Hw 1. Disassembly

A. Use Ghidra to disassemble and decompile a binary executable (50%)

Please follow the tutorial slides to install Ghidra and answer the following questions.

Q1. The program “a.exe” will ask for a password. If the right password is entered, a congrats message will appear on the screen. Try to use Ghidra (or whatever tools you would like to use) to dissemble a.exe and extract the password and the congrats message. In your answer, please include

1. Your steps (e.g., screenshots etc.).
2. The password you found.
3. The congrats message you found.

B. Obfuscation (50%)

Before starting part B, please check the GitHub page of ollvm[1] for installation and usage instructions.

For question Q2 and Q3, you need to write (or find) a tiny C/C++ program and use Ghidra to demonstrate the differences in the machine code generated from the program by a regular compiler (e.g., clang) and the obfuscating compiler ollvm.

The program doesn’t need to be complex. A 10~20 lines code should be sufficient showing the differences.

Q2. Explain the “Control Flow Flattening” feature of ollvm. Apply it to the program and report your findings. Please submit a copy of the source code of your program as well.

[1] https://github.com/obfuscator-llvm/obfuscator/wiki/Installation

Q3. Explain the “Bogus Control Flow” feature of ollvm. Apply it to the program and report your findings. Please submit a copy of the source code of your program as well.

C. Submission

All your files should be organized in the following hierarchy and zipped into a . zip file named HW1_xxxxxxx.zip, where xxxxxxx is your student ID.

The zip file must include:

- Source code you use for the homework. If the code is used in Question X, please name the file to qX.c or qX.cpp.
- A report in PDF format with the answers to the questions. Name your report as xxxxxxx.pdf, where xxxxxxx is your student ID.

D. Reference

https://ghidra-sre.org/
https://github.com/obfuscator-llvm/obfuscator