Comp 7615 Computer Systems Technology November 2018

Malware Analysis

Assignment #4

Due Date: November 10, 2018 - 1000 hrs. This is an individual assignment.

Objective: To reverse engineer and analyze an unknown binary and explain its functionality in detail. **Always carry out code analysis in a safe and protected environment**.

Assignment:

- You have been provided with a sample binary (“**ass4**”), which you will analyze and reverse engineer using the techniques discussed in the current module.
- The objective is to fully understand and provide a detailed explanation of the functionality of the code.
- Start with static analysis, followed by dynamic analysis.
- As usual run all programs in a safe and isolated environment.
- Follow the steps outlined in the lecture and notes for this module.
- Provide **detailed explanations and screenshots** of all the steps that were performed as part of your analysis.

Constraints:

- The experiments for assignment are to be carried out using any of the tools covered to date.
- Your experiments must clearly show the portions of dissembled code that were used for the detailed authentication code analysis.
- You must provide evidence to back up all of your analysis and conclusions.
- Your grade will be based on the amount of technical detail and depth of analysis provided in your report.

To Be Submitted:

- All your documentation must be submitted in **PDF** format.
- Submit a **zip** file containing all the code and documents as described above in the **sharein** folder for this course under “**Assignment #4**”.

Evaluation:

(1). **Documentation/Report**:	/ 5
(2). **Evidence:**	/ 20
(3). **Detailed Analysis**:	/ 25
Total:	/ 50