

**实验报告**

**实 验（三）**

题 目 Binary Bomb

二进制炸弹

专 业 计算机类

学　　 号 1190200523

班　　 级 1903002

学 生 石翔宇

指 导 教 师 郑贵滨

实 验 地 点 G709

实 验 日 期 2021.4.23

**计算机科学与技术学院**

**目 录**

[第1章 实验基本信息 - 3 -](#_Toc496608242)

[1.1 实验目的 - 3 -](#_Toc496608243)

[1.2 实验环境与工具 - 3 -](#_Toc496608244)

[1.2.1 硬件环境 - 3 -](#_Toc496608245)

[1.2.2 软件环境 - 3 -](#_Toc496608246)

[1.2.3 开发工具 - 3 -](#_Toc496608247)

[1.3 实验预习 - 3 -](#_Toc496608248)

[第2章 实验环境建立 - 4 -](#_Toc496608249)

[2.1 Ubuntu下CodeBlocks反汇编（10分） - 4 -](#_Toc496608250)

[2.2 Ubuntu下EDB运行环境建立（10分） - 4 -](#_Toc496608251)

[第3章 各阶段炸弹破解与分析 - 5 -](#_Toc496608252)

[3.1 阶段1的破解与分析 - 5 -](#_Toc496608253)

[3.2 阶段2的破解与分析 - 5 -](#_Toc496608254)

[3.3 阶段3的破解与分析 - 5 -](#_Toc496608255)

[3.4 阶段4的破解与分析 - 5 -](#_Toc496608256)

[3.5 阶段5的破解与分析 - 5 -](#_Toc496608257)

[3.6 阶段6的破解与分析 - 5 -](#_Toc496608258)

[3.7 阶段7的破解与分析(隐藏阶段) - 6 -](#_Toc496608259)

[第4章 总结 - 7 -](#_Toc496608260)

[4.1 请总结本次实验的收获 - 7 -](#_Toc496608261)

[4.2 请给出对本次实验内容的建议 - 7 -](#_Toc496608262)

[参考文献 - 8 -](#_Toc496608263)

# 第1章 实验基本信息

## 1.1 实验目的

* 熟练掌握计算机系统的ISA指令系统与寻址方式
* 熟练掌握Linux下调试器的反汇编调试跟踪分析机器语言的方法
* 增强对程序机器级表示、汇编语言、调试器和逆向工程等的理解

## 1.2 实验环境与工具

### 1.2.1 硬件环境

* Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
* 16GB RAM
* 1TB HDD + 512G SSD

### 1.2.2 软件环境

* Windows 10 21H1
* Ubuntu 20.04 LTS

### 1.2.3 开发工具

* VSCode，CodeBlocks，gcc+gdb，edb

## 1.3 实验预习

* 上实验课前，必须认真预习实验指导书（PPT或PDF）
* 了解实验的目的、实验环境与软硬件工具、实验操作步骤，复习与实验有关的理论知识。
* 请写出C语言下包含字符串比较、循环、分支（含switch）、函数调用、递归、指针、结构、链表等的例子程序sample.c。
* 生成执行程序sample.out。
* 用gcc –S或CodeBlocks或GDB或OBJDUMP等，反汇编，比较。
* 列出每一部分的C语言对应的汇编语言。
* 修改编译选项-O (缺省2)、O0、O1、O2、O3，-m32/m64。再次查看生成的汇编语言与原来的区别。
* 注意O1之后无栈帧，EBP做别的用途。-fno-omit-frame-pointer加上栈指针。
* GDB命令详解 –tui模式 ^XA切换 layout改变等等
* 有目的地学习: 看VS的功能GDB命令用什么？

# 第2章 实验环境建立

## 2.1 Ubuntu下CodeBlocks反汇编（10分）

CodeBlocks运行hellolinux.c。反汇编查看printf函数的实现。

要求：C、ASM、内存(显示hello等内容)、堆栈（call printf前）、寄存器同时在一个窗口。

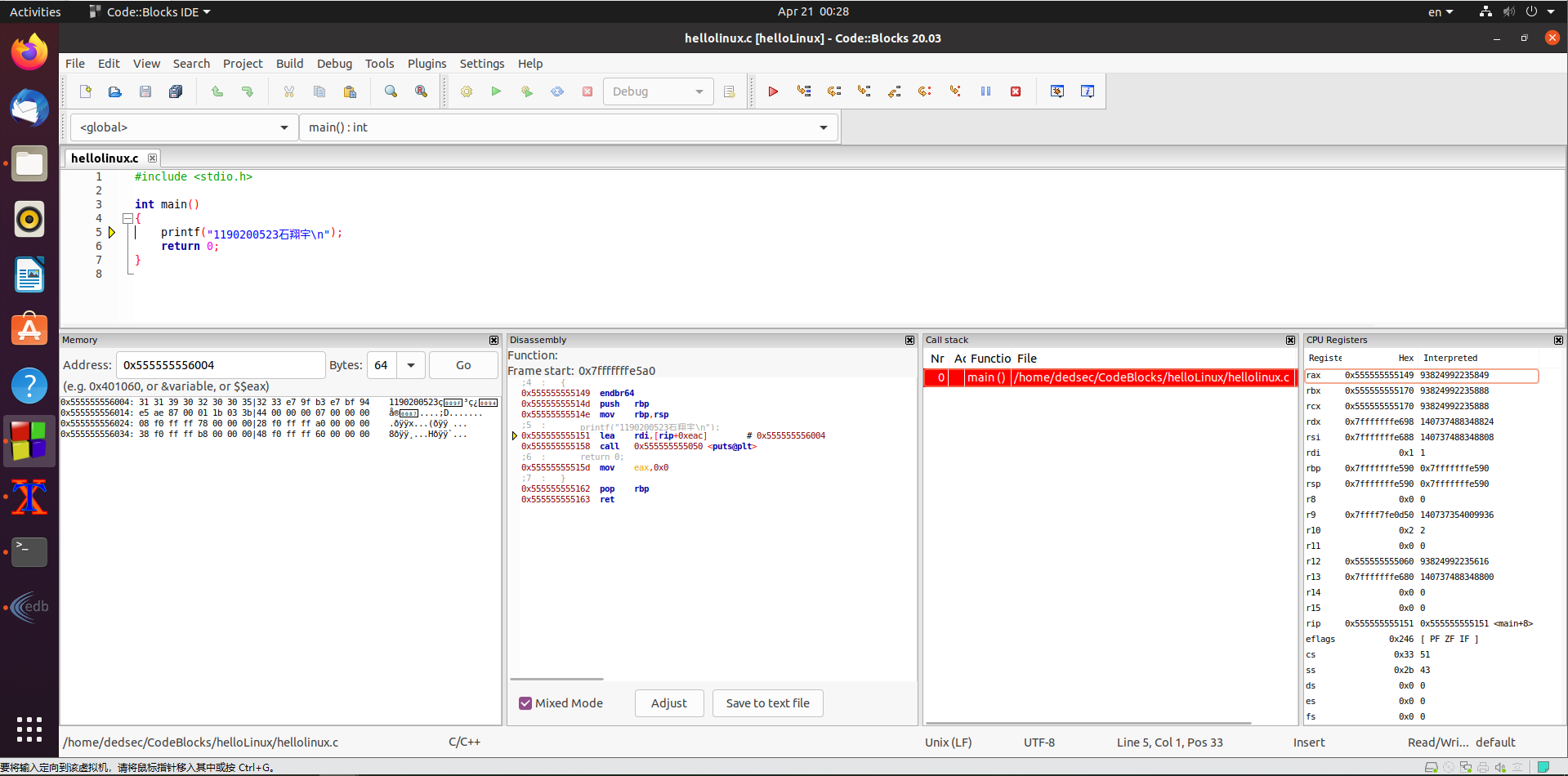


图2-1 Ubuntu下CodeBlocks反汇编截图

## 2.2 Ubuntu下EDB运行环境建立（10分）

用EDB调试hellolinux.c的执行文件，截图，要求同2.1

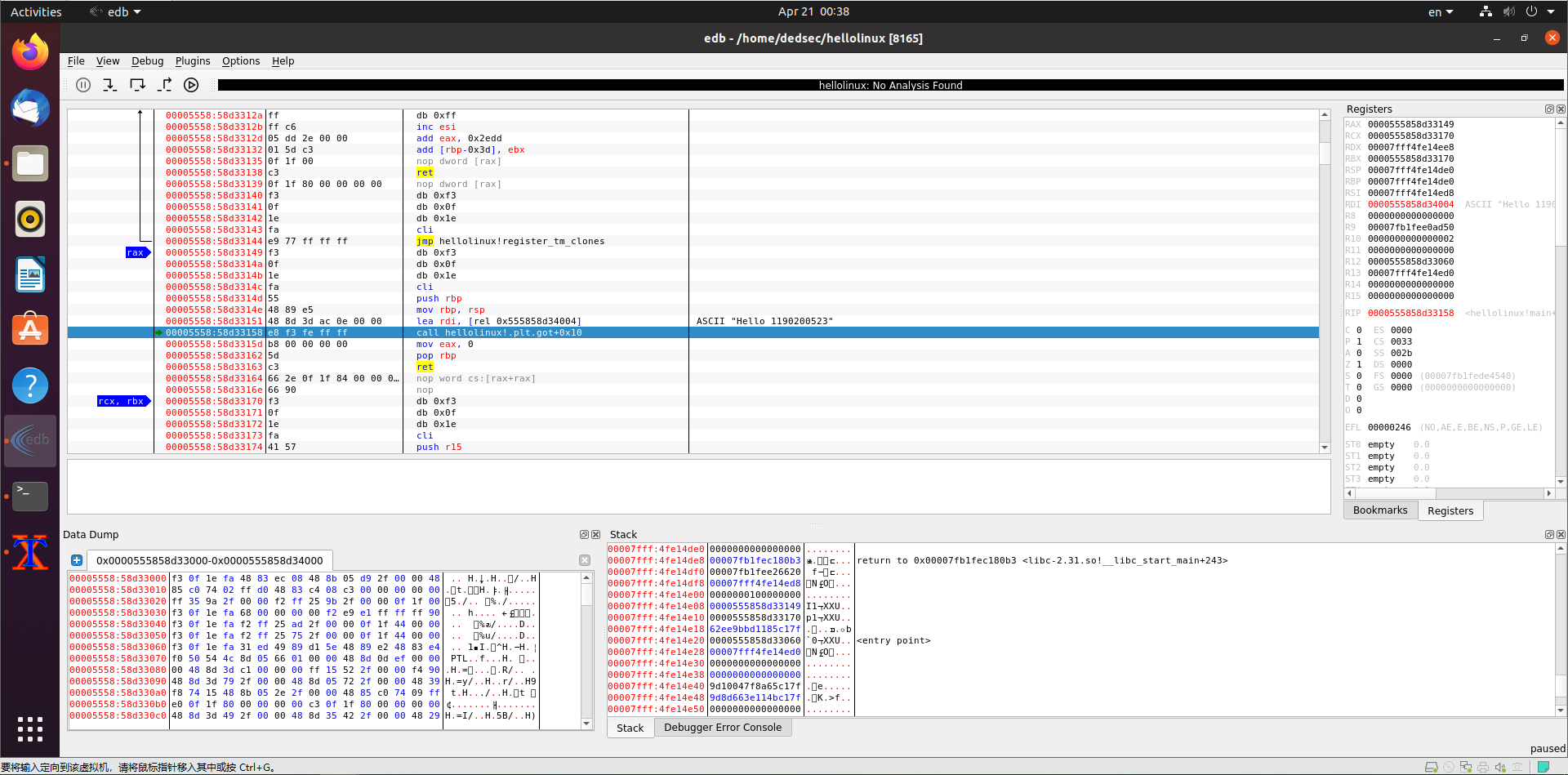


图2-2 Ubuntu下EDB截图

# 第3章 各阶段炸弹破解与分析

每阶段15分（密码10分，分析5分），总分不超过80分

## 3.1 阶段1的破解与分析

密码如下：You can Russia from land here in Alaska.

破解过程：

1. 查看反汇编代码得知此阶段比较字符串是否相等。
2. 由反汇编代码 4013fd: be 50 31 40 00 mov $0x403150,%esi得知答案字符串存在0x403150处
3. 提取得字符串16进制表示59 6f 75 20 63 61 6e 20 52 75 73 73 69 61 20 66 72 6f 6d 20 6c 61 6e 64 20 68 65 72 65 20 69 6e 20 41 6c 61 73 6b 61 2e
4. 转换成字符串“You can Russia from land here in Alaska.”，得到答案

## 3.2 阶段2的破解与分析

密码如下：1 2 4 7 11 16（满足第一个数为非负整数，其余依次递增1,2,3,4,5的六个整数即可）

1. 破解过程：查看反汇编代码

401421: e8 ef 04 00 00 callq 401915 <read\_six\_numbers>

及read\_six\_numbers的有关内容得知此阶段首先输入6个整数，存储于%rbp-0x30处。

1. 由反汇编代码

401426: 83 7d d0 00 cmpl $0x0,-0x30(%rbp)

40142a: 78 07 js 401433 <phase\_2+0x1f>

可知第一个数字不能为负数

1. 40142c: bb 01 00 00 00 mov $0x1,%ebx

首先设置%ebx为1，%ebx代表当前进行到第几个数字（下标从0开始），

401442: 83 fb 05 cmp $0x5,%ebx

401445: 7f 17 jg 40145e <phase\_2+0x4a>

当%ebx达到6时跳出，

401447: 48 63 c3 movslq %ebx,%rax

令%rax = %ebx，%rax表示当前第几个数字，

40144a: 8d 53 ff lea -0x1(%rbx),%edx

令%edx = %rbx(%ebx) – 1，%edx表示当前数字的前一个，

40144d: 48 63 d2 movslq %edx,%rdx

401450: 89 d9 mov %ebx,%ecx

令%ecx = %ebx，表示当前第几个数，也即当前数字需要比前一个数字大多少，

401452: 03 4c 95 d0 add -0x30(%rbp,%rdx,4),%ecx

-0x30(%rbp,%rdx,4)表示前一个数字的值，加到%ecx上，现在的%ecx就表示当前数字期望的值，

401456: 39 4c 85 d0 cmp %ecx,-0x30(%rbp,%rax,4)

-0x30(%rbp,%rax,4)表示输入的当前数字的值，%ecx表示当前数字期望的值，将两个数字进行比较，

40145a: 74 e3 je 40143f <phase\_2+0x2b>

若两数字相等则回到0x40143f，继续循环，

40145c: eb dc jmp 40143a <phase\_2+0x26>

否则炸弹爆炸。

1. 由此可知，满足第一个数为非负整数，其余依次递增1,2,3,4,5的六个整数即为答案。

## 3.3 阶段3的破解与分析

密码如下：

破解过程：

## 3.4 阶段4的破解与分析

密码如下：

破解过程：

## 3.5 阶段5的破解与分析

密码如下：

破解过程：

## 3.6 阶段6的破解与分析

密码如下：

破解过程：

## 3.7 阶段7的破解与分析(隐藏阶段)

密码如下：

破解过程：

# 第4章 总结

## 4.1 请总结本次实验的收获

## 4.2 请给出对本次实验内容的建议

注：本章为酌情加分项。

# 参考文献

**为完成本次实验你翻阅的书籍与网站等**

[1] 林来兴. 空间控制技术[M]. 北京：中国宇航出版社，1992：25-42.

[2] 辛希孟. 信息技术与信息服务国际研讨会论文集：A集[C]. 北京：中国科学出版社，1999.

[3] 赵耀东. 新时代的工业工程师[M/OL]. 台北：天下文化出版社，1998 [1998-09-26]. http://www.ie.nthu.edu.tw/info/ie.newie.htm（Big5）.

[4] 谌颖. 空间交会控制理论与方法研究[D]. 哈尔滨：哈尔滨工业大学，1992：8-13.

[5] KANAMORI H. Shaking Without Quaking[J]. Science，1998，279（5359）：2063-2064.

[6] CHRISTINE M. Plant Physiology: Plant Biology in the Genome Era[J/OL]. Science，1998，281：331-332[1998-09-23]. http://www.sciencemag.org/cgi/ collection/anatmorp.