# Final Project: Static Malware Analysis

See Webcourses and the syllabus for due dates.

## What to turn in

For the problems in this homework that require an English answer, you will upload a word document or a PDF file. However, some parts of the problems require an upload of an IDA Pro database (`.idb`) file.

## General Directions

The zip file for this homework is encrypted to avoid having your virus scanner delete it. The password is "malware" (without the quotes).
You will need the IDA Pro tool. The free version is available at
https://www.hex-rays.com/products/ida/support/download_freeware.shtml.
This homework is intended for individuals; as it is substituting for a final exam, we would strongly prefer that you not work in groups.

## What to Read

Read Part 2 (Chapters 4-7) of the book *Practical Malware Analysis* [SH12]. If you have time also read chapters 5-7 of the book *The IDA PRO Book* [Eag11]. If you don't have *The IDA Pro Book*, consider getting it! If you can't get the book, look at the tutorial material at
https://www.hex-rays.com/products/ida/index.shtml. The IDA Pro manual is at
https://www.hex-rays.com/products/ida/support/idadoc/.

## Problems

If you run the code, be sure to do it in a virtual machine or some other safe environment! See Chapter 2 of the book *Practical Malware Analysis* [SH12] and the course's analysis tools page for how to do this.

1. [Reversing] In this problem you will reverse engineer the program in `s3.exe` that is contained in the zip file (`final.zip`). Use (the free version of) IDA Pro for this.
   (a) (5 points) What is the entry point of the program?
   (b) (10 points) Using (the free version of) IDA Pro, comment each line of the code. You need only comment the lines of code that contain instructions (not data or IDA pro declaration or information lines) in the identified functions. To comment a line of code in IDA Pro, put the mouse cursor in the line, then type the colon (:) key; a comment dialog will appear. Fill in a comment and then click on the OK button. The colon (:) key can also be used to edit a comment (and override automatically generated comments) in the same way.

   Your comments on the code will be graded on how informative they are from a high-level perspective. That is, the comments should describe the high-level purpose of the code if possible. For example, instead of saying that the instruction `mov ebp, esp` "puts the value of esp into ebp", it is more informative to say that this instruction "sets the base pointer for the new stack frame."

   Hints: Look up calls to Windows API functions by searching for information about them from MSDN (or use a web search). It will help if you rename the automatically-generated variable names. Once you have saved your IDA Pro session as a database file (`.idb` file), you can work with that file outside of a virtual machine, as long as you don't try to run the file using the debugger.

Save your work often, as there is no "undo" key in IDA Pro. You can also produce a listing file (with your comments) by using the File > Produce... > Produce LST file menu.

You will hand in an IDA Pro database file (named with a `.idb` file extension) or a listing file for this part of the question.

(c) (5 points) What does the function at the program's entry point do? Give an English explanation that is justified by the disassembly.

(d) (10 points) Produce C code that is functionally equivalent to the function that starts at virtual address `00401000h`. Check your code over to make sure that the details are justified based on the disassembly.

(e) (5 points) [SecurelyConstruct] Does the code for the program `s3.exe` have any vulnerabilities you can see? Give a high-level English description.

(f) (10 points) What input would need to be given to the program `s3.exe` that would make it output the string `"you win!"`? Give the input (the exact characters) and a brief justification based on the disassembly.

2. [Reversing] In this problem you will reverse engineer the program in `l34.exe` that is contained in the zip file (`final.zip`). Use (the free version of) IDA Pro for this.

(a) (30 points) Using (the free version of) IDA Pro, comment each line of the code. You need only comment the lines of code that contain instructions (not data or IDA pro declaration or information lines) in the identified functions. You don't have to comment on every single line of code, but do enough of the main functions to answer the other questions (below). In particular, you don't have to comment on all of the DLL, library functions, and all of the functions generated by the compiler (as boilerplate) for interfacing with the Windows OS.

Your comments on the code will be graded on how informative they are from a high-level perspective.

You will hand in an IDA Pro database file (named with a `.idb` file extension) or a listing file for this part of the question.

(b) (15 points) How can the program be successfully installed? Give detailed instructions that are justified by the disassembly.

(c) (10 points) What does the program do after it installs itself? Give a high level English description that makes reference to the disassembly to justify details.

# Points

This homework's total points: 100.

# References

[Eag11] Chris Eagle. *The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler*. No Starch Press, San Francisco, 2011.

[SH12] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, San Francisco, 2012.