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

PowerShell Transcripts

Exercise 4.5

# Instructions

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

# Overview

You can use transcripts to record a direct log of what happens in a PowerShell session.

# Requirements

PowerShell Core

# Task—Start-Transcript, Stop-Transcript

To find the Event Viewer app, tap the [Flag] key and start typing “Event Viewer.” (Open it when it appears under Best Match.) It will look something like this:

## Steps

1. Start recording a transcript:  
   **Start-Transcript**
2. “Mark” some output into the transcript:   
   **Write-Output "mark"**
3. Try to perform a “downgrade attack” on your computer:   
   **powershell.exe -version 2**
   1. Enter:   
      **$PSVersionTable**
   2. Did it work? Click or tap here to enter text. If you see version 2 in the PSVersionTable, then your downgrade attack succeeded; if so, type **exit** to leave PowerShell version 2 and return to PowerShell Core.
4. Stop recording your transcript:   
   **Stop-Transcript**   
   What is the complete path to the file where your transcript was stored? Click or tap here to enter text. (Note: by default, the path is your account’s Documents folder, and the name of the transcript file has the pattern:  
    PowerShell\_transcript.*<machine name>*.*<random string>*.*<DateTime code>*.txt.)
5. Have a look at your transcript:   
   **Get-Content** <complete path to your transcript file>
   1. The file has three sections, delimited by lines that look like this: **\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***.
   2. The top section is a detailed header with lots of attributes and their values. What is the value of the “Host Application” attribute? Click or tap here to enter text.
   3. The middle section is the actual transcript of your input prompts, input, and output. Does your “mark” command’s output appear in the transcript? Click or tap here to enter text.
   4. Is there any output recorded for your “downgrade attack” attempt? Click or tap here to enter text.
   5. The bottom section shows one more attribute, the DateTime code at which Stop-Transcript was executed. What is the value of your “End time” attribute? Click or tap here to enter text.

# Deliverable

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