Week3-ClassActivity-FunctionsAndEventLogs
SYS-320
Ben W
SP24

Deliverables:

1. Login-Logoff records

```
PS C:\Users\champuser\Documents\scripts> Get-EventLog system -Source Microsoft-Windows-Winlogon

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    1219 Jan 26 18:08  Information Microsoft-Windows...       7001 User Logon Notification for Customer Experience Improvement Program
    1173 Jan 26 18:07  Information Microsoft-Windows...       7002 User Logoff Notification for Customer Experience Improvement Program
    1092 Jan 23 13:38  Information Microsoft-Windows...       7001 User Logon Notification for Customer Experience Improvement Program
     927 Jun 19 17:12  Information Microsoft-Windows...       7002 User Logoff Notification for Customer Experience Improvement Program
```

2. Empty Array, Loop, form new object

```powershell
# Powershell Script
# SYS-320 - Ben W

$winlogon = Get-EventLog system -Source Microsoft-Windows-Winlogon -After (Get-Date).AddDays(-14)

$winlogonTable = @()

for ($i=0; $i -lt $winlogon.count; $i++) {

    $event = "none"
    if ($winlogon[$i].InstanceId -eq "7001") { $event="Logon" }
    if ($winlogon[$i].InstanceId -eq "7002")  { $event="Logoff" }

    $user = $winlogon[$i].ReplacementStrings[1]

    $winlogonTable += [pscustomobject]@{"Time" = $winlogon[$i].TimeGenerated;
                                        "Id" = $winlogon[$i].InstanceId;
                                       "Event" = $event;
                                        "User" = $user;
                                        }
}

$winlogonTable
```

```
PS C:\Users\champuser\Documents\scripts> C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab03-Cla

Time                   Id Event  User
----                   -- -----  ----
1/26/2024 6:08:25 PM 7001 Logon  S-1-5-21-763900785-69722804-1183231302-1002
1/26/2024 6:07:31 PM 7002 Logoff S-1-5-21-763900785-69722804-1183231302-1002
1/23/2024 1:38:40 PM 7001 Logon  S-1-5-21-763900785-69722804-1183231302-1002
```

3. Translate Userid to User

```
Time                   Id Event  User
----                   -- -----  ----
1/26/2024 6:08:25 PM 7001 Logon  DESKTOP-KVBUJDD\champuser
1/26/2024 6:07:31 PM 7002 Logoff DESKTOP-KVBUJDD\champuser
1/23/2024 1:38:40 PM 7001 Logon  DESKTOP-KVBUJDD\champuser
```

4. Convert to function

```
function Get-LogonEvent($daysOld) {

    $winlogon = Get-EventLog system -Source Microsoft-Windows-Winlogon -After (Get-Date).AddDays(-$daysOld)

    $winlogonTable = @()

    for ($i=0; $i -lt $winlogon.count; $i++) {

        $event = "none"
        if ($winlogon[$i].InstanceId -eq "7001") { $event="Logon" }
        if ($winlogon[$i].InstanceId -eq "7002")  { $event="Logoff" }

        $userid = $winlogon[$i].ReplacementStrings[1]

        $userid = New-Object System.Security.Principal.SecurityIdentifier($userid)

        $user = $userid.Translate([System.Security.Principal.NTAccount])

        $winlogonTable += [pscustomobject]@{"Time" = $winlogon[$i].TimeGenerated;
                                            "Id" = $winlogon[$i].InstanceId;
                                          "Event" = $event;
                                           "User" = $user;
                                           }
    }

    $winlogonTable
}
```

5. Startup and Shutdown log functions

```
function Get-ShutdownEvent($daysOld) {
    $winlog = Get-EventLog system -InstanceId 2147489654 -After (Get-Date).AddDays(-$daysOld)

    $winlogTable = @()

    for ($i=0; $i -lt $winlog.count; $i++) {

        $event = "Shutdown"

        $user = "System"

        $winlogTable += [pscustomobject]@{"Time" = $winlog[$i].TimeGenerated;
                                          "Id" = $winlog[$i].EventID;
                                      "Event" = $event;
                                       "User" = $user;
                                      }
    }



    $winlogTable
}
function Get-StartupEvent($daysOld) {
    $winlog = Get-EventLog system -InstanceId 2147489653 -After (Get-Date).AddDays(-$daysOld)

    $winlogTable = @()

    for ($i=0; $i -lt $winlog.count; $i++) {

        $event = "Startup"

        $user = "System"

        $winlogTable += [pscustomobject]@{"Time" = $winlog[$i].TimeGenerated;
                                          "Id" = $winlog[$i].EventID;
                                      "Event" = $event;
                                       "User" = $user;
                                      }
    }



    $winlogTable

}
```

6. Dot Notation calling the functions

```
1   cd $PSScriptRoot
2
3   . .\ps_lab03-1-all.ps1
4
5   Get-LogonEvent 15
6
7   Get-ShutdownEvent 25
8
9   Get-StartupEvent 25
```

```
PS C:\Users\champuser\Documents\sys320git\PowershellLabs\Lab03

Time                   Id Event    User
----                   -- -----    ----
1/26/2024 6:08:25 PM 7001 Logon    DESKTOP-KVBUJDD\champuser
1/26/2024 6:07:31 PM 7002 Logoff   DESKTOP-KVBUJDD\champuser
1/23/2024 1:38:40 PM 7001 Logon    DESKTOP-KVBUJDD\champuser
1/26/2024 6:07:32 PM 6006 Shutdown System
1/23/2024 1:29:03 PM 6006 Shutdown System
1/26/2024 6:08:04 PM 6005 Startup  System
1/23/2024 1:29:34 PM 6005 Startup  System
1/23/2024 1:28:13 PM 6005 Startup  System
```

7. Github Link: https://github.com/benjamin-weatherill/SYS-320/tree/main/PowershellLabs/Lab03-Class Activity