Advanced Scripting

Steganography

*Last Updated: 12/2/2021 1:23 PM Version 1*

*Document Prepared for: CIT361 Student*

Name Click or tap here to enter text. ID Click or tap here to enter text.

Instructions

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

Overview

In this exercise, you will explore the applications of steganography using PowerShell.

Requirements

* Internet access.
* PowerShell.
* Invoke-PSImage Script.
* Decode\_PS\_Stego Application.

Setup

1. Please go to [https://github.com/Invoke-PSImage](https://github.com/peewpw/Invoke-PSImage) and download the zip file.
2. Unzip the file and store it in your files where it is easily found via file path.
3. Go to <https://github.com/PCsXcetra/Decode_PS_Stego> and download the zip file.
4. Unzip the file and uncompress the **PowershellStegoDecode** file using 7-Zip or File Viewer Plus in the Microsoft store.

Task 1 — Setup and Examine Script

1. For this exercise we must disable parts of Windows Defender and change the Execution Policy on your machine.
   1. Go to Windows Defender, click on the virus & threat protection section, click manage settings under virus & threat protection settings, and turn off Real-Time Protection.
   2. Open a PowerShell window as an Administrator
   3. Type **Set-ExecutionPolicy Bypass** and type **[A]** to agree to all.
2. Open VSCode and examine the Invoke-PSImage script. In a short description, describe what it does.  Click or tap here to enter text.
   1. This is a script created to either input a message or a script and embed that in a PNG file. It changes the RGB values a bit to embed a message or code within the picture that can be extracted later.

Task 2 — Import the Module and Embed Steganography

1. In PowerShell navigate to the file directory where **Invoke-PSImage-master** is located and enter the file.
   1. Type **Import-Module .\Invoke-PSImage.ps1** if done correctly there shouldn’t be any errors. If there are go back and make sure all the steps of Task 1 have been completed.
2. Find a .jpg file online that is relatively small. This will help with the encrypting time of the program. Place it in the same directory you are in.
3. In the GitHub repository of Invoke-PSImage what are the arguments used for encryption, and what are they for? Click or tap here to enter text.
4. In VSCode make a new file called **message.txt** and input your secret message, don’t forget to save it.
   1. In your terminal type **Invoke-PSImage -Script .\message.txt -Out .\secretpic.png -Image <.\(the name of the image you want to embed a message in)>**
   2. As you can see a big message comes out, don’t worry about this
5. Go to your Powershell Stego Decode program which was extracted earlier.
   1. Click select file, select your image named **secretpic.png** and click Get Data.
   2. Now you can see your secret message! What does your message say? (don’t include all the garbled text, just the message.)Click or tap here to enter text.

Deliverable

Upload this document with completed answers to I-Learn.