Lab02.1-ProcessManagement1
SYS-320
Ben W
SP24

Deliverables:

1. PS script, list processes starting with “C”

```powershell
# Powershell Script
# SYS-320 - Ben W
# List every process starting with "C"

Get-Process "C*" | Select ProcessName
```

```
PS C:\Windows\system32> C:\Users\champuser\Documents\s

ProcessName
-----------
conhost
conhost
csrss
csrss
ctfmon
```

2. PS script, list processes whose path doesn’t include “system32”

```powershell
# Powershell Script
# SYS-320 - Ben W
# List processes not in system32

Get-Process | Where-Object { $_.Path -notlike "*system32*" } | Select-Object ProcessName, Path
```

```
PS C:\Windows\system32> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab02-1\ps_lab02-1_2.ps1

ProcessName                                            Path
-----------                                            ----
ApplicationFrameHost
bash
conhost
conhost
csrss
csrss
ctfmon
dllhost
dllhost
dwm
explorer
fontdrvhost
fontdrvhost
git-bash
GoogleCrashHandler                                     C:\Program Files (x86)\Google\Update\1.3.36.352\GoogleCrashHandler.exe
GoogleCrashHandler64
Idle
lsass
Memory Compression
mintty
msdtc
MsMpEng
NisSrv
powershell
powershell_ise                                         C:\Windows\syswow64\WindowsPowerShell\v1.0\PowerShell_ISE.exe
Registry
RuntimeBroker
RuntimeBroker
RuntimeBroker
SearchUI
SecurityHealthService
SecurityHealthSystray
services
SgrmBroker
ShellExperienceHost
sihost
```

Works, but a weird bug not showing paths for many objects, therefore not allowing them to be sorted out.

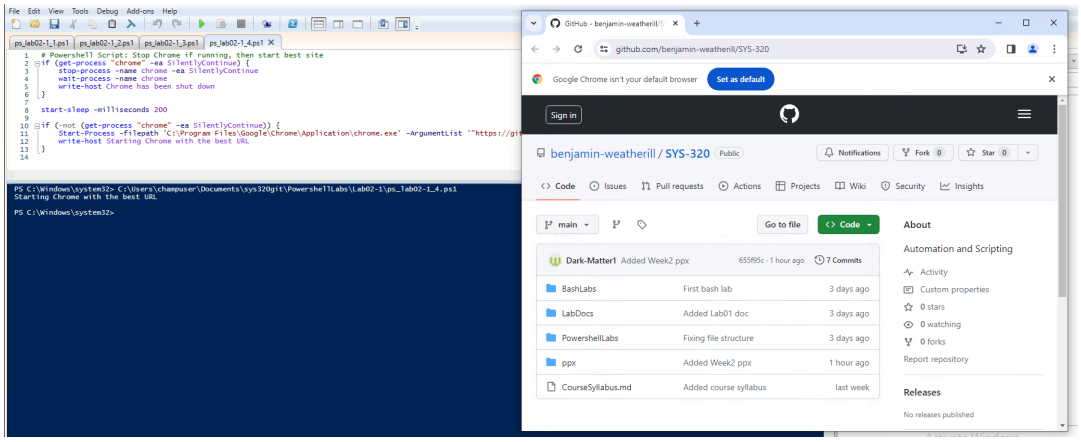
3. PS script, list every stopped service, alphabetical + save to csv

```powershell
# Powershell Script
# SYS-320 - Ben W
# List stopped services alphebetically and save to csv

Get-Service | Where-Object { $_.Status -ilike "Stopped" } | Select-Object Name, DisplayName | ConvertTo-Csv
```

```
PS C:\Windows\system32> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab02-1\ps_lab02-1_3.ps1
#TYPE Selected.System.ServiceProcess.ServiceController
"Name","DisplayName"
"AJRouter","AllJoyn Router Service"
"ALG","Application Layer Gateway Service"
"AppIDSvc","Application Identity"
"AppMgmt","Application Management"
"AppReadiness","App Readiness"
"AppVClient","Microsoft App-V Client"
"AppXSvc","AppX Deployment Service (AppXSVC)"
"AssignedAccessManagerSvc","AssignedAccessManager Service"
"AxInstSV","ActiveX Installer (AxInstSV)"
"BcastDVRUserService_ac2b8","GameDVR and Broadcast User Service_ac2b8"
"BDESVC","BitLocker Drive Encryption Service"
"BITS","Background Intelligent Transfer Service"
"BluetoothUserService_ac2b8","Bluetooth User Support Service_ac2b8"
"BTAGService","Bluetooth Audio Gateway Service"
"bthserv","Bluetooth Support Service"
"camsvc","Capability Access Manager Service"
"CaptureService_ac2b8","CaptureService_ac2b8"
"CertPropSvc","Certificate Propagation"
"ClipSVC","Client License Service (ClipSVC)"
"ConsentUxUserSvc_ac2b8","ConsentUX_ac2b8"
"CscService","Offline Files"
"defragsvc","Optimize drives"
"DeviceAssociationService","Device Association Service"
"DevicePickerUserSvc_ac2b8","DevicePicker_ac2b8"
"DevicesFlowUserSvc_ac2b8","DevicesFlow_ac2b8"
"DevQueryBroker","DevQuery Background Discovery Broker"
"diagnosticshub.standardcollector.service","Microsoft (R) Diagnostics Hub Standard Collector Service"
"diagsvc","Diagnostic Execution Service"
"DisplayEnhancementService","Display Enhancement Service"
"DmEnrollmentSvc","Device Management Enrollment Service"
"dmwappushservice","Device Management Wireless Application Protocol (WAP) Push message Routing Service"
```

4. PS script, starts chrome if not running, closes if running



```powershell
# Powershell Script: Stop Chrome if running, then start best site
if (get-process "chrome" -ea SilentlyContinue) {
    stop-process -name chrome -ea SilentlyContinue
    wait-process -name chrome
    write-host Chrome has been shut down
}

start-sleep -milliseconds 200

if (-not (get-process "chrome" -ea SilentlyContinue)) {
    Start-Process -filepath 'C:\Program Files\Google\Chrome\Application\chrome.exe' -ArgumentList '"https://github.com/benjamin-weatherill/SYS-320"'
    write-host Starting Chrome with the best URL
}
```

```
PS C:\Windows\system32> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab02-1\ps_lab02-1_4.ps1
Starting Chrome with the best URL

PS C:\Windows\system32> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab02-1\ps_lab02-1_4.ps1
Chrome has been shut down

PS C:\Windows\system32> |
```

5. Number 4 GitHub Link: https://github.com/benjamin-weatherill/SYS-320/blob/main/PowershellLabs/Lab02-1/ps_lab02-1_4.ps1