Lessons Learned

* How to use the tools
* Created a cycle of analysis-design-implementation-testing for each problem encountered as we executed the program
* Learned what is the best approach to malicious, irritating code segments, or function calls
  + Whether we redirect jumps, return a function, rewrite program to execute empty cycles, or modifying where the input was being stored in the stack
  + Tracing through each line of the executable in the Window Visual Studios debugger
* What recommendations would you give to others investigating an unknown executable?
  + 1. Recommend Relyze or another reverse engineering tool that shows the flow of a program
       - Helps see how the code executes
       - How the different functions work with each other
    2. Recommend running the program in a safe environment such as a VM
       - Can observe the program behavior at runtime and identify different problems
    3. Keep a work log of code that was changed, where it was, what it was originally, what it was changed to
       - Version control
       - Test after each change
    4. Regular group meetings
       - Issue tracking
       - Work update