哈爾濱工業大學

实验报告

实 验（三）

题　　目 Binary Bomb

二进制炸弹

专　　业 计算机类

学　　号 1160300823

班　　级 1603008

学　　生 陈柯昊

指 导 教 师 吴锐

实 验 地 点 G712

实 验 日 期 2017/10/26

计算机科学与技术学院

目 录

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；2GHz；2G RAM；256GHD Disk 以上

1.2.2 软件环境

Windows7 64 位以上；VirtualBox/Vmware 11 以上；Ubuntu 16.04 LTS 64 位/优麒麟 64 位；

1.2.3 开发工具

Visual Studio 2010 64 位以上；GDB/OBJDUMP；KDD 等

1.3 实验预习

填写

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。

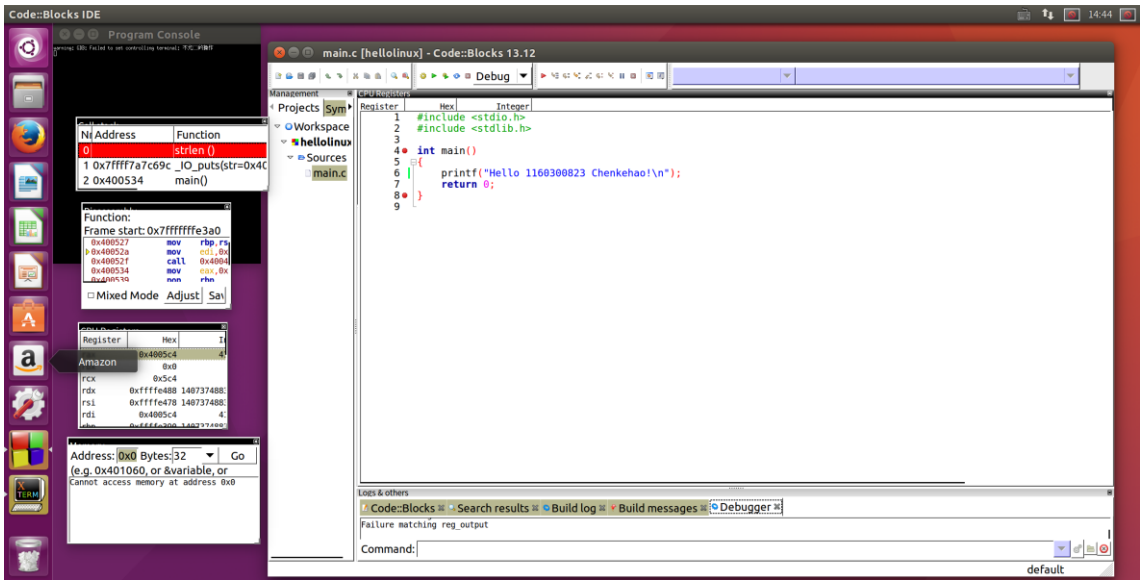

图 2-1 Ubuntu 下 CodeBlocks 反汇编截图

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

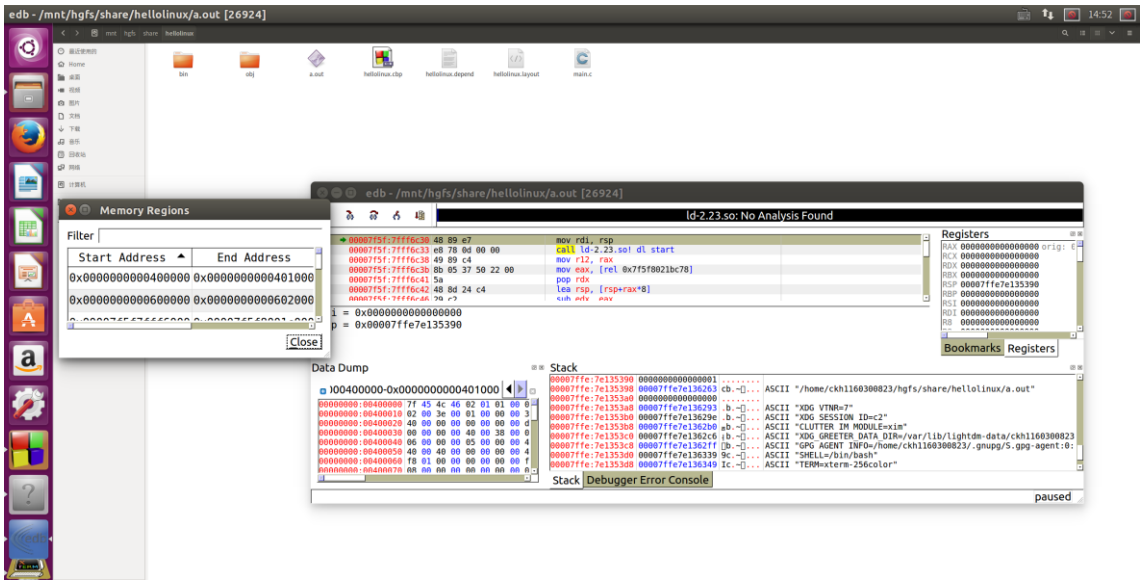

图 2-2　Ubuntu 下 EDB 截图

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：I turned the moon into something I call a Death Star.

破解过程：本题中有异常明显的暗示，显然，这个函数是一个判断字符串是否相等的函数。可以看到 MOV 调用了一个神奇的地址 0x402460，于是果断 x/2s 0x402460 得到字符串，从而通过第一关。

3.2 阶段 2 的破解与分析

密码如下：0 1 1 2 3 5

破解过程：本题考察循环结构。首先观察函数名，得知是一个要读取 6 个数字的函数。看到下面用 0x0 进行比较，则确定第一个数字为 0。再向下，有用 0x1 进行比较，则确定第二个数字为 1。如果没有注意到这个条件，则会发现，在下面的循环结构中，a[i] = a[i-1]+a[i-2]是不能成立的。循环结构内的具体运算由(%rbx),%eax 得知。

3.3 阶段 3 的破解与分析

密码如下：0 i 531

破解过程：首先观察函数，发现是一个读入的函数。发现前面调用了一个奇妙的地址，打开 gdb 运行 x/s 进行分析，得到结果：%d %c %d，由此得知我们要输入的是 “int char int”，可以通过$0x7,0x10(%rsp)发现炸弹触发的条件是第一个数字大于 7，则第一个数字有 0 1 2 3 4 5 6 7 共 8 种可能，即本题是一道多解题。为方便，我只针对为 0 的情况进行解体。($rsp)+0x14 存放第三个数字 $eax 存放第二个字符。事实上，第二个字符存放的是 ASCII 码，数值为 105，为字母 i 。而第三个数字通过计算得到 531，即为所求。

3.4 阶段 4 的破解与分析

密码如下：6 6

破解过程：本题首先还是关注了一下函数名称前面的一串地址，用 x/s 命令可知 "%d %d"，可知本题的结果应该是两个 int 型的数，后续又有要求这两个数字大于 0。cmp $0x6,%eax 由这一行又可知 func4 的返回值应该为 0x6（6）。同时再向下看可以发现第二个参数被限制为 6，第一个参数应该∈[0,14]的范围。此时回头看 func4，发现是一个递归的程序。通过分析，得到第一个参数也为 6。

3.5 阶段 5 的破解与分析

密码如下：WQMVUW

破解过程：已经过了 4 个阶段，看到奇怪的地址先试一下吧。

```
0x402510 <array.3600>:  "maduiersnfotvbylSo you think you can stop the bomb with ct
rl-c, do you?"
0x402558:       "Curses, you've found the secret phase!"
(gdb)
```

不小心试出来隐藏关钥匙了.....意外之喜？

```
 syntax error in expression, near
gdb) x/s 0x4024c7
x4024c7:        "sabres"
gdb)
```

以及

```
callq  4013c4 <string_length>
cmp    $0x6,%eax
```

让我知道要输入长度为 6 的字符串。有了这些条件，我们再进行具体分析。

```
'maduiersnfotvbyl
```

似乎 这是解题的一个关键部分。观察这个

比较长的字符串，正好有 16 位，这就让人联想到可能“sabres”与这个表呈现一种对应的关系。翻译后，sabres 对应着 71d657，可能是在表示对应的 ASCII 值的末尾值。用 WQMVUW 尝试一下，果然过了。

-------以及原来这不是隐藏关密码啊，失望。

3.6 阶段 6 的破解与分析

密码如下：4 3 6 5 2 1

破解过程：做完题太久了，已经看不懂打的草稿了，遂放弃。

3.7 阶段 7 的破解与分析(隐藏阶段)

密码如下：35

破解过程：做完题太久了，已经看不懂打的草稿了，遂放弃。

第 4 章 总结

4.1 请总结本次实验的收获

本次实验是目前为止我最喜欢的实验，它让我以一种富有兴趣的方式熟悉了汇编语言的各种使用。在解题过程中，我熟悉了数组、链表、指针、跳转等各种汇编语言常见的模式。

4.2 请给出对本次实验内容的建议

感觉程序中有些内存地址，顺着查找下一个字符串会可以找到其他题目的内容……

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.