实验 - reverse 专题2

实验简介

课程主要介绍了常见的三种混淆方式和其对应的去混淆思路与方法，实验中将进行复习和实践

基础部分 - 去混淆实战

二进制代码见附件中的 `basic.elf`

main函数去混淆 30分

- 识别 `main` 函数中使用的混淆方式
- 重写 `main` 函数为 C 代码并完成去混淆
- 报告中请记录操作步骤以及最后去除混淆的C代码

sub_400A70 函数去混淆 30分

- 识别 `sub_400A70` 函数（即位于地址 0x400a70 处函数）中使用的混淆方式
- 重写 `sub_400A70` 函数为 C 代码并完成去混淆
- 报告中请记录操作步骤以及最后去除混淆的C代码

sub_4009D0 函数去混淆 30分

- 识别 `sub_4009d0` 函数（即位于地址 0x4009d0 处函数）中使用的混淆方式
- 重写 `sub_4009d0` 函数为 C 代码并完成去混淆
- 报告中请记录操作步骤以及最后去除混淆的C代码

getflag 10分

完成去混淆后这个题目的逻辑似乎很清楚了，请完成逆向并获得该逆向题的 flag

挑战部分 - 虚拟机去混淆

如果虚拟机和混淆一起使用会发生什么?

尝试破解 advanced.elf 这个程序并给出该题目的 flag

拓展问题和阅读

- ollvm源代码
  - https://github.com/obfuscator-llvm/obfuscator