**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： 黄志鹏 学号：2017303008 班级： 计科一班**

**实验时间： 2020 年 4 月 20 日至 5 月 6 日**

**实验报告提交时间： 2020 年 5 月 6 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：**  第一关：    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，关键点在0x401af8。查询0x401af8中的字符串。    输入字符串，答案正确，通关。    第二关：    通过阅读汇编代码可知，里面有一个read\_six\_numbers函数，故推测它是读入6个数字，分析下面代码：    （1）程序先读取6个数字，rbp作为开始指针，rbp+12作为终点，共循环3次，每次判断M[rbg]与M[rbg+12]是否相等，不相等则爆炸，且每次比较间隔四个字节，而int刚好为4个字节，所以推测程序判断输入6个数字序列第i个是否等于i+3，i=0，1，2。  （2）同时注意到，r12d累计了i=0，1，2的值，若为零则爆炸。  （3）输入数组应满足a[i]=a[i+3]且a[1]+a[2]+a[3]!=0 ，i=1，2，3  输入1 2 3 1 2 3 ，答案正确。    第三关：      通过阅读汇编代码可知，里面有一个\_\_isoc99\_sscanf@plt函数，故先查看0x401ebe 中存放着什么字符串，结果可知输入为两个整数。又因为scanf调用前，传入第三第四个参数了，他们存在rsp+8和rsp+12位置，故应该是int型。    根据可知，输入的第一个数字不能大于7，否则爆炸。  接下来有一个变址跳转，通过gdb查看跳转位置：    跳转位置分别如下所示：    可以知道这是个switch语句，通过输入的第一个数字来进行相应的跳转，假设输入的第一个数字为0，则后面的代码则是将第2个输入的数字与0x217进行比较，相等就通过，而0x217是535的16进制，以此类推。  因此输入以上任一答案 0 535，答案正确，通关。    第四关：    通过阅读汇编代码可知，里面有一个\_\_isoc99\_sscanf@plt函数，故先查看0x401ec1 中存放着什么字符串，结果可知输入为1个整数。    随后指令比较整数是否大于零，若不大于零则爆炸    然后比较55与func4返回值是否相等，不等则爆炸，由此可知主要问题再func4上。    通过分析代码可知，此函数是一个递归函数。且为fun4(x) = fun4(x-1)+fun4(x-2)，由此可解得参数x为9。    第五关：    通过阅读汇编代码可知，里面有一个\_\_isoc99\_sscanf@plt函数，故先查看0x401ebe 中存放着什么字符串，结果可知输入为2个整数。    在处理第一个数字时只保留后四位，即mod16，且不能等于15。接下来有一个循环，跳出循环的条件为eax中的值为15，且要求循环退出时edx要为12而eax=M（0x401ba0+rax\*4)，4是因为int有四个字节，由此可看出该循环为数组跳转，而且跳转次数应为12此。同时由每次ecx+=eax可知，累加和ecx应该等于第二个输入的整数。  关键在于0x401ba0及其后面数组存放着什么，所以需先查找0x401ba0处数组。    满足循环次数edx=12时，输入的第一个数字mod 16后必须为7，从7下标开始，分别累加11+13+9+4+8+0+10+1+2+14+6+15 = 93， 输入第二个数字必须为93。    第六关：    查询strtol@plt的用法是将输入的字符串，转化为long型整数，然后保存在0x602780处，然后再传入fun6函数。返回值rax经过三次寻址，再与输入的元素，相等即可拆解炸弹。  随便输入一个数字，查看断点0x40110e的rax。    此时可知输入600可拆除炸弹。  而fun6函数里面含有大量的跳转，较难分析，故不再深入。  至此，所有炸弹都拆除。 |
| 1. **实验结论：**   利用GDB调试工具和objdump反汇编工具，通过分析汇编代码，成功拆除6个炸弹，如图所示： |
| **六、心得体会：**  1. 通过本次实验，我简单掌握了GDB调试工具和objdump反汇编工具的，能够阅读并分析一些简单的汇编代码。  2. 对程序控制语句、函数、返回值、堆栈结构是如何运行的有了更深的理解。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：冯禹洪  2020年 月 日 |
| 备注： |
|  |