《计算机系统基础实验》任务书

# **实验三 二进制炸弹破解**

# 实验目的与要求

1. 熟悉动态与静态反汇编工具；
2. 熟悉程序的机器级表示，掌握逆向工程的原理与技能；
3. 完成执行程序的调试，提升对计算机系统的理解与分析能力。

# **实验内容**

（上机实验环境说明：本次实验使用使用Linux环境，需要使用gdb和objdump工具。)

## 任务3.1 破解“二进制炸弹”

“二进制炸弹”是一个 Linux 可执行程序。每个同学按自己学号的后七位数字，到群文件中下载自己的压缩包，解压后可得到bomb执行程序和bomb.c总控源程序。

bomb执行程序由六个阶段组成。每个阶段都需要输入特定的字符串。如果输入了正确的字符串，那么该阶段就“解除”。 否则，炸弹会通过打印“BOOM！！！”。每个同学的目标是解除尽可能多的阶段。

* 进度提示：

本实验使用两次课内上机，8学时完成。找出尽可能多的密码字符串。

# **提示**

每个同学的“解除”字符串也会不同。每个炸弹阶段会测试不同的方面：

第1阶段：字符串比较

第 2 阶段：循环

第 3 阶段：条件/开关

第 4 阶段：递归调用和堆栈规则

第 5 阶段：：指针

第 6 阶段：：链表/指针/结构体

还有一个“秘密阶段”，仅当学生将特定字符串附加到第四阶段时才会出现。

为了拆除炸弹，学生必须使用调试器，通常是gdb反汇编执行文件，并单步执行每个阶段的机器代码，使用课程中的知识来推断“解除”字符串。

还可以使用objdump工具，将bomb执行程序静态反汇编，通过研读生成的源程序，理解和掌握bomb的执行过程。objdump反汇编得到源程序的命令为：

objdump -d bomb > bomb.s