计算机科学与技术学院 计算机系统原理 课程实验报告

|  |  |  |
| --- | --- | --- |
| 实验题目：二进制炸弹拆除 | | 学号：201805130155 |
| 班级：18级3班 | 姓名：赵雨晗 | |
| Email：[408639122@qq.com](mailto:408639122@qq.com) | | |
| 实验目的：  (1) 熟悉MIPS指令集；  (2) 根据反汇编程序可以分析程序的功能和执行流程；  (3) 熟悉GDB调试工具，帮助程序理解。 | | |
| 实验软件和硬件环境：  Intel®Core™i7-8750H @ 2.20GHz  Wsl Debian + qemu 虚拟机  Mipsel 小端机 | | |
| 实验原理和方法：  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MIPS二进制可执行文件bomb，不提供源代码（提供汇编代码帮助理解）。 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）！ 要求同学运用GDB 调试工具，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。 | | |
| 实验步骤：（不要求罗列完整源代码）   1. bomb\_1   反汇编之后，可以看到进入了文本比较函数，进入函数后找到内存地址发现指向了 “Let’s begin now!”字符串，输入后进入第二个炸弹。   1. bomb\_2   反汇编phase\_2    首先发现需要读入六个数字，跟随函数进行单步调试，首先发现第一个数字必须是1。之后会进入次数为6的循环    继续理解汇编代码，找到学号和输入的数字在内存中所在的位置    可以发现这里是从后向前每次取出一位乘号进行累乘，并与输入的数字进行比较，然后成功发现规律，bomb\_2拆除。   1. bomb\_3   依然是对第三个炸弹进行反汇编，然后使用上面的技巧，首先找到输入的数据在内存中所储存的位置，发现取出了输入的第一个数字，并且判断必须为个位数，然后观察炸弹3汇编代码的结构，发现有很多类似的结构，而且一共有10个，猜测是根据输入数字进入switch语句，进入语句后发现会拿出来第三个数字相乘，根据自己学号的最后一位找到自己学号的倍数，进入第二个分支，并跟随调试找到输入的第二个数字的值。炸弹三拆除    对应学号炸弹三答案为 2 b 151   1. bomb\_4   第四个实验为递归函数，直接查看原汇编代码可以较清楚的看懂整个递归过程，可以学号根据学好单双分别递归终点为 8和 13，递归发现fun7为求Fibonacci序列，8为第5项，输入5后，炸弹拆除。   1. bomb\_5   第五个实验是字符串加密，首先观察输入函数发现需要输入一个字符串，观察汇编代码发现字符串长度需要为6    单步调试找到循环变量和输入字符串所存在的位置，发现对于输入的每个字符进行了取后四位的操作    通过后面比对字符串函数猜测是根据我们输入的字符串加密    找到比对字符串的处理发现用到了汇编代码最后的array.3607    继续读代码发现原理是利用输入数字的二进制后四位对array.3607进行映射，最后需要得到giants，按照array.3607进行查找，找到一种可行的答案是opekma。  6.bomb\_6  首先看输入，需要输入六个数字，跟随gdb进行单步调试，发现使用了6个名为node的结构体，在汇编代码中查看node变量，发现其中有键值和地址值，猜测其为链表结构。    跟随gdb进行调试，有了上面的经验，只需要找到循环变量的位置，循环的汇编代码就变得非常容易理解，第一个循坏是判断输入数字合法，第二个循环是取出输入数字所对应的node，第三个循环把取出node首尾相连，连接成链表，第四个循环判断链表的顺序应该是从头到尾根据学号递增或递减，根据node值找到答案。  学号末尾为奇数答案为 4 2 6 3 1 5，此题通过。  7.secret\_phase 在第四个炸弹中，scanf函数中的参数为”%d %s”，所以判断应该从第四个实验中进入此炸弹，观察汇编代码中的字符串，发现还有一个austinpowers没有用到，尝试后成功进入secret\_phase，发现需要输入一串字符串并使用了stroll这个函数将输入的数字转换为二进制。  发现进入一个名为fun7的函数，函数的传入变量是输入的数字和一个地址值，跟随传入的地址值找到使用的数组n1，n21，n22···，根据变量名称猜测数组为二叉树，又根据键值，可以发现该树为二叉搜索树，所以只需要简单的读fun7函数的代码，就可以发现fun7为递归函数，很容易猜出其为dfs函数    回到secret\_phase发现通过炸弹的条件是fun7函数返回值为7，又因为上面将输入字符串转化为了二进制，读代码很容易得到，输入的字符串就是树上的路径，0为进入左儿子，1为进入右儿子，根据树的形状，得到答案。 | | |
| 结论分析与体会：  拆炸弹是很有意思的事情，从对汇编代码一头雾水到努力读代码逐渐适应并总结出技巧的过程是十分有趣的，在读程序汇编代码的过程中，我们也知道了我们写的C++代码，是以什么思路来编译的，这为以后学习编译原理也打下了基础，希望能够多一点这样的实验，既提高了动手能力，也使实验变得不再那样枯燥乏味。 | | |