计算机系统课程设计

设计内容：
1 二进制程序逆向工程
2 缓冲区溢出攻击
3 程序的链接

设计目标：
1 加深对计算机系统的理解和掌握：程序的机器级表示、汇编与反汇编、二进制程序分析与调试、逆向工程；函数调用规则、栈结构、缓冲区溢出攻击原理、方法与防范；程序链接中符号解析、重定位等基本概念、位置无关代码和 ELF 文件的基本组成；
2 从程序员角度认识计算机系统，分析高级语言对应的机器行为及其对程序执行结果和性能的影响，解决计算机系统设计、程序开发过程中的关键问题；
3 掌握计算机系统思维，理解高级语言中数据、运算、过程调用和 I/O 操作等在计算机系统中的实现方法，将程序设计、汇编语言、系统结构、操作系统、编译链接中的重要概念贯穿起来；
4 掌握各种开源的编译调试工具，能够对分析优化程序设计，提高在代码调试、性能提升、软件移植和鲁棒性等方面的能力。

设计任务：
1 学习 MOOC 内容
https://www.icourse163.org/learn/NJU-1449521162
第五周 二进制程序逆向工程
第 1 讲 二进制炸弹实验：概述
第 2 讲 二进制炸弹实验：字符串比较
第 3 讲 二进制炸弹实验：浮点数表示
第 4 讲 二进制炸弹实验：课后实验

https://www.icourse163.org/learn/NJU-1449521162
第六周 缓冲区溢出攻击
第 1 讲 缓冲区溢出攻击实验：概述
第 2 讲 缓冲区溢出攻击实验：目标程序与辅助工具
第 3 讲 缓冲区溢出攻击实验：Level 0
第 4 讲 缓冲区溢出攻击实验：Level 1 及课后实验

https://www.icourse163.org/learn/NJU-1449521162
第七周 程序的链接
第 1 讲 链接与 ELF 实验：概述
第 2 讲 链接与 ELF 实验：静态数据与 ELF 数据节
第 3 讲 链接与 ELF 实验：指令与 ELF 代码节及课后实验

2 完成作业
从以下三个主题中任选至少 3 个小题（可以属于同一主题，也可以分属不同主题，鼓励多选），完成课程设计实验，并撰写设计报告，详细说明实验完成的步骤和原理。

2.1 二进制逆向工程
2.1.1 循环（phase2）
2.1.2 条件/分支（phase3）
2.1.3 递归调用和栈（phase4）
2.1.4 指针（phase5）
2.1.5 链表/指针/结构（phase6）
2.1.6 隐藏阶段
详见 MOOC 二进制逆向工程实验文档
注意：本实验提供的代码和 MOOC 视频讲解内容不完全相同，需要根据代码中的实际内容完成作业。

2.2 缓冲区溢出攻击
2.1 bang（level2）
2.2 rumble（level3）
2.3 boom（level4）
2.4 kaboom（level5）
详见 MOOC 缓冲区溢出攻击实验文档
注意：和本实验提供的代码和 MOOC 视频讲解内容不完全相同，需要根据代码中的实际内容完成作业。

2.3 链接与 ELF
2.1 符号解析（phase3）
2.2 switch 语句与重定位（phase4）
2.3 可重定位目标文件（phase5）
2.4 位置无关代码（phase6）
详见 MOOC 链接与 ELF 实验文档
注意：和本实验提供的代码和 MOOC 视频讲解内容不完全相同，需要根据代码中的实际内容完成作业。