<https://os.cybbh.io/public/os/latest/008_windows_process_validity/winproc_fg.html#_1_what_is_process_validity_and_why_it_matters>

### How to view Processes and DLLs

* PowerShell: Get-Process - [Microsoft Reference](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-process?view=powershell-7.1)
* CMD: tasklist
* View all Processes, sort them by PID.
  + Get-Process | Sort -Property Id | more
* View all processes, but sort by PID and only show the properties I define.
  + Get-Process | Select Name, Id, Description | Sort -Property Id | more
* View only the processes I define and sort by PID
  + Get-Process SMSS,CSRSS,LSASS | Sort -Property Id
* View modules/DLLs used by defined processes and their file locations.
  + Get-Process chrome | foreach {$a} {$\_.modules} | more
  + Get-Process -Name "\*chrome\*" | Select-Object -ExpandProperty Modules | more

Pipe in a ft -wrap to see full file name/path

PS C:\Users\student> Get-Process chrome | foreach {$a} {$\_.modules} | more

PS C:\Users\student> Get-Process chrome | foreach {$a} {$\_.modules} | Where-Object ModuleName -like '\\*chrome\*' | more

* View an instance of all Win32 (system) services.
  + Get-Ciminstance Win32\_service | Select Name, Processid, Pathname | more
    - Pipe in ft -wrap to see full file name/path

#### 2.2.2 View Processes in Command Prompt

* tasklist /v

/svc

/m | more

/m /fi "IMAGENAME eq chrome.exe"

/fo:{table|list|csv}`

strings

/fi "IMAGENAME eq lsass.exe"

### How to View Services

Powershell Get-Ciminstance

Get-Service

CMD

net start

sc query

* View a defined service, showing all properties in list format.
  + get-service ALG | format-list

## Scheduled Tasks

* View all properties of the first scheduled task.
  + Get-ScheduledTask | Select \* | select -First 1

Task To Run: powershell.exe -win hidden -encode JABMAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAG8AYwBrAGUAdABzAC4AVABjAHAATABpAHMAdABlAG4AZQByACgANgA2ADYANgApADsAJABMAC4AUwB0AGEAcgB0ACgAKQA7AFMAdABhAHIAdAAtAFMAbABlAGUAcAAgAC0AcwAgADYAMAA=

This is BASE 64

#### Confirm IchBinBosh exists and View Properties

* In Command Prompt
  + schtasks /query | select-string -pattern IchBinBosh -Context 2,4
* In PowerShell
  + Get-ScheduledTask | Select \* | select-string -pattern IchBinBosh -Context 2,4

## 4. Network Connections

* netstat /?
* netstat -anob | more

## 5. Identifying Abnormalities/Suspicious Activity

* Ex. scvhost instead of svchost

Windows\_Processes\_Basics\_1

5

What Sysinternals tool shows malware persistence locations in tabs within its GUI?

**Autoruns**

Windows\_Processes\_Basics\_2

5

What Sysinternals tool is used to investigate processes?

**process explorer**

Windows\_Processes\_Basics\_3

5

What Sysinternals tool can be used to investigate network connection attempts?

**TCPView**

Windows\_Processes\_Basics\_4

5

What Sysinternals tool can view permissions?

**AccessChk**

Windows\_Processes\_Basics\_5

5

What Sysinternals tool allows us to view and modify handles?

**Handle**

Windows\_Processes\_Basics\_6

5

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

**Downloads**

Windows\_Processes\_Basics\_7

5

What is the default Windows download directory that everyone has access to? The flag is the absolute path to the directory.

**C:\users\public\downloads**

Windows\_Processes\_Basics\_8

5

What Sysinternals tool shows service load order?

**loadorder**

Windows\_Processes\_Basics\_9

5

What is the service name of Windows Defender Firewall?

**MpsSvc**

Windows\_Processes\_Basics\_10

5

What SysInternals tool reports .dlls loaded into processes?

**ListDLLs**

Windows UAC

## 1.4 View file manifest settings

*The Sysinternals Tool sigcheck will allow the viewing of these settings.*

PS C:\Users\student> net use \* http://live.sysinternals.com

PS C:\Users\student> z:

View the autoelevate setting of slui

PS Z:\> ./sigcheck -m C:\Windows\System32\slui.exe

View the highest available setting of regedit

PS Z:\> ./sigcheck -m C:\windows\regedit.exe

How to locate Windows executables that have autoelevate in the manifest

PS Z:\> ./strings –s c:\windows\system32\\*.exe | findstr /i autoelevate

autoelevate to highest privilege

Demo using Procmon to find registry keys called by autoelevate applications

1. Open Procmon
2. Run fodhelper.exe
3. Stop Capture
4. Create Filter ProcessName is fodhelper.exe
5. Create Filter Operation is RegOpenKey Action Include
6. Look for Registry Keys HKCU\software\classes
7. Look for Registry Keys HKCU\ms-settings\shell\open\command

This is where your three options for requestedExecutionLevel start to come out:

**asInvoker**: The application will run with the same permissions as the process that started it. The application can be elevated to a higher permission level by selecting Run as Administrator.

**highestAvailable**: The application will run with the highest permission level that it can. If the user who starts the application is a member of the Administrators group, this option is the same as requireAdministrator. If the highest available permission level is higher than the level of the opening process, the system will prompt for credentials.

**requireAdministrator**: The application will run with administrator permissions. The user who starts the application must be a member of the Administrators group. If the opening process is not running with administrative permissions, the system will prompt for credentials.

**Registry key that hold UAC value**

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

SysInternals

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

New-PSDrive -Name "SysInt" -PSProvider FileSystem -Root "\\live.sysinternals.com\Tools"

$wc = new-object System.Net.WebClient

$wc.DownloadFile("https://download.sysinternals.com/files/SysinternalsSuite.zip",

"$pwd\SysinternalsSuite.zip")

Expand-Archive C:\SysinternalsSuite.zip

PROCMON

## Autoruns

## Procexp

## TCPView

## PsExec

## PsLoggedon

## LogonSessiosn

## PsList

## PsInfo

## Strings- strings -a C:\users\andy.dwyer\Desktop\<doc>.txt

## Handle- start-transcript

Windows\_UAC\_Basics\_4

10

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

Make sure you’re on homestation\*

step 1: net use \* <http://live.sysinternals.com>

step 2: scp -r Z:\sigcheck.exe 10.11.0.3:\users\andy.dwyer\Downloads

step 3: z:

step 4: ls

step 5 ./sigcheck -m C:\windows\system32\schtasks.exe

Windows\_Services\_Basics\_3

5

What PowerShell command will list all services?

**Get-Service**

Windows\_Services\_Basics\_4

5

What registry location holds all service data?

**HKLM\SYSTEM\CurrentControlSet\Services**

Windows\_Services\_Basics\_6

10

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

**get-service | where-object {$\_.DisplayName -eq “Totally-Legit”} | more**

Windows\_Volatility\_Data

5

In terms of Volatile Data, what locations are the MOST volatile?

Flag format: location,location

**registers,cache**

Windows\_Memory\_Analysis\_Basics\_3

10

What is the 12th plugin listed in the Volatility help menu?

**cmdscan**

Windows\_Memory\_Analysis\_Basics\_1

5

What switch/argument will list all plugins for Volatility?

**-h**

Windows\_Memory\_Analysis\_Basics\_2

5

What command do you run to find which memory profile to use with a memory image?

**imageinfo**

Windows\_Memory\_Analysis\_Plugin\_3

5

What Volatility plugin will show driver objects?

**driverscan**

Windows\_Memory\_Analysis\_Plugin\_2

5

What Volatility plugin will extract command history by scanning for \_COMMAND\_HISTORY?

**cmdscan**