Python Scripting for CS – Lab 1

Keyloggers

# Purpose

In this lab, you will have the opportunity to practice modifying an existing script and setting up a keylogger on your machine.

## Skills

The purpose of this assignment is to help you practice the following skills that are essential to your success:

* Use verbs for the skills
* For example: Construct a command based on the syntax provided by a PowerShell help file

## Knowledge

This assignment will also help you become familiar with the following important content knowledge in this discipline:

* Could use competencies or learning objectives

# Instructions

Follow the instructions laid out in this lab, starting with Task 1. Tasks will build on each other and should not be done out of order.

There are critical thinking questions for you to answer on your own as well as definitions defined in **bold.** Critical thinking questions are identified in **green** with the corresponding employability skill.

Commands will be written in this Font and highlighted yellow. If the command is case sensitive, the letters that require capitalization will be underlined.

File names and programs will be written in this font and highlighted in gray. If the path or file name includes <a portion like this>, replace that piece with the required information, removing the <>.

Tasks that connect to previous course work will ask you to **Recall & Apply** from previous Learning Modules or classes.

# Criteria for Success

This assignment is worth 20 points. You will be graded on the script you modified as part of this lab.

# Lab Environment

In this class, you will be using VMs set up in Cloud.

# Log into Cloud

1. Access NWTC cloud at <https://lab.nwtc.edu>
2. Login using your username and password assigned in Lab 1
3. Start your Kali Linux VM

# Task 1: Download and Run keylogger.py

1. On your Kali VM, navigate to <https://github.com/RachelGehrke/PythonCS>
2. Go to LM01
3. Download keylogger.py and save it in your blackhat/vepython3 folder
4. Open keylogger.py in VS Code
5. Open a terminal window
6. **Recall & Apply Learning from Lab 0** & **Think Critically and Creatively:** Activate your virtual environment
   1. This *must* be done prior to installing any packages or running our script
7. Run the following command to install the pynput library:
   1. sudo pip install pynput
8. From your terminal and in your activated environment, run the following command:
   1. python keylogger.py
   2. HINT: Make sure your terminal window is pointing to your blackhat/vepython3 folder. You may have to modify the above command depending on the current working directory of your terminal
9. Once your script is running, open a text editor and try typing a few things.
10. Go back to your terminal and use ctrl + z to stop your python script.
11. Open keylog.txt and view the results.

# Task 2: Modifying keylogger.py

1. Save a copy of the keylogger.py as keyloggerv2.py
2. Open keyloggerv2.py in VS Code if you are not already in VS Code.
3. Our goal is to modify our keylogger so that when a user types an @ sign, it will log the current window title so we know where they were using an email address and hopefully that will lead us to knowing where they were trying to log in.
4. We are going to accomplish this by checking if the key they pressed is holding an @ sign. If it is, we are going to get the window title and logging it in keylog.txt
5. The first thing we need to do is import the os module into our script. The os module will allow us to use operating system functionality right in our script.
6. Because we’re following PEP 8 development guidelines and our imports should be in alphabetical order, under import logging, insert a line that says import os
7. We are going to spruce up our code a little bit before we add the relevant bits by adding in two new variables.

**Recall & Apply Learning from Intro to PowerShell** && **Think Critically and Creatively:** What are variables used for?

1. Above setting the logging basicConfig method, create a variable and name it format. Assign it ‘%(asctime)s - %(message)s’
   1. format = ‘%(asctime)s - %(message)s'
2. Using what you learned in the previous step, under your format variable, create a new variable called filename and assign it the string ‘keylog.txt’
3. Ask critical thinking questions with the following format:
   1. **[NWTC Employability Skill]:** Question?
4. Words that need definitions should be in **bold**
   1. **Word:** Definition
5. If giving any kind of command, highlight in yellow and use Consolas font: get-process | get-member
6. I usually add in a piece at the end about cleanup and next steps (maybe filling out the review questions, etc)
7. Pictures should have a title of *Figure #*
8. If you are calling a picture or graph, place the image above the numbered instruction. In the instruction, refer to the Figure #. For example, (see Figure 1 above).
9. When connecting to previous Learning Plans or other classes, use the following format: **Recall & Apply Learning from Learning Plan 1**