Python Scripting for CS – Lab 2

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:

* Modify an existing script
* Use Visual Studio Code
* Use Kali Linux
* Use logic
* Utilize Python libraries and modules

## Knowledge

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

* Utilize the basic syntax, data types, and control structures of Python
* Apply Python scripting skills to cybersecurity tasks
* Write Python scripts in a virtual environment

# Instructions

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

Answer the critical thinking questions as best you can.

# Formatting

|  |  |  |
| --- | --- | --- |
| Formatting | Explanation | Example |
| Definitions | Definitions are defined in bold | **Word:** This is the definition |
| Employability Skills | Employability skills are defined in green and associated with critical thinking questions | **Think Critically and Creatively** |
| Commands | Commands are written in Consolas and highlighted in yellow. Commands that are case sensitive will have an underline underneath the capitalized letter. | get-service |
| File names/paths, programs, & buttons | File names, programs, and buttons are written in Consolas and highlighted in gray. | C:\Tools\processes.txt |
| <dynamic content> | Content in <> should be replaced with what is required, removing the <> as well | \\<servername>\Home |
| Examples | Examples will be in Consolas and highlighted in blue | **skywalker.local** |
| Recall & Apply | Tasks that connect to previous course work will ask you to recall and apply learning from previous Learning Modules or classes | **Recall & Apply Learning from Network Essentials** |

# Criteria for Success

This assignment is worth 20 points. You will be graded on the script you created 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 LM02
3. Download keylogger.py and save it in your pythoncs/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 pythoncs/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.
   1. 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
4. Ensure that the following modules are imported in your script:
   1. logging
   2. os
5. We are going to spruce up our code a little bit before we add the relevant bits by adding in two new variables.
6. Assign it ‘%(asctime)s - %(message)s’
   1. format = ‘%(asctime)s - %(message)s'
7. 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’
8. Within the function, we are going to add an IF statement to check if the key pressed is @.
9. Your IF statement must include the following:
   1. window\_title = os.popen(‘xdotool getactivewindow getwindowname’).read()
   2. Modify the format variable to f’{window\_title}
   3. Recreate the logging.basicconfig to use the updated format variable
   4. Update logging.info to use the updated format
10. Test your script by typing an @ in any website.
11. Turn in your .py file and your keylog.txt file to the dropbox on Canvas for up to 20 points.