|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 课程编号 1502760001-07  题目类型 实验3 | |  |  |  | | --- | --- | --- | | **得分** | **教师签名** | **批改日期** | |  | 冯禹洪 |  | |

**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： 计算机与软件学院所有专业**

**指导教师： 冯禹洪**

**报告人： 学号： 班级：**

**实验时间： 年 月 日至 月 日**

**实验报告提交时间： 年 月 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**)。 |
| **四、实验过程及内容：**  **以下是某助教的实验过程以及实验思路，仅供同学们学习参考。请同学们学习后删除以下教程内容（包括此段红字），并基于自己的Linux用户（用户名为学生名称加学号）进行实验，认真记录自己的实验过程以及实验思路，并撰写实验结论与心得。**  注1：  当前用户可能对bomb\_64文件没有执行权限，建议先用ls查看文件权限，若没有执行权限，请用chmod +x bomb命令增加当前用户对bomb文件的执行权限。  注2：  若用命令./bomb执行该文件提示no such file时，请先用 su szu 切换到szu账户，然后输入命令sudo apt-get install lib32z1，等待下载安装完毕即可。   * 第一关  1. 首先对bomb文件进行反汇编，并将结果输出到1.txt。      1. 为方便查阅汇编代码，在图形化界面中将txt结果用文本编辑器打开。 2. 已知本实验共有6个关卡，下面先开始第一关，打开txt，定位到phase\_1函数处。      1. 【主要思路】 通过阅读汇编代码可知，里面有一个strings\_not\_equal函数，故我们推测它进行字符串比较。且比较后的结果，有je跳转指令，可能是相等则通关。故程序自身应有一个字符串，经代码检测，关键点在0x401af8。 故下面进入gdb调试，然后查看0x401af8该地址对应的数据。      1. 由上图可知，第一关的答案是“Science isn’t about why, it’s about why not?”。 2. 对答案进行测试。成功过关！   上面一段请在最终的实验报告中，请删除，包括此句话。剩余关卡，请同学们按以上步骤完成。 |
| **五、实验结论：** |
| **六、心得体会：** |
| 指导教师批阅意见：  成绩评定：  指导教师签字：冯禹洪  2024年 月 日 |
| 备注： |