

**实验报告**

**实 验（三）**

题　　 目 二进制炸弹Binary Bomb

专　　 业 人工智能

学　　 号 2021112845

班　　 级 2103601

学 生 张智雄

指 导 老 师 郑贵滨

实 验 地 点 G.709

实 验 日 期 2023.4.2

**计算学部**

**目 录**

[第1章 实验基本信息 - 3 -](#_Toc19846)

[1.1 实验目的 - 3 -](#_Toc19505)

[1.2 实验环境与工具 - 3 -](#_Toc15894)

[1.2.1 硬件环境 - 3 -](#_Toc16679)

[1.2.2 软件环境 - 3 -](#_Toc1640)

[1.2.3 开发工具 - 3 -](#_Toc311)

[1.3 实验预习 - 3 -](#_Toc20293)

[第2章 实验环境建立 - 4 -](#_Toc3866)

[2.1 Ubuntu下CodeBlocks反汇编（10分） - 4 -](#_Toc24906)

[2.2 Ubuntu下EDB运行环境建立（10分） - 4 -](#_Toc18077)

[第3章 各阶段炸弹破解与分析 - 5 -](#_Toc4144)

[3.1 阶段1的破解与分析 - 5 -](#_Toc24389)

[3.2 阶段2的破解与分析 - 5 -](#_Toc25931)

[3.3 阶段3的破解与分析 - 5 -](#_Toc21845)

[3.4 阶段4的破解与分析 - 5 -](#_Toc11024)

[3.5 阶段5的破解与分析 - 5 -](#_Toc29641)

[3.6 阶段6的破解与分析 - 5 -](#_Toc18838)

[3.7 阶段7的破解与分析(隐藏阶段) - 6 -](#_Toc20276)

[第4章 总结 - 7 -](#_Toc9339)

[4.1 请总结本次实验的收获 - 7 -](#_Toc16563)

[4.2 请给出对本次实验内容的建议 - 7 -](#_Toc27793)

[参考文献 - 8 -](#_Toc10577)

# 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

X64 CPU；2.30GHz；16G RAM；1.5THD disk

### 1.2.2 软件环境

Windows11 64位；Vmware Workstation 17 Pro；Ubuntu 22.10

### 1.2.3 开发工具

Visual Studio 2019 64位；CodeBlocks 64位；vim+gcc

## 1.3 实验预习

1. 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。
2. 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。
3. 生成执行程序sample.out。
4. 用gcc –S或CodeBlocks或GDB或OBJDUMP等，反汇编，比较。
5. 列出每一部分的C语言对应的汇编语言。
6. 修改编译选项-O (缺省2)、O0、O1、O3、Og、-m32/m64。再次查看生成的汇编语言与原来的区别。
7. 注意O1之后缺省无栈帧，RBP为普通寄存器。用 -fno-omit-frame-pointer 加上栈指针。
8. GDB命令详解 –tui模式 ^XA切换 layout改变等等
9. 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hello.c。反汇编查看printf函数的实现。

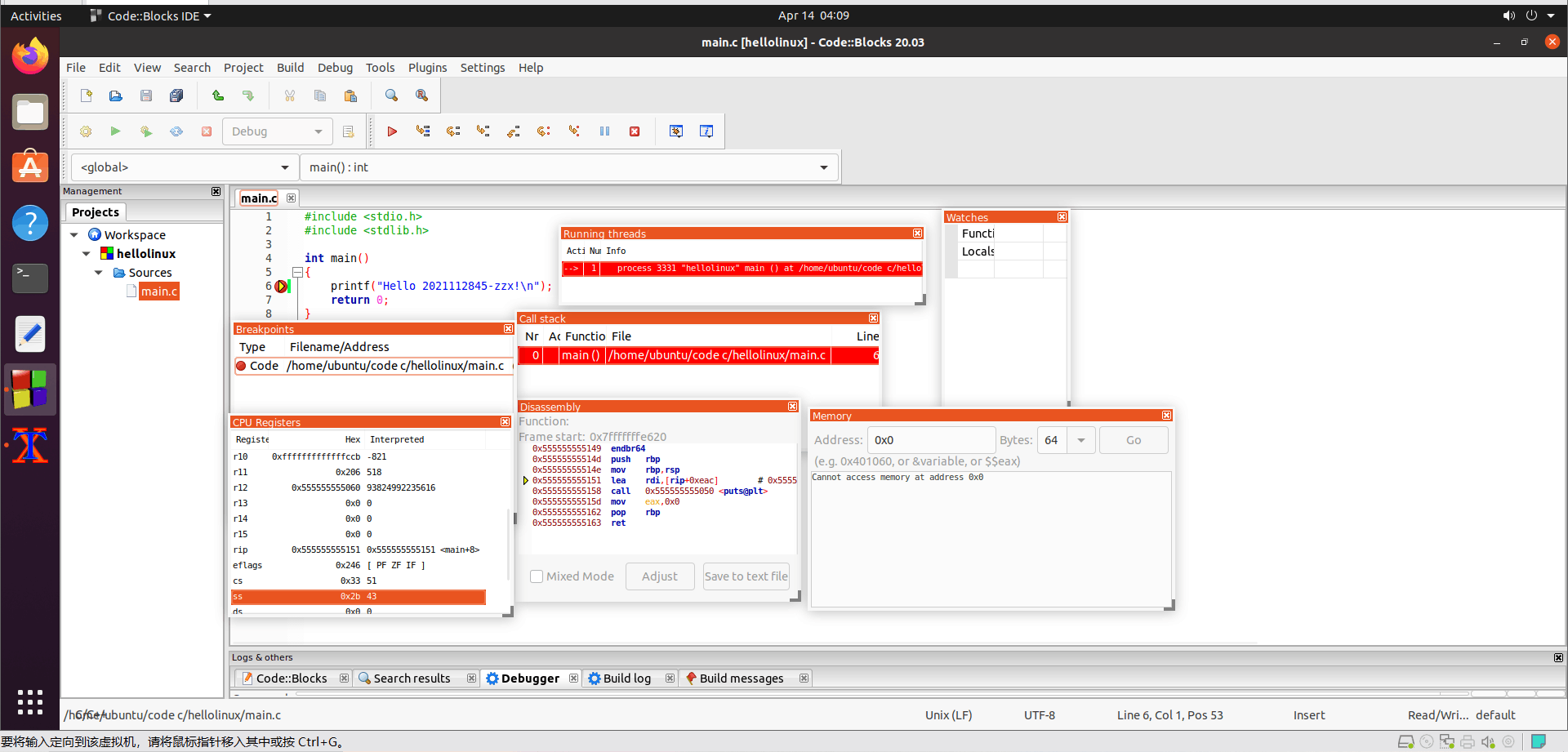


图2-1 Ubuntu下CodeBlocks反汇编截图

## 2.2 Ubuntu下EDB运行环境建立（10分）

用EDB调试hello.c的执行文件，截图，要求同2.1

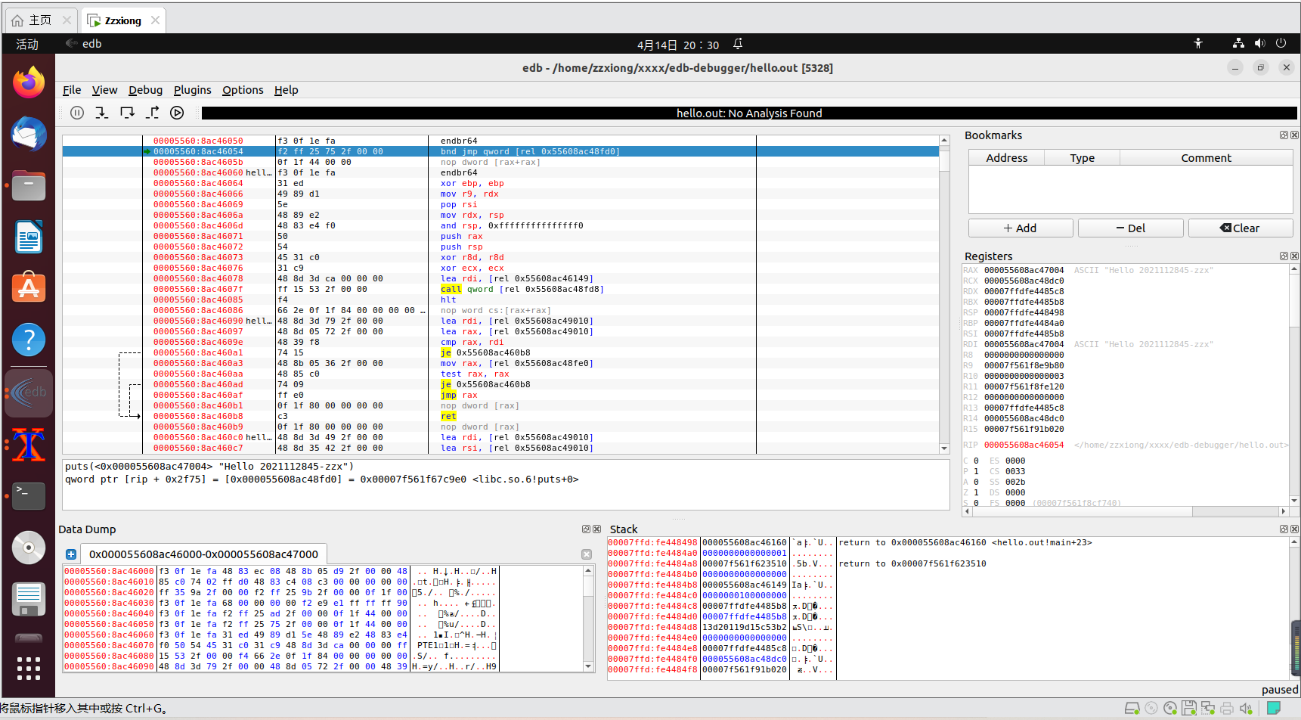


图2-2 Ubuntu下EDB截图

# 第3章 各阶段炸弹破解与分析

每阶段30分，密码10分，分析20分，总分不超过80分

## 3.1 阶段1的破解与分析

密码如下：All your base are belong to us.

破解过程：首先反汇编阶段1的函数代码，如下图3-1-1所示，观察分析得到此函数的运行逻辑：输入一个字符串，若与预设字符串不相同，则炸弹爆炸。

文本

描述已自动生成

图3-1-1 phase\_1反汇编代码

注意到在调用函数strings\_not\_equal时，地址0x403150传入作为函数参数，推测答案存放在此地址中，直接查看该地址的字符串，得到答案。



图3-1-2 phase\_1答案

## 3.2 阶段2的破解与分析

密码如下：1 2 4 8 16 32 64

破解过程：首先反汇编阶段2的函数代码，如下图3-2-1所示，注意到在0x401421地址处调用函数read\_six\_numbers，推测本关输入为6个数（起始地址为-x30(%rbp)）。

随后比较第一个数-x30(%rbp)与1，若不等于1，则炸弹引爆，于是第一个数解得为1。而后初始化%ebx为1，并作为循环标志量(int i = 1; i <=5; i++)。

文本

中度可信度描述已自动生成

图3-2-1 phase\_2反汇编代码

分析循环内部反汇编代码知，该程序检查首项为1，项数为6，公比为2的等比数列，可等价于如下代码：

文本

描述已自动生成

图3-2-2 phase\_2等价代码

故答案为1 2 4 8 16 32。

## 3.3 阶段3的破解与分析

密码如下：0 88 / 1 298 / 2 788 / 3 66 / 4 535 / 5 273 / 6 77 / 7 429

破解过程：首先反汇编阶段3的函数代码，截取部分如下图3-3-1所示，首先观察到输入的参数有两个，而后检查输入要求，得到输入要求为“%d %d”，分别储存在-0x8(%rbp)和-0x4(%rbp)中，同时注意到第一个参数-0x4(%rbp)必须<=7，否则炸弹引爆。

文本

描述已自动生成

图3-3-1 phase\_3反汇编代码

而后查看跳转表，跳转至相应地址可以发现会返回一个整数至%eax，即为第二个参数。故答案为0 88 / 1 298 / 2 788 / 3 66 / 4 535 / 5 273 / 6 77 / 7 429

图形用户界面, 文本

描述已自动生成



图3-3-1 phase\_3跳转表示意

## 3.4 阶段4的破解与分析

密码如下：108 2 / 162 3 / 216 4

破解过程：首先反汇编阶段4的函数代码，截取部分如下图3-4-1所示，观察到输入的参数有两个，分别储存在-0x8(%rbp)和-0x4(%rbp)中，注意到第二个输入值（地址为-0x4(%rbp)）的取值范围为，即可取2,3,4三个值，而后将与第二个参数传入func4函数，比较最后的返回值%eax与第一个输入值（地址为-0x8(%rbp)）进行比较，若不相同则炸弹爆炸。

文本

描述已自动生成

图3-4-1 phase\_4反汇编代码

而后查看的反汇编代码如下图3-4-2所示，可以看到当时函数返回值为；当时，函数返回值为。



文本

描述已自动生成

**递归主体**



图3-4-2 func4反汇编代码

分析递归主体得到。

运行函数程序得。故答案为108 2 / 162 3 / 216 4。

## 3.5 阶段5的破解与分析

密码如下：llllla（答案不唯一）

破解过程：首先反汇编阶段5的函数代码，截取部分如下图3-5-1所示，观察到函数开始时调用了string\_length函数，且若返回值不为6，则炸弹爆炸，因而输入为一个长度为6的字符串。同时注意到在函数包含一个从0到5的一个循环节，而在循环节中，将%rbx数组内的数据与0xf做按位与运算，将结果保存在%edx中，同时提取0x4031e0地址下数组内偏移量为%edx的数据进行累加，若最后累加结果不为0x41（十进制65），则炸弹爆炸。

文本

描述已自动生成

**循环**

图3-4-1 phase\_4反汇编代码

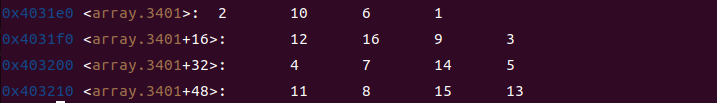


图3-4-2 0x4031e0地址下数组数据

因此，phase\_5函数可等价为下图代码，只需输入满足程序要求的6位字符串即可拆除炸弹，llllla为其中之一（答案不唯一）。

文本

描述已自动生成

图3-5-3 phase\_5等价代码

## 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

1. 了解了计算机系统的ISA指令系统与寻址方式，加深了对计算机指令的理解。
2. 熟悉了在Linux系统下使用GDB对程序进行调试分析，及利用反汇编调试跟踪分析机器语言的方法，加深了对程序运行中计算机各部分如内存、堆栈的工作原理的理解。
3. 熟悉了汇编语言，简单了解了高级语言到汇编语言编译过程，并结合具体实验巩固了程序的机器级表示相关知识。

## 4.2 请给出对本次实验内容的建议

1. 对EDB的安装及使用的教程和讲述不是很明确
2. 增加PPT部分内容的注解，有时不太能理解PPT的指令的用途及功能

注：本章为酌情加分项。

# 参考文献

[1]RANDALE.BRYANT, DAVIDR.O’HALLARON. 深入理解计算机系统[M]. 机械工业出版社, 2011.