实验 - 逆向

实验简介

这一节课讲了多种逆向工具的使用方法, 也实战演示了几个程序的逆向破解. 那么现在就到了同学们大显身手的时候了!

基础部分

1. IDA操作练习 (40 points)

课堂上画了较多的时间介绍IDA软件的相关操作，为了变得更熟练，请完成如下联系

> 请随意选取程序，课上的程序，或者自己编译的程序均可

- 将目标程序正确载入IDA（请按架构正确载入）
- 载入后找到main函数并对汇编窗口的CFG页面和代码页面进行展示
- 通过 F5 查看 main 函数的伪代码内容
- 尝试修改 main 的函数名为其他名字
- 尝试修改 main 的函数参数个数
- 尝试进入字符串窗口找到字符串并进行引用查找
- 尝试利用 edit - patch 任意修改程序的代码（没学过汇编的可以简单 nop 一下指令）
- （如果是windows host）尝试跑一下 IDA 的 local debug 功能

2. reverse1 (30 points)

url: https://zjusec.com/challenges/26

要求记录分析过程，并给出解答的flag

3. 分享的zju云盘中的attachment(30 points)

url: https://pan.zju.edu.cn/share/612f7d5bc15ee7745c9a21dba4

要求记录分析过程，并给出解答的flag

挑战部分

1. reverse2 (40 points)

url: https://zjusec.com/challenges/15

静态工具逆向起来好像很麻烦的样子呀! 动调一下! 是不是有MessageBox可以下断点呢?

2. Start

url: https://zjusec.com/challenges/91

第一节课的原理都讲过了哦. 静态实在找不到的话试试看动调!

3. Hidden Executable

url : https://zjusec.com/challenges/135

第一节课上粗略的讲解了一下elf文件结构, 有兴趣的同学可以了解一下PE文件结构.

文档要求

以上基础部分题目是必做题, 需要描述详细的解题过程和最终的解密脚本. 挑战部分不做额外要求, 但当然希望大家也能试一试(题目难度大概是随题号上升的), 记录自己解题时候的心路历程. 最后, 做题时出现实在解决不了的问题欢迎私戳问我! 祝大家做题愉快!