**深 圳 大 学 实 验 报 告**

**课程名称： 计算机系统(2)**

**实验项目名称： 逆向工程实验**

**学院： 计算机与软件学院**

**专业： 软件工程（腾班）**

**指导教师： 罗胜**

**报告人： 赵美玲 学号： 2023155025**

**实验时间： 2025年4月18日至5月5日**

**实验报告提交时间： 2025年5月5日**

**教务处制**

|  |
| --- |
| **一、 实验目标与要求：**   1. 理解程序（控制语句、函数、返回值、堆栈结构）是如何运行的 2. 掌握GDB调试工具和objdump反汇编工具 |
| **二、实验环境：**   1. 计算机（Intel CPU） 2. Linux64位操作系统（Ubuntu 17） 3. GDB调试工具 4. objdump反汇编工具 |
| **三、实验方法与步骤：**  本实验设计为一个黑客拆解二进制炸弹的游戏。我们仅给黑客（同学）提供一个二进制可执行文件bomb\_64和主函数所在的源程序bomb\_64.c，不提供每个关卡的源代码。程序运行中有6个关卡（6个phase），每个关卡需要用户输入正确的字符串或数字才能通关，否则会引爆炸弹（打印出一条错误信息，并导致评分下降）！  要求同学运用**GDB调试工具和objdump反汇编工具**，通过分析汇编代码**，**找到在每个phase程序段中，引导程序跳转到“explode\_bomb”程序段的地方，并分析其成功跳转的条件，以此为突破口寻找应该在命令行输入何种字符串来通关。  本实验需解决Phase\_1(**15分**)、Phase\_2(**15分**)、Phase\_3(**15分**)、Phase\_4(**15分**)、Phase\_5(**15分**)、Phase\_6(**10分**)。通过**截图+文字**的形式把实验过程写在实验报告上，最后并撰写**实验结论与心得(15分**)。 |
| 1. **实验过程及内容：** 2. 对二进制文件进行反汇编，将结果保存到1.txt。   2866ea9b25e7634104e07704e89d135   1. 打开txt文件，观察每个关卡的位置。   371499a5b68858dd4cf289f79fa86c0   1. 开始闯关 2. 第一关   ddc88dc8dad73976b08f6c8c2c14e0e  通过逐条解析汇编代码意义，可知，程序会判断输入内容和储存在0x401af8位置的值是否相同，若相同则通关，否则引爆炸弹。 进入gdb调试，查看该地址内容，得知字符串内容。 9913ecebaf70812abae14afbf2e8fe7  闯关时输入字符串即可。   1. 第二关 b7453bebc2d66cfb1681b952f7ad7e8   分析汇编代码发现，这段函数是对输入的六个数字一依次进行处理和比较，观察到跳出循环且不爆炸的地址为400ee0，再观察跳转条件为`%r12d` 寄存器的值不为0，而`%r12d`寄存器存储的值为数字的累加结果。  另外每次循环都会判断[rbp]和[rbp+0xc]的值是否相等，又rbp最初存储的是第一个数的地址，那么循环判断的即是前三个数字和后三个数字是否相等。  因此，总的来说，这个循环从第一个数字到第三个数字，并且判断是否满足两个条件，一个是当前数字与当前数字后的 第三个数字是否相等，若不相等则引爆炸弹；另外一个是会循环的数字进行累加，并判断是否出现累加结果为0的情况，若出现则引爆炸弹。  666666满足以上两个条件，注意数字之间要有空格。   1. 第三关   b63136f30b909381ea9764937a2822d  分析代码，输入两个数a,b。其中a的值影响跳转，跳转后存入值到寄存器中判断是否和b相等，可看出共有八组数据可以过关，其中我们选择地址0x401b60进行测试，gdb查询后如下  93a0420afd3a601df35988cac4cb194    由此可得，该组数据为0，535   1. 第四关   其中func4是递归函数，它接受一个整数参数，返回一个整数结果。 而函数的功能是计算一个特定的递归表达式并返回计算结果，通过分析得，该函数是求斐波那契数列第n项的递归函数。  Phase4函数作用是解析用户输入的值，并调用递归函数func4，最后检查结果是否为55，如果是则通关，错误则爆炸，用常识可知，斐波那契数列第9项为55，所以该关答案为9。   1. 第五关 分析函数可知有个数组实现跳转功能类似k = next[k]，查看得   cc99635dcef701007f5080adcdf4958  分析函数得，该函数共跳转12次，第二个输入值应该等于每次跳转的目标累加，所以答案应该为7 93。   1. 第六关   分析代码可知，最后需要edx和rax的值相等即可通关，那么在600~679范围内的数都符合要求，随意选择即可。 |
| **五、实验结论：**  最后运行结果如下，可知解题正确，通关  a37fa4213471b7e5fc3aa70afb4dfbe |
| **六、心得体会：**  最开始没有打开实验报告的模版，没看到说有可能没有权限运行文件，所以一直出错  9913ecebaf70812abae14afbf2e8fe7  最后在网上找到解决方法后还沾沾自喜，结果最后发现实验报告里写清楚了，下次做实验之前还是要好好看看模版。  本次实验主要运用了反汇编函数，将正常代码转为汇编代码分析程序如何运行，更有可读性吧，每一步都可以分析其下一步怎么走，理解了递归，堆栈这些函数在汇编层面上是如何运行的。 |

|  |
| --- |
| 指导教师批阅意见：  成绩评定：  指导教师签字：罗胜  2025年 5月5 日 |
| 备注： |