**CSEC 476 Malware Reverse Engineering**

**Fun with Programming & Reversing Project**

Task #1

* Using your knowledge of C/C++, design a simple program that uses a client and server to communicate back and forth, such that the server can elicit the client to:
  + List out currently running processes
  + Upload/download a file
  + Send client information to the server, including
    - IP address
    - MAC address
    - Username
    - Operating System
* Data sent in transit from the client to the server (and vice versa) MUST be encrypted or encoded
  + Coders’ choice what you use, but it MUST be YOUR design! BE CREATIVE!
    - Static libraries and APIs for common algorithms (AES, Blowfish, TEA, etc.) are strictly prohibited

Task #2

* After completing your program, your second task is to reverse engineer the client.
  + Completely annotate the subroutine(s) responsible for your encryption/encoding algorithms.
    - Appropriately naming subroutine(s)
    - Naming all variables, and what they do within the IDB
  + Explain, using IDA, how the program interprets commands from the server and how it processes the output
    - Use screenshots, here, to help illustrate exactly what is going on.
    - Annotations within your IDB may also be helpful.
* Explain how tinkering with compiler settings can change the disassembly of your program.
  + Provide examples of settings you used and screenshots.

**Goals**

* By writing your own program and reversing it, you will become more familiar with x86 constructs.
* Since the code is your own, you will have a good idea of how it should run. This should help inform your reversing.

**Details**

* You may work in groups of two, but no more than three individuals can be in a single group.
* The client must be written in C/C++ and work on Windows 10.
* Presentations MUST NOT exceed 30 minutes, BE PREPARED to demo your work.

**Expectations**

* You will be expected to conduct a live demo of all the capabilities outlined in Task #1.
* Provide a PowerPoint presentation to the class explaining the following
  + Your approach and implementation
  + Answers to all the bullets poised in Task #2
    - Thoroughly documenting all desired variables in IDA
* You will be evaluated on the following
  + Creativity in design and implementation
    - The more sophisticated, the better. This is at the professor’s discretion.
  + Explanation to the class of your approach and implementation.
  + Answers to the class on the criteria from Task #2
    - Thorough documentation/explanation is an absolute must!

**Due Date**

* Day 1 of Week 14
  + Be ready with slides that speak to the material set forth in the project expectations.
  + Be prepared to demonstrate your program in action. You will *do it live!*