System and Software Security

Fall 2022

Instructor: Van-Linh Nguyen

Assignment 01

Due: **2022/10/19 11:59**

General policy:

- No delay unless you have good reasons to explain.
- The report must be converted into .PDF file (Don't use Microsoft Docx or other formats)
- Please pack all your submissions in one zip file with name "SSS2022-HW1-StudentID" and send to cybersccu@gmail.com
- Copy and paste from others **are not allowed**. If you have extensive resources to refer, please cite the source. I highly recommend the answer/code in your own words (English).
- I can randomly pick someone in our class to demonstrate the homework results and answer questions. The demonstration will get additional 10-20 points (if it works).
- If there is any question on the homework, you can send email to cybersccu@gmail.com

1. Programming

Mastering Assembly programming plays a critical role to understand malware analysis and system security in depth. Please write an Assembly program to do the following features

- ✓ Input your name from the keyboard (10 pts)
- ✓ Duplicate several folders with your name in disk C:\ or a pre-defined path (20pts)

Expected Output: Assembly program source code with your comments of the function ability of each code group

2. Reverse Engineering

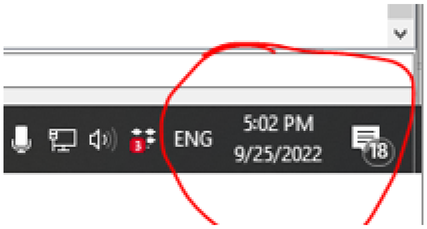
In our lessons, I have introduced that there are two methods for malware analysis: Static Analysis (Disassembler) and Dynamic Analysis (run malware in Sandbox/virtual machine and use tools to monitor its behavior). In this assignment, please reverse the provided malware (link below) and report the following information

- ✓ The attack goals (how it works, what damages/ annoyance it can cause) (10pts)
- ✓ The window kernel functions it used (10pts)
- ✓ Which system files did the malware modify or update? (10pts)

- ✓ Suggestion how to prevent the malware (10pts)

Malware download link: https://ccucyberseclab.github.io/store/malware/Lab1.zip

Expected Output: a report file with detail descriptions of how you find out the information and screenshot with window time at the bottom right of your PC.



3. Window kernel files

In our lessons, I have introduced fundamental architectures of Window kernel. Based on the knowledge, please do the following things

- Please list 8 most important/common kernel files in Window 10 Pro and their functions (10pts)
- Please find the location of your printer driver files (.dll) and its version (10pts). If you have no printer, you can find the location of all Window driver files.

Expected Output: Please append your list/screenshots to the report file in the question 2 above.

4. Hashing the important files

Protecting our system against malware modification is an essential task of a security expert. In this lab, you can practice to protect important files by hashing your important files and provide hash code for reference. In the future, you can use these hash code to check whether your files are modified.

- Hash your report file + code with MD5 and SHA1 and then create a text file "HashCode.txt" to insert the created hash code (10 pts)

Expected Output: Please create a text file "HashCode.txt" to insert the created hash code