Something Awesome Report

Introduction:

My proposal for something awesome was to create a rubber ducky. My main motivation behind this project was to get myself to work on a hardware project.

After completing this project:

- I was able to learn how to program for arduino boards (beginner).
- Learn how to use powershell at a beginner level and found this to be much better than windows cmd.
- Explored about windows registry and learn how to manipulate windows registry keys.
- Create a windows task which launches a powershell process to run a powershell script.
- Learned how to create an exe of a python script. (pyinstaller).

Goals set at the start of the term were:

- DIY USB Rubber Ducky with an Arduino. (Done)
- Keyboard and mouse emulation. (Keyboard emulation done)
- Deliver and execute payloads automatically. (Done)
- Focus on Extended goals. (Did not set them in the proposal. Hopefully one of the four payloads can count as an extended goal.)
- At the end of the term write a blog about the something awesome project. (Done)
    - Link : https://www.openlearning.com/u/usamasadiq-q5zh3h/blog/SomethingAwesomeUpdate/

Implementation:

In order to recreate a rubber ducky using arduino, I used sparkfun arduino micro pro and a USB to Micro-B Adapter which enables me to connect arduino as a USB to the computer. Arduino Micro Pro board has a USB transceiver inside 34U4 which allows us to connect.

Following is a brief description about the payloads:

1. Open notebook using windows Run and print Hello World:
    a. This was really a simple payload\script in order to complete the Keyboard emulation and automatic delivery of payloads.

2. Steel Wifi Password:
    a. This payload first finds the SSID of the current wifi and sends the output to a Temp.txt file. Then it attaches Temp.txt file and sends an email. In the end, it will delete the Temp.txt file to cover our tracks.

3. Bypass UAC and create an admin account:
    a. This payload first bypasses the UAC. It will then run powershell as an admin and use the net command on powershell to create a user named ‘ADMIN’ and give it admin.rights This script also uses windows registry to hide the account from windows lock screen. In the end, it will delete the entries of windows run by deleting the entries from windows registry.

4. Bypass UAC, Run logger.exe and Create a Task using Task Scheduler:
    a. This payload again will first bypass the UAC. It will change its directory to %userprofile% and then download 3 files from my google drive. The 3 files downloaded are logger.exe, and 2 powershell scripts. Logger.exe is a keylogger written in python using pynput library and then converted to an exe using pyinstaller. The other two powershell scripts are responsible to stop the logger.exe process, send an email with an attachment file ‘Key_log.txt’, delete ‘Key_log.txt’ and then start logger.exe again. The payload then creates a Task using Task scheduler in powershell. The task will be responsible to run the powershell script after every x minutes which we can be set. The thinking behind creating a task was to get an email of key_log.txt after every x minutes.

Conclusion and Improvements:

One of the goals I set initially was to also learn soldering parts of the USB rubber ducky but due to campus closure and not wanting to buy a soldering set, I was not able to complete that. One of the roadblocks I faced was to set the delay after the commands. It took a little bit of time to fine tune those delays. I also feel that the last payload can be improved as I can hide the task which is created from the Task Scheduler UI and minimize or rescale powershell windows to a smaller size. Still at the end if I look back at the journey, I was able to learn quite a lot and hopefully my journey will not stop here.