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：缓冲区溢出 | | 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.了解缓冲区溢出的原理；  2.了解程序的栈结构、函数调用以及参数传递的规则；  3.了解MIPS指令是如何编码的；  4.加深对debug工具（如GDB）的了解。 | | |
| 实验软件和硬件环境：  龙芯mipsel 小端 | | |
| 实验原理和方法：  本实验利用了缓冲区溢出的原理，需要你来构造特定的字符串，这些字符串将被加载到缓冲区中，来完成溢出的操作。在实验中，你将要完成的任务是：对栈中数据进行修改，以此达成跳转到指定函数的目的。该实验将帮助你了解MIPS架构下栈中的数据是怎么组织的，程序跳转的时候栈和寄存器是如何配合的。 | | |
| 实验步骤：（不要求罗列完整源代码）   1. 首先使用GDB工具查看attack函数的反汇编代码。 2. 随机构造一组数据，找到缓冲区的大小与所在的内存。 3. 计算出所需要的数列，找到函数返回地址，构造数列利用缓冲区溢出覆盖目的地址，完成实验。 | | |
| 结论分析与体会：   1. 深刻理解了程序执行过程中的存储结构以及程序堆区栈区的存储策略。 2. 更深一步了解汇编代码，理解在程序执行过程中各个寄存器的作用。 3. 对程序的安全性有了更深一步的理解。 | | |