Advanced Scripting   
The Windows Registry

Last Updated: 4/18/2024 10:23 AM Version 1  
Document Prepared for: CYBER360 Student

# Name Click here to enter name ID Click here to enter id

# Instructions

Answer all questions directly in this document. You will save and upload this completed document as your homework submission.

# Overview

The Windows Registry has grown into a vast database tree holding configuration settings for Windows and its applications, largely replacing traditional text-based **.ini** configuration files. In contrast, most configuration files for Linux and its applications continue to be plaintext files collected in directories such as **/etc** and **/usr/share**.

# Requirements

PowerShell Core for Windows

# Task 1—Hives and Keys

Type regedt32 and press Enter to launch the Windows Registry editor GUI utility. *Caution: be careful! It is possible to make careless registry changes that can accidentally render a Windows host unusable.*

## Steps

1. The Registry Editor looks a bit like the File Explorer app. Notice the five root keys:   
   A screenshot of a computer

   Description automatically generated
2. More Registry jargon: Registry root keys are also known as *hives*. Folders and subfolders are usually known as *keys* and *subkeys*. each key (node) in the tree can contain registry *values*. Each value has a *name*, *type*, and *data*.
   1. Navigate to **HKEY\_LOCAL\_MACHINE/SOFTWARE/Microsoft/PowerShellCore**, by double-clicking on each key (folder) in turn in this Registry path.
   2. In the right pane you should see two values, one of type **REG\_SZ** named **Default**.
      1. What is the name of the other key? Click or tap here to enter text.
      2. What is its type? Click or tap here to enter text.
      3. What is its data? Click or tap here to enter text.
   3. You should also see two subkeys (subfolders) under **PowerShellCore**.
      1. What is the subkey under **InstalledVersions**?
      2. What is the data of the **InstallLocation** value in that subkey? Click or tap here to enter text.
      3. What is the subkey under **ProgramsMenuShortcut**? Click or tap here to enter text.
      4. What is the data of the **Installed** value in that subkey? Click or tap here to enter text.
3. Close the Registry Editor app.

# Task 2—Navigate the Registry Using PSDrives and Registry Objects

The same cmdlets used to interact with a filesystem, such as **Set-Location**, **Get-ChildItem**, etc. may be used to operate the Windows Registry.

## Steps

1. At your PowerShellCore (Windows) prompt, enter:   
   **Get-PSDrive**   
   There are many PSDrives. Use the Where-Object cmdlet to filter the collection of drives down to just those provided by the Registry:   
   **Get-PSDrive | ? { $\_.Provider.Name -eq 'Registry' } | Format-List**
   1. What is the four-letter abbreviated name for HKEY\_CURRENT\_USER? Click or tap here to enter text.
   2. What is the four-letter abbreviated name for HKEY\_LOCAL\_MACHINE? Click or tap here to enter text.
2. Use PowerShell Core to navigate to the PowerShellCore subkey.
   1. Enter:   
      **Set-Location HKLM:/Software/Microsoft/PowerShellCore**   
      **Get-ChildItem**
   2. Do you see the same subfolders that you saw in the previous task? Click or tap here to enter text.
   3. Enter:   
      **Get-ChildItem InstalledVersions**
3. The other Registry hives may be navigated using a path starting with **Registry::** and delimiting each key node with a backslash **\** separator. Enter (all on one line):   
   **Get-ChildItem -Path Registry::HKEY\_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion | Format-List**
4. Use **Get-ItemProperty** to get the individual entries out of a registry key. Enter the following command (all on one line) to see the file category values associated with registered filename extensions:   
   **Get-ItemProperty -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap**
5. Enter the following command (all on one line) to see the programs registered to automatically run at startup:   
   **Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Run**   
   (Substitute the registry hive **HKCU** to see programs registered to start upon login.)
6. (Optional): Launch another PowerShell Core (Windows) with administrator privilege and enter (all on one line):   
   **Set-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run -Name Notepad -Value "C:\Windows\System32\notepad.exe"**   
   After this, the Notepad accessory will also start up at each login. To remove it: (all on one line)   
   **Remove-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run -Name Notepad**

# Deliverable

Upload this document with completed answers to I-Learn Canvas.