | select name #see second from top

ntdll.dll

#*https://techexpert.tips/powershell/powershell-dll-loaded-running-process/*

19. While examining the Windows Defender Firewall, what is the LogAllowedConnections setting set to, for the Public profile?

https://support.moonpoint.com/os/windows/software/security/firewall/advfirewall.php netsh advfirewall show currentprofile



```
C:\>netsh advfirewall show currentprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

OR

#google LogAllowedConnections setting and go to website [*https://support.moonpoint.com/os/windows/software/security/firewall/advfirewall.php*](https://support.moonpoint.com/os/windows/software/security/firewall/advfirewall.php)

#Open cmd prompt

netsh advfirewall show currentprofile

#Notice logallowedconnections

Disable

20. ***A nonstandard port has been opened by possible malware on the system. Identify the port.***

#Open tcpview sysinternal

#Notice that powershell.exe is listening on port 6666

#Powershell would use TCP/5985 = HTTP or TCP/5986 = HTTPS, so you know this one could be malware

6666

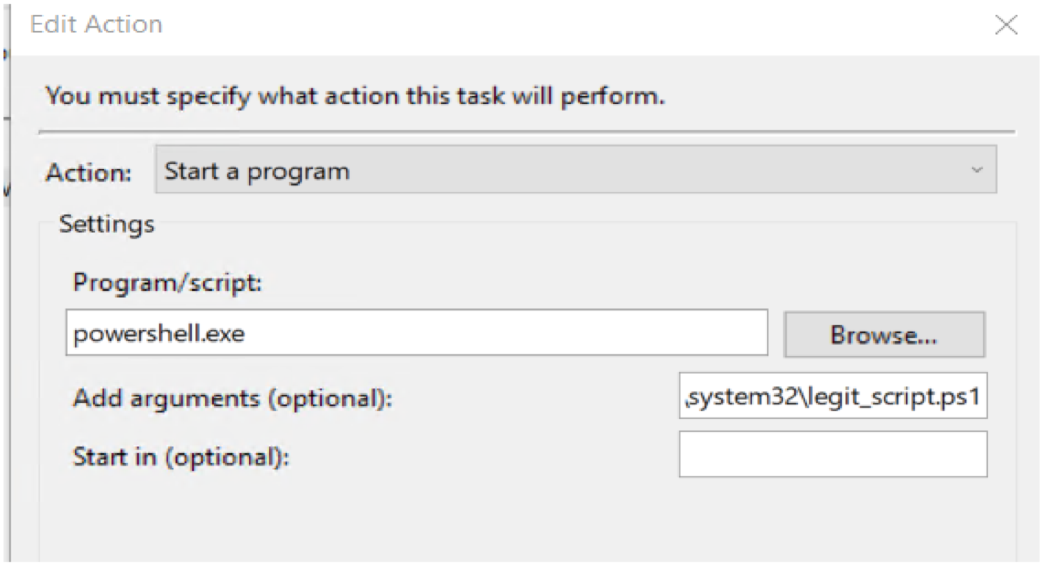
21. Determine what mechanism opened the port from hidden_processes_7. The flag is the name of the file.

- Run Task Scheduler as administrator

- On the right hand side “Display All Running Tasks”

- Notice GoogleUpdater current action is to run powershell ????
- Close and right click GoogleUpdater, Select properties
- Double click the actions, notice under arguments “-noexit -windowstyle hidden -File C:\windows\system32\legit_script.ps1”

legit_script.ps1



Edit Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: powershell.exe

Add arguments (optional): system32\legit_script.ps1

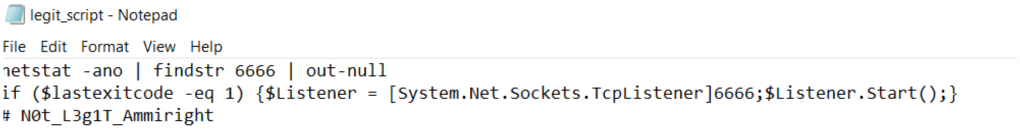
Start in (optional):

22. **Identify the flag from the file in hidden_processes_8.**

Open Files traverse to C:\windows\system32\legit_script.ps1

Open with notepad

N0t_L3g1T_Ammiright



legit_script - Notepad

```
netstat -ano | findstr 6666 | out-null
if ($lastexitcode -eq 1) {$Listener = [System.Net.Sockets.TcpListener]6666;$Listener.Start();}
# N0t_L3g1T_Ammiright
```

************ Windows UAC *************

1. What Sysinternals tool will allow you to view a file's manifest?

- sigcheck

2. What is the RequestedExecutionLevel for an application to run with the same permissions as the process that started it?

- asInvoker

3. What RequestedExecutionLevel will prompt the user for Administrator credentials if they're not a member of the Administrator's group?

- requireAdministrator

4. What registry key holds UAC values?

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

5. The flag is the RequestedExecutionLevel of the schtasks.exe file.

net use * http://live.sysinternals.com

z:

./sigcheck -m C:\Windows\System32\schtasks.exe

Scroll down to see description

asInvoker

6. Determine which UAC subkey property shows whether UAC is enabled or not. The flag is the data value in that property.

Hint: Make sure you're on the correct box.

Once on file server

Powershell

Cd HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies

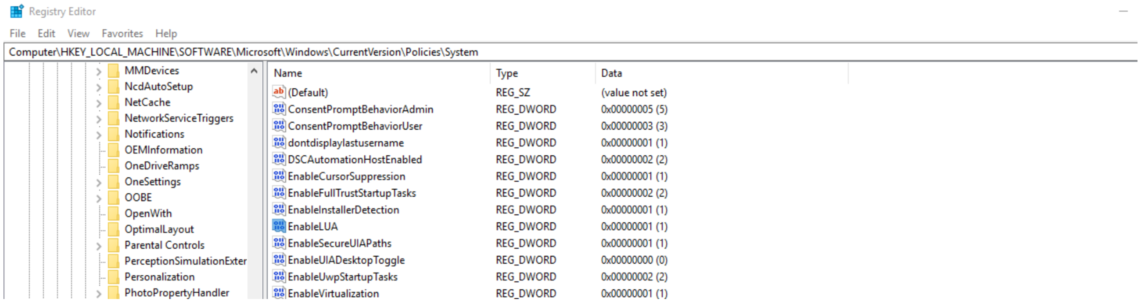
ls -force

SEE —-> EnableLUA : 4919

EnableLUA – Shows if UAC is enable or not

1

https://documentation.n-able.com/N-central/userguide/Content/Automation/Policies/Diagnostics/pol_UACEnabled_Check.htm



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

MMDevices
NcdAutoSetup
NetCache
NetworkServiceTriggers
Notifications
OEMInformation
OneDriveRamps
OneSettings
OOBE
OpenWith
OptimalLayout
Parental Controls
PerceptionSimulationExter
Personalization
PhotoPropertyHandler

Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000005 (5)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
dontdisplaylastusername	REG_DWORD	0x00000001 (1)
DSCAutomationHostEnabled	REG_DWORD	0x00000002 (2)
EnableCursorSuppression	REG_DWORD	0x00000001 (1)
EnableFullTrustStartupTasks	REG_DWORD	0x00000002 (2)
EnableInstallerDetection	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)
EnableUIADesktopToggle	REG_DWORD	0x00000000 (0)
EnableUwpStartupTasks	REG_DWORD	0x00000002 (2)
EnableVirtualization	REG_DWORD	0x00000001 (1)

7. Provide the name of the UAC [Registry subkey] property that determines what level UAC is set to (Example UAC levels: Default, Always, Notify).

ConsentPromptBehaviorAdmin

https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-group-policy-and-registry-key-settings#user-account-control-allow-uiaccess-applications-to-prompt-for-elevation-without-using-the-secure-desktop

- Once on file server

Powershell

1. Cd HKLM
2. Cd SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
3. Ls -force ###to see the files/output
4. SEE —->ConsentPromptBehaviorAdmin (answ)

   5 #this level of UAC is set to Default, Always, Notify

8. Query the registry subkey where UAC settings are stored and provide the flag.

Once on file server

Powershell

Cd HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies

- this is where UAC setting are stored

ls -force

Flag: NiceJob

********** Windows Services *************

1. What command-line (cmd) command will show service information?

- sc.exe

2. What command-line (cmd) command will show all services, running or not running?The flag is the full command, for all services.

sc queryex type=service state=all

3. What PowerShell command will list all services?

- get-service

4. What registry location holds all service data?

- HKLM\SYSTEM\CurrentControlSet\Services

5. What registry subkey holds a service's .dll location? The flag is the subkey name (full path not needed)

#which has a value of a list of service names to find the list of services to load, and then each service in that #list, use the key

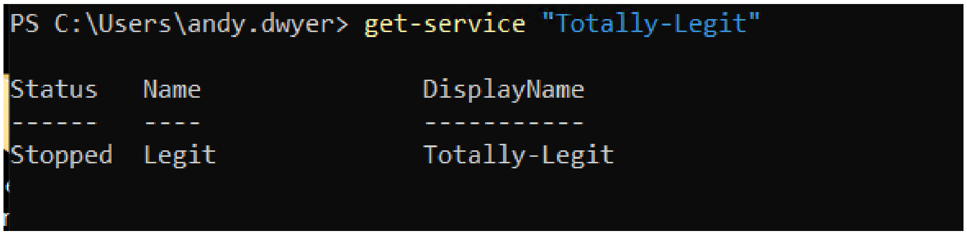
#HKLM:\SYSTEM\CurrentControlSet\Services\<NAME>\Parameters

Flag: Parameters

6. Services have a name and display name, which could be different. What is the service name of the only Totally-Legit service?

Get-service "Totally-Legit"

Name is Legit



```
PS C:\Users\andy.dwyer> get-service "Totally-Legit"

Status   Name               DisplayName
------   ----               -----------
Stopped  Legit              Totally-Legit
```

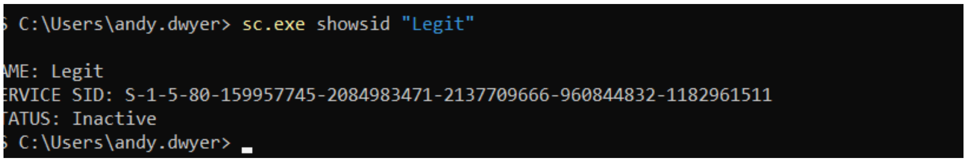
7. Figure out the SID of the only Totally-Legit service.

Example: S-1-5-80-159957745-2084983471-2137709666-960844832-[1182961511]

Submit only the [bracketed] portion of the SID.

HINT: Run the command on the service name, not the display name.

- sc.exe showsid "Legit"



```
$ C:\Users\andy.dwyer> sc.exe showsid "Legit"

AME: Legit
ERVICE SID: S-1-5-80-159957745-2084983471-2137709666-960844832-1182961511
TATUS: Inactive
$ C:\Users\andy.dwyer> _
```

********** Windows Auditing and Logs ************

1. What Sysinternals tool will allow you to read the SQLite3 database containing the web history of chrome?
   a. Strings

2. What is the registry location of recent docs for the current user?

- HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

3. BAM settings are stored in different registry locations based on the version of Windows 10. What version of Windows 10 is workstation2 running? The answer is the 4 digit

   PS C:\Users> wmic os get BuildNumber

   BuildNumber

   17134

   OR

Get-ComputerInfo | select WindowsProductName, WindowsVersion, OsHardwareAbstractionLayer

1803

#can also check ReleaseID by command below

Get-Item 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\'

4. Figure out the last access time of the hosts file.

   Flag format: _mm/dd/yyyy

   PS C:\> Get-Childitem -Recurse $env:USERPROFILE\AppData\Roaming\Micros\Windows \Recent -ErrorAction SilentlyContinue | select FullName,LastAccessTime

   - 07/20/2022

5. What is the literal path of the prefetch directory?

```
Get-ChildItem $PATH "Prefetch" -recurse
```

C:\windows\prefetch

#OR

From material

\Root\Windows\Prefetch

C:\Windows\Prefetch

6. In the Recycle Bin, there is a file that contains the actual contents of the recycled file. What are the first two characters of this filename?

   To see the content of the recycled folder

   ```
   PS C:\> Get-Childitem 'C:\$RECYCLE.BIN' -Recurse -Verbose -Force | select FullName
   ```

   Here, $R – gives the content of the deleted file

   $I – gives the location of the file

   Ans: $R

7. What are the first 8 characters of the Globally Unique Identifier (GUID) used to list applications found in the UserAssist registry key (Windows 7 and later)?

   Ans: CEBFF5CD

8. What cipher method are UserAssist files encoded in?
   a. ROT13
9. What main Windows log would show invalid login attempts?
   a. Security
10. What main Windows log will show whether Windows updates were applied recently?
    a. System
11. When reading logs, you may notice ... at the end of the line where the message is truncated. What format-table switch/argument will display the entire output? Flag format: -argument

- -wrap

12. Find the questionable website that the user browsed to (using Chrome), that appears to be malicious.
    a. Use this command to look for recent broweser hsitory and juts URL’s:

```
$History| Select-String -Pattern "(https|http):\/\/[a-zA-Z_0-9]+\.\w+[\.]?\w+" -AllMatches|foreach {$_.Matches.Groups[0].Value}| ft
```

Anw: https://www.exploitdb.com

Or

```
Get-Content 'C:\users\student\AppData\Local\Google\Chrome\User Data\Default\History'
```

https://www.exploit-db.com/

13. **There is a file that was recently opened that may contain PII.Get the flag from the contents of the file.Hint: We're not interested in numbers.**

To see all the files that are recently opened

```
Get-Item 'Registry::\HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.*'
```

We see the txt file was opened now to see where is the location of this file

```
Get-Item "REGISTRY::HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt" | select -Expand property | ForEach-Object { [System.Text.Encoding]::Default.GetString((Get-ItemProperty -Path "REGISTRY::HKEY_USERS\*\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt" -Name $_).$_)}
```

This gives us the location: Directory: C:\Users\student\Documents

Now change directory and rread the .txt file: PS C:\Users\student\Documents> Get-Content "3-14-24.txt"

Answ: Flag, Found A.

OR

```
Get-Item "REGISTRY::HKEY_USERS\\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt" | select -Expand property | ForEach-Object {[System.Text.Encoding]::Default.GetString((Get-ItemProperty -Path "REGISTRY::HKEY_USERS\\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt" -Name $).$)}

#returns the path of the file you need

cd C:\Users\student\Documents

ls

get-content 3-14-24.txt
```

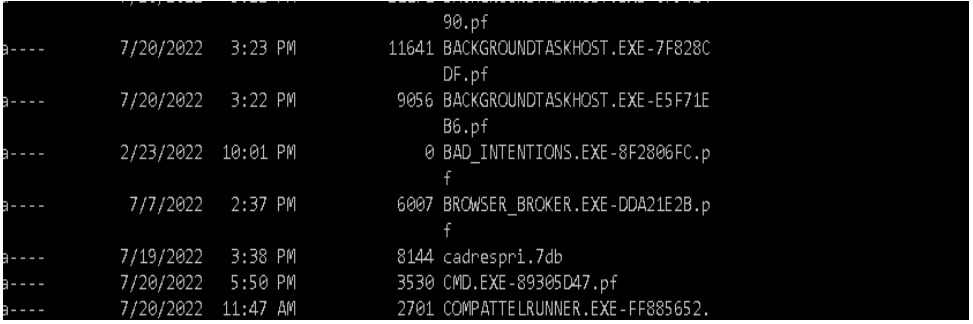
Flag: Flag, Found A.

14. Enter the full path of the program that was run on this computer from an abnormal location.

```
shutdown /r
```

```
Get-Item HKLM:\SYSTEM\CurrentControlSet\Services\bam\UserSettings\*gar6
```

C:\Windows\Temp\bad_intentions.exe

15. Enter the name of the questionable file in the prefetch folder.
    a. Use the command to look for the files on Prefetch
        i. PS C:\> Get-Childitem -Path 'C:\Windows\Prefetch' -ErrorAction Continue
    b. Going through the files, a file jumps out called Bad
    c. 

```
                                                  90.pf
a----         7/20/2022   3:23 PM          11641 BACKGROUNDTASKHOST.EXE-7F828C
                                                  DF.pf
a----         7/20/2022   3:22 PM           9056 BACKGROUNDTASKHOST.EXE-E5F71E
                                                  B6.pf
a----         2/23/2022  10:01 PM              0 BAD_INTENTIONS.EXE-8F2806FC.p
                                                  f
a----          7/7/2022   2:37 PM           6007 BROWSER_BROKER.EXE-DDA21E2B.p
                                                  f
a----         7/19/2022   3:38 PM           8144 cadrespri.7db
a----         7/20/2022   5:50 PM           3530 CMD.EXE-89305D47.pf
a----         7/20/2022  11:47 AM           2701 COMPATTELRUNNER.EXE-FF885652.
```

Bad_intentions.exe

OR

```
Get-Childitem -Path 'C:\Windows\Prefetch' -ErrorAction Continue
```

DARK_THOTS-8F2869FC.pf

BAD_INTENTIONS.EXE-8F2806FC.pf

16. What is the creation time of the questionable file in the prefetch folder?Flag format: mm/dd/yyyy

02/20/2022

or

```
Get-ChildItem -Recurse C:\Windows\Prefetch\DARK_THOTS-8F2869FC.pf -ErrorAction Continue | select FullName, LastAccessTime, FullName
```

02/23/2022

#OR

Just look to the left of the item after previous command

17. Recover the flag from the Recycle Bin. Enter the name of the recycle bin file that contained the contents of the flag, and the contents of the deleted file. Flag format: filename,contents

```
Get-Childitem 'C:\$RECYCLE.BIN' -Recurse -Verbose -Force | select FullName | format-table -wrap
```

```
Get-Content 'C:\$RECYCLE.BIN\S-1-5-21-2881336348-3190591231-4063445930-1003\$RZDAQ4U.txt'
```

$RZDAQ4U.txt,DontTrashMeyo

18. **Find the file in the jump list location that might allow privilege escalation.**

```
Get-Childitem -Recurse C:\Users\*\AppData\Roaming\Microsoft\Windows\Recent -ErrorAction Continue | select FullName, LastAccessTime
```

```
cd C:\Users\student\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
```

```
ls -force
```

```
Get-content .\5f7b5f1e01b81337.automaticDestinations-ms
```

UIDPWD.txt

19. **Check event logs for a flag string. Machine: file-server**
    a. **To check the event log and search for the flag**
        i. Get-Eventlog -LogName System | ft -wrap | findstr /i "flag"

    This gives us the flag :3v3nt_LOg

******* Windows Active Directory Enumeration **********

1. **What is the domain portion of the following SID:**

   S-1-5-21-1004336348-1177238915-682003330-1000

   - https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers

- 21-1004336348-1177238915-682003330

2. **What PowerShell command will list domain groups?**

   - Get-ADGroup

3. **What PowerShell command will list all users anD their default properties? The flag is the full command with arguments.**

   - Get-ADUser -Filter *

4. **What PowerShell command will allow you to search Active Directory accounts for expired accounts without having to create a filter?**

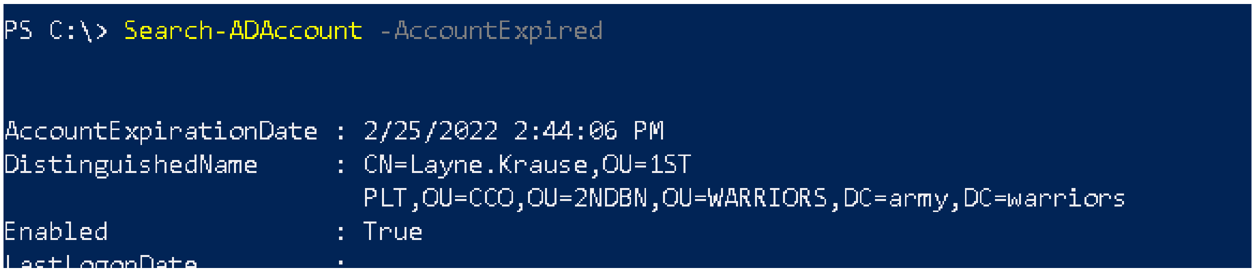
   The flag is only the command, no arguments/switches.

   - search-adaccount

5. **Find the expired accounts that aren't disabled. List the last names in Alphabetical Order, separated with a comma, and no space between. Flag format: name,name**

   - search-adaccount –AccountExpired

   - krause,page



```
PS C:\> Search-ADAccount -AccountExpired


AccountExpirationDate : 2/25/2022 2:44:06 PM
DistinguishedName     : CN=Layne.Krause,OU=1ST
                        PLT,OU=CCO,OU=2NDBN,OU=WARRIORS,DC=army,DC=warriors
Enabled               : True
LastLogonDate         :
```

https://docs.microsoft.com/en-us/powershell/module/activedirectory/search-adaccount?view=windowsserver2022-ps

6. **Find the unprofessional email addresses. List the email's domain.**

   To get all the users email adddrss:

   Get-ADUser -Filter * -Properties emailaddress |select emailaddress

   - All the emails are mail.mil beside one which is ashleymadison.com

7. **The flag is the unprofessionally named file located somewhere on the Warrior Share.**

Connect to the Warrior Share:

net use * "\\file-server\warrior share"

- to change the path to different drive: Set-Location -Path Z:/

- To get child items(folders/files) in current and all subdiretories of the Z drive

```
Get-ChildItem -path 'Z:\' -Recurse –Force
```

Here, path 'Z:\' can be replaced with other drives or if we want to search for only pdf we can do 'Z:\*.pdf'

After looking through all directory we see a file called

Lulz.pdf which seems unprofessional

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-childitem?view=powershell-7.2

8. **The flag is the name of the user who is requesting modified access rights.**

   Connect to the Warrior Share: net use * "\\file-server\warrior share"

   - After connecting to the fileserver, we look through the directoreis, we know S6 handles all the access request so we go to brigade folder throught file path: \\file-server\warrior share\Brigade HQ\S-6 in file explored
   - We find pdf 14287.pdf, after opening this we see –K as the initial. Need to find the full name. To find full name we know tis email was regarding printer issues so lets see all the groups in this directory:
   - Get-ADGroup -Filter * #Lists all the groups
   - Get-ADgroupMember –Identity 'Printer Group' -recursive #To see all the mmbers of this group
   - To get the names and phonenumbers:
   - Get-ADGroupMember -Identity 'Print Server Group' -recursive | select name, telephoneNumbers
   - We find only one name with intial K

9. **The flag is the name of the file where someone is requesting modified access rights**
   a. 14287.pdf

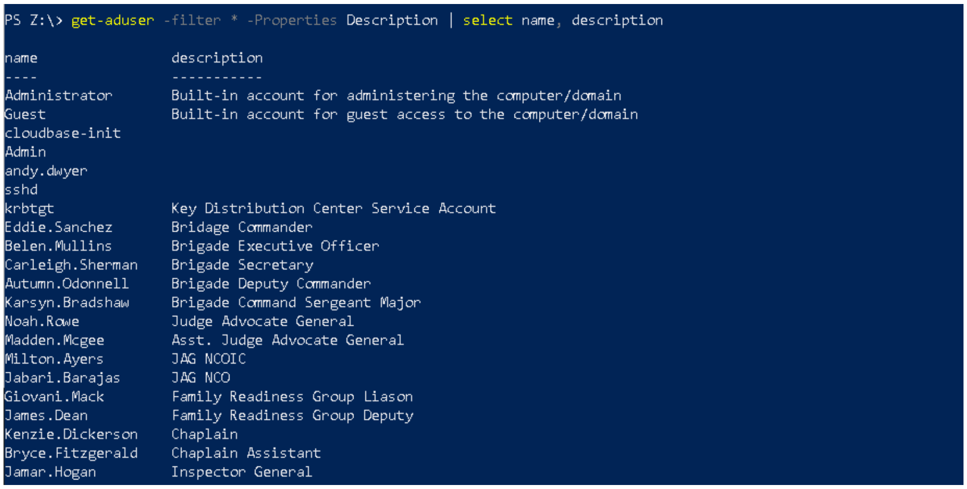
10. **Find the accounts that contain unprofessional information in the description.**

    List the last names in Alphabetical Order, separated by a comma, with no space

    Flag format: name,name

    - To get the names of all the users along with description get-aduser -filter * -Properties Description | select name, description

Brandywine,Jimenez



```
PS Z:\> get-aduser -filter * -Properties Description | select name, description

name                 description
----                 -----------
Administrator        Built-in account for administering the computer/domain
Guest                Built-in account for guest access to the computer/domain
cloudbase-init
Admin
andy.dwyer
sshd
krbtgt               Key Distribution Center Service Account
Eddie.Sanchez        Bridage Commander
Belen.Mullins        Brigade Executive Officer
Carleigh.Sherman     Brigade Secretary
Autumn.Odonnell      Brigade Deputy Commander
Karsyn.Bradshaw      Brigade Command Sergeant Major
Noah.Rowe            Judge Advocate General
Madden.Mcgee         Asst. Judge Advocate General
Milton.Ayers         JAG NCOIC
Jabari.Barajas       JAG NCO
Giovani.Mack         Family Readiness Group Liason
James.Dean           Family Readiness Group Deputy
Kenzie.Dickerson     Chaplain
Bryce.Fitzgerald     Chaplain Assistant
Jamar.Hogan          Inspector General
```

11. Find the following three accounts:

two accounts with passwords that never expire

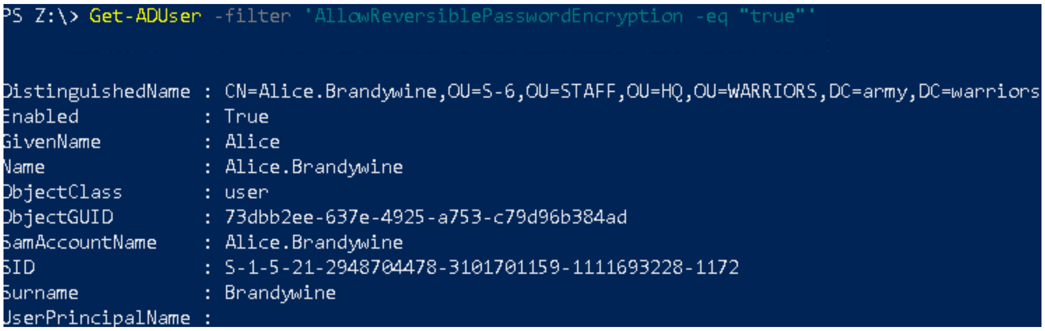
one account that has its password stored using reversible encryption

List the last names in Alphabetical Order, comma-separated, no spaces. Do not list built-in accounts.

First look for the properties which you can use to filter through. The command to look for all the properties is:

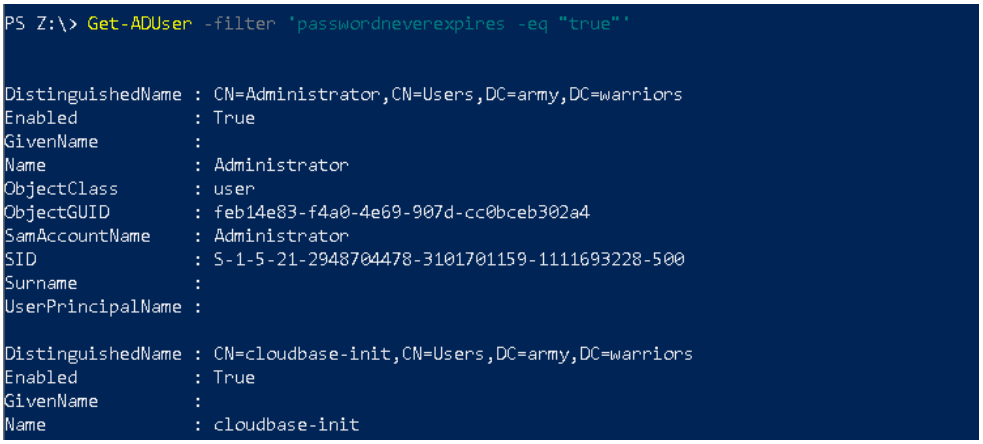
Get-ADUser -filter * -Properties *

- After looking at all the properties we can see that properties we need is AllowReversiblePasswordEncryption and passwordneverexpires
- Now using these properties to find the answer
- Get-ADUser -filter 'passwordneverexpires -eq "true"'
    - Here, we are using the filter and asking to give values if this property is set to true



```
PS Z:\> Get-ADUser -filter 'AllowReversiblePasswordEncryption -eq "true"'


DistinguishedName : CN=Alice.Brandywine,OU=S-6,OU=STAFF,OU=HQ,OU=WARRIORS,DC=army,DC=warriors
Enabled           : True
GivenName         : Alice
Name              : Alice.Brandywine
ObjectClass       : user
ObjectGUID        : 73dbb2ee-637e-4925-a753-c79d96b384ad
SamAccountName    : Alice.Brandywine
SID               : S-1-5-21-2948704478-3101701159-1111693228-1172
Surname           : Brandywine
UserPrincipalName :
```



```
PS Z:\> Get-ADUser -filter 'passwordneverexpires -eq "true"'


DistinguishedName : CN=Administrator,CN=Users,DC=army,DC=warriors
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : feb14e83-f4a0-4e69-907d-cc0bceb302a4
SamAccountName    : Administrator
SID               : S-1-5-21-2948704478-3101701159-1111693228-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=cloudbase-init,CN=Users,DC=army,DC=warriors
Enabled           : True
GivenName         :
Name              : cloudbase-init
```

We know not to use the built-in account, so answers are

brandywine,ibarra,sanchez

12. The flag is the name of the file containing PII on the Warrior Share.

to view all the files in directories and sub-directories:

Get-ChildItem -path 'Z:\' -Recurse –Force

Going through the files we can see phone_matrix.xlsx

13. Find the short name of the domain in which this server is a part of.

To find the name of the domain:

Get-WmiObject -Class win32_NTDomain

Ans: ARMY

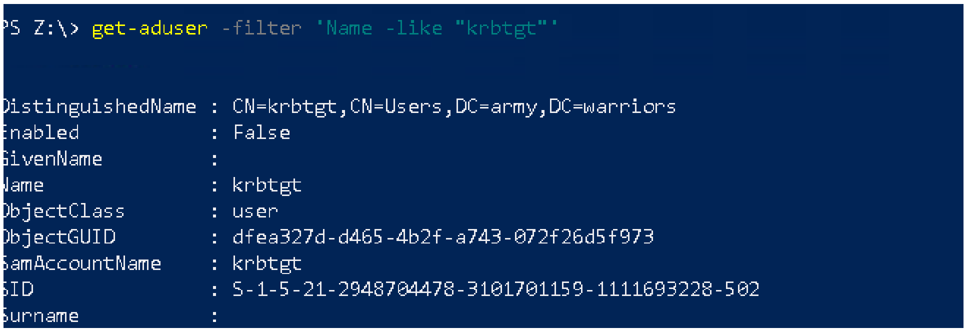
14. What is the RID of the krbtgt account.

Example: S-1-5-21-1004336348-1177238915-682003330-[501]

To filter the name “***krbtgt”*** *use the command:*

get-aduser -filter 'Name -like "krbtgt"'

answer: 502



```
PS Z:\> get-aduser -filter 'Name -like "krbtgt"'

DistinguishedName : CN=krbtgt,CN=Users,DC=army,DC=warriors
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : dfea327d-d465-4b2f-a743-072f26d5f973
SamAccountName    : krbtgt
SID               : S-1-5-21-2948704478-3101701159-1111693228-502
Surname           :
```

15. How many users are members of the Domain Admins group?

Get-ADGroupMember -Identity "domain admins"

asnw#1

16. How many total users are members of the Domain Admins group?

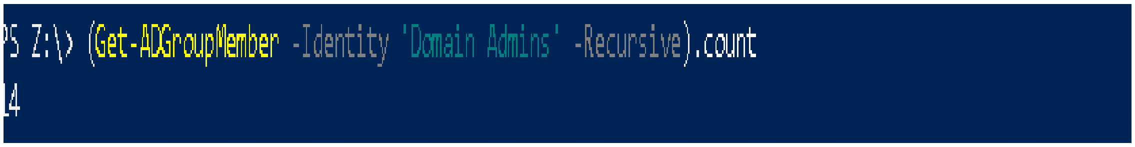
to get the number of people in Domain Admin group

Get-ADGroupMember -Identity 'Domain Admins' -Recursive

Now, to count

(Get-ADGroupMember -Identity 'Domain Admins' -Recursive).count

- 14



```
PS Z:\> (Get-ADGroupMember -Identity 'Domain Admins' -Recursive).count
14
```

17. Continue to follow the insider trail to find additional insider threats and their compromised mission. The flag is the full name of the next insider threat identified.

HINT: Search the Active Directory record of the user identified in search_insider_2.

the name of the insider threat is karen.nance. Now, to look for the properties of karen

Get-ADUser karen.nance -Properties *

Here, we see street address looks weird:

rkcrpg zl arkg pbzzhavpngvba ng 06:30 uef gbzbeebj zbeavat. Ybpngvba sbe qrgnvyf v aibyivat n uvtuyl pynffvsvrq bcrengvba hcybnqrq gb Gvssnal

Now, using ROT13 to decipher we get message: expect my next communication at 06:30 hrs tomorrow morning. Location for details involving a highly classified operation uploaded to Tiffany

Now, we know tiffany is another user. To get more details of Tiffany:

```
Get-ADUser -filter "name -like 'Tiffany*'"
```

```
Tiffany.Bellacino
```

18. Continue to follow the insider trail to find additional insider threats and their compromised mission.

The flag is the username resulting from assembling clues within a user's records.

HINT: Search the Active Directory record of the user identified in follow_insider_trail_1. Piece together clues to identify another insider threat.

To get more details on Tiffany:

```
Get-ADUser -filter "name -like 'Tiffany*'"-Properties *
```

To get more information containing wise on the word

```
Get-ADUser -Filter "name -like '*wis*'"
```

```
- Damian.Lewis
```

20. Continue to follow the insider trail to find additional insider threats and their compromised mission.

The flag is the full name of the insider threat identified.

HINT: Search the Active Directory record for the user identified in follow_insider_trail_2

Trying to get more information on Damian

```
-           Get-ADUser -filter "name -like '*Damian*'"-Properties *
```

Here on the Info Section, we can see a note from Isiah. So, let find more information of Isiah

```
Get-ADUser -Filter "name -like '*Isiah*'"
```

```
Isiah.Jesus
```

21. Continue to follow the insider trail to find additional insider threats and their compromised mission. This flag is a video link.

Hint: Search the Active Directory record for the user identified in follow_insider_trail_3.

```
Get-ADUser -filter "name -like '*Isiah*'"-Properties *
```

Here, street address has some funky numbers:
aHR0cHM6Ly93d3cueW91dHViZS5jb20vd2F0Y2g/dj1kUXc0dzlXZ1hjUQ==

Converting thhttps://www.youtube.com/watch?v=dQw4w9WgXcQ

is from base64 it will give us: