实验 - reverse 专题1

实验简介

课程简单介绍了壳与虚拟机两种保护手段，作业中将对它们进行复习和拓展

基础部分

完成简单加密壳 (50分)

请根据提供的模板代码以及课堂上老师的演示，利用 `.init_array` 技术实现对于程序逻辑简单保护的加密壳，要求

- 至少保护 `main`，鼓励保护更多函数，或者更细粒度
- 不能简单异或加密，要求使用其他加密方式，如置换，或者流加密
- 提交最后源代码以及证明加壳程序成功运行的截图

完成简单栈虚拟机 (50分)

有如下要求

- 首先根据给定源代码完成逻辑分析，并给出flag
- 拓展已有栈虚拟机指令，要求至少支持
  - 栈上加法
  - 栈上减法
  - 栈上移位
  - 栈上异或
  - 栈上与
  - 栈上或
  - 其他可以根据兴趣做额外支持
- 根据拓展的指令重写 `vmcodes`，实现更复杂的判断逻辑而不是目前简单的比较；如完成凯撒加密后再比较
- 提交最后的虚拟机代码以及运行虚拟指令描述

挑战部分

阅读课堂上介绍的 dropper 的代码

https://github.com/marcusbotacin/Dropper

并将这类dump壳迁移到 Linux 平台上

> ELF没有resouce的概念，但可以使用objcopy来实现类似功能

拓展问题和阅读

- 壳和虚拟机哪种保护更好，为什么?

建议学习

- 课堂展示的 VM 的 blog
  - https://resources.infosecinstitute.com/topic/reverse-engineering-virtual-machine-protected-binaries/
- Hacklivestream
  - https://www.youtube.com/watch?v=nKhX0Pk3a5A
- C++逆向基础
  - https://pabloariasal.github.io/2017/06/10/understanding-virtual-tables/