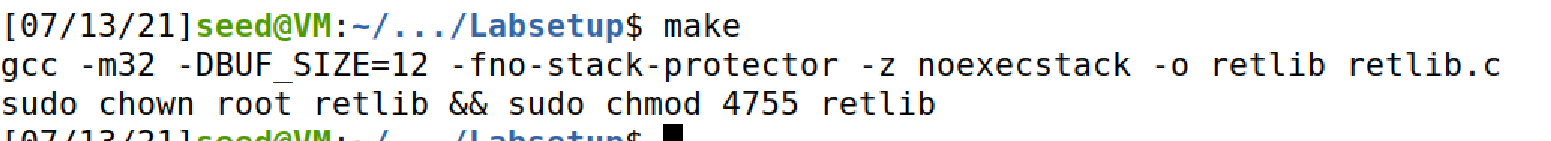
Return-to-libc Attack Lab

姓名：黄禧敏

学号：57119109

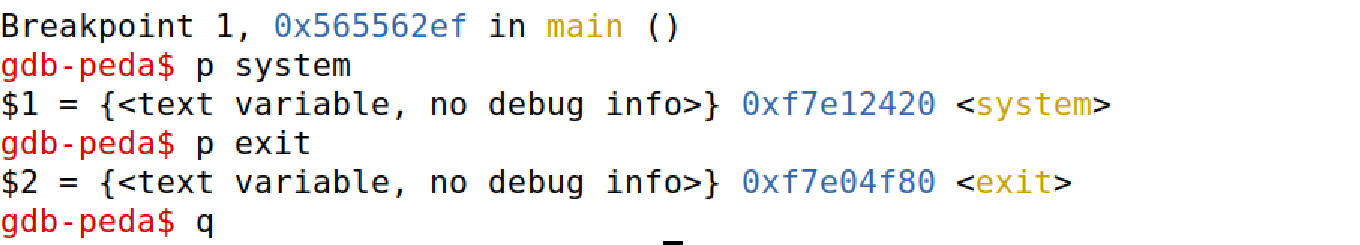
日期：2021/7/13



**Task 1:**

Finding out the Addresses of libc Functions

通过gdb调试获得system地址



**Task 2:**

Putting the shell string in the memory

打印/bin/sh作为环境变量地址，注意打印的程序名要和retlib一样长;

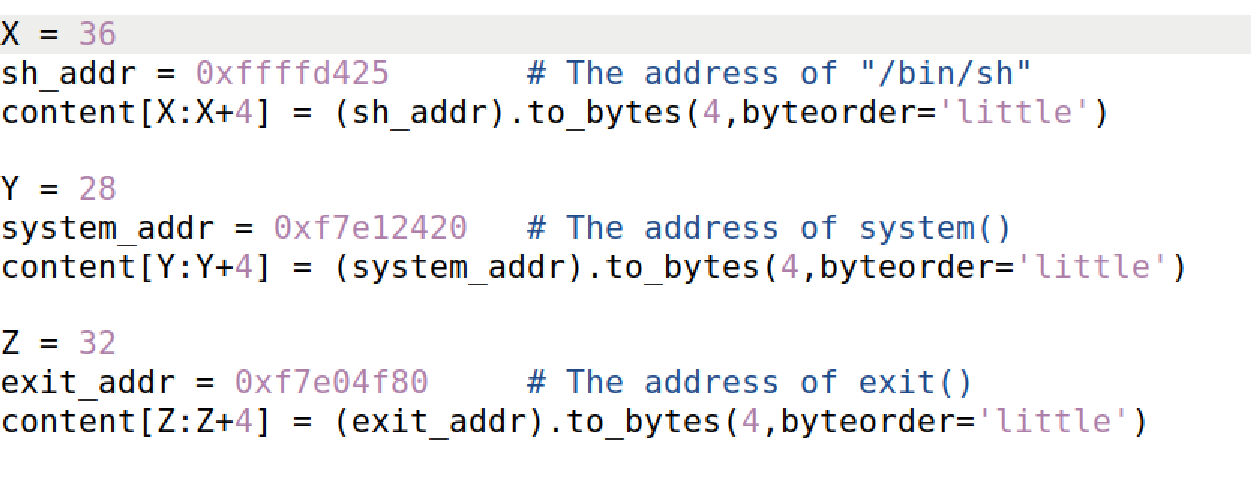


**Task 3:**

Launching the Attack

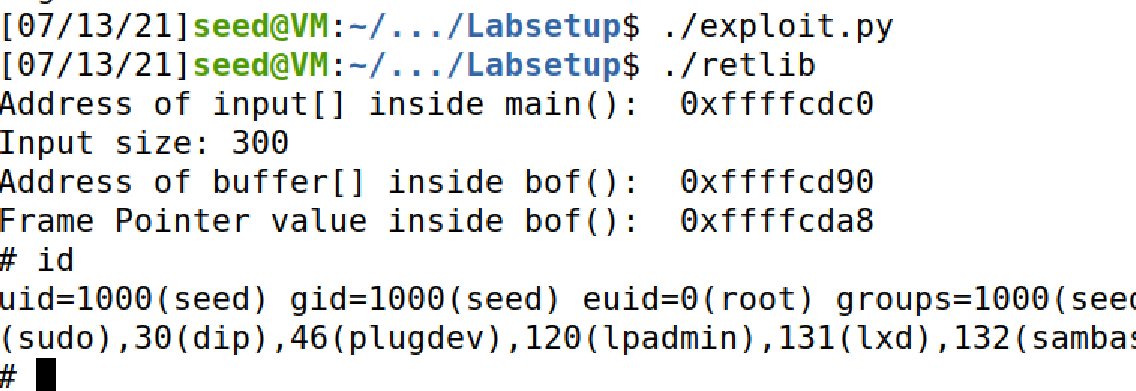
填写address，X,Y,Z

X为参数地址，Y为被攻击程序返回地址，Z为攻击函数返回地址；



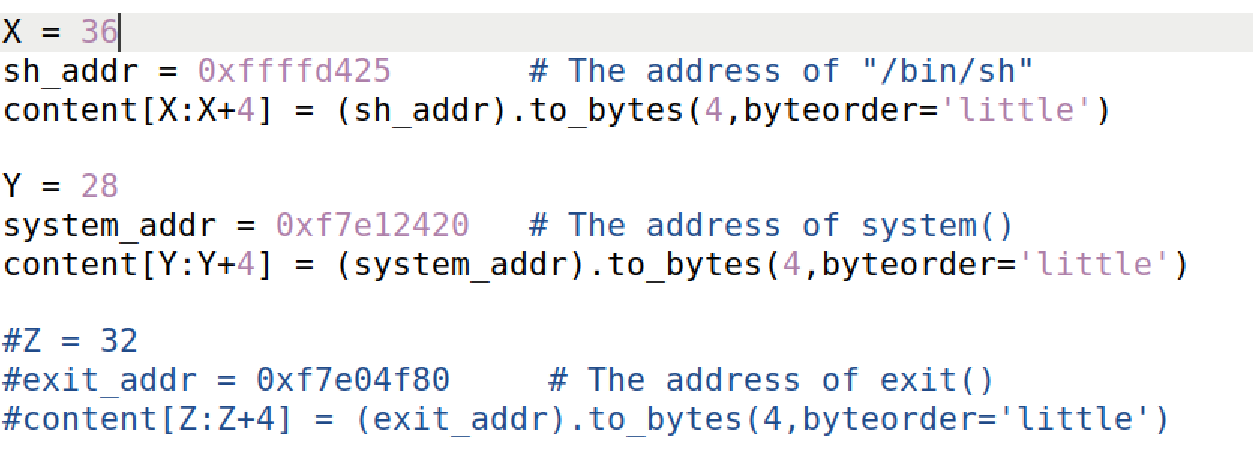
攻击结果：

得到root shell;



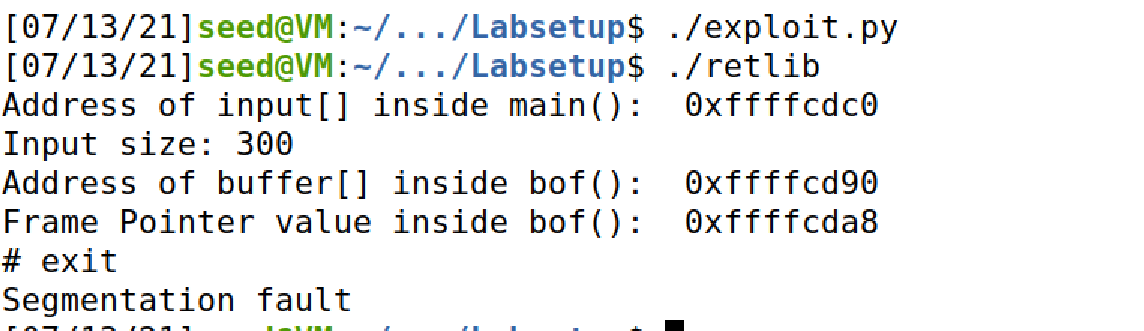
**测试1：**

去掉exit();



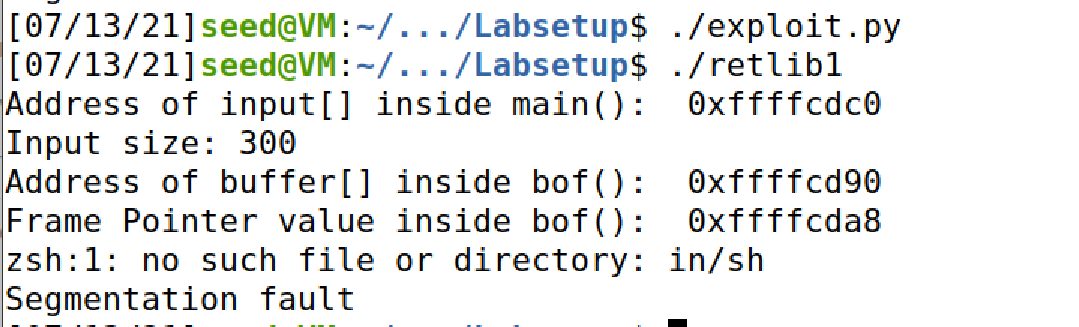
测试结果：

攻击成功，但是在退出时由于没有正确的返回地址，因此会出现segmentfault。



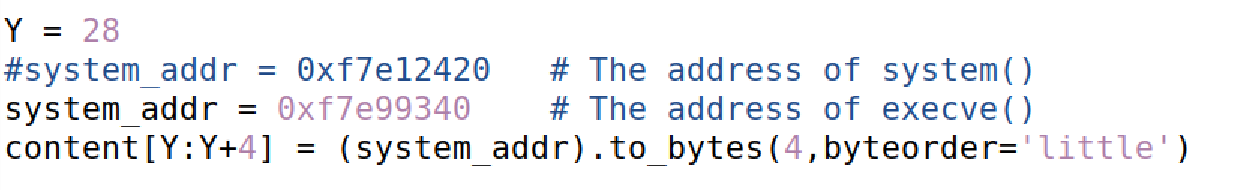
**测试2：**

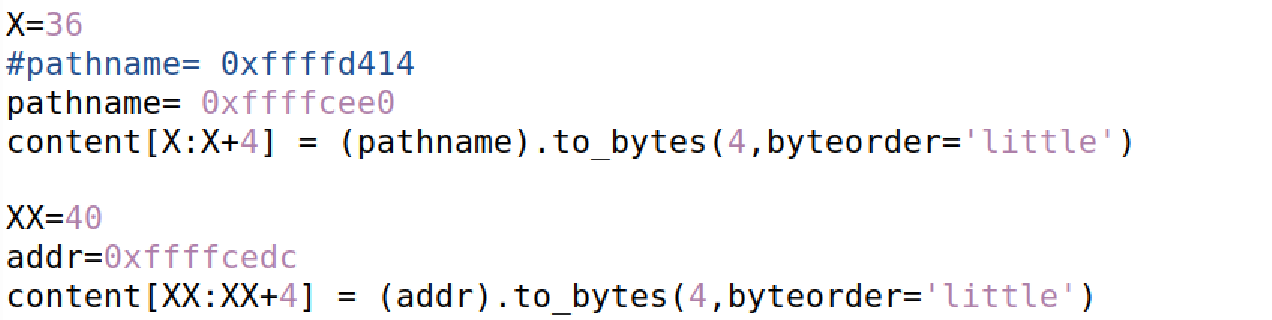
更改retlib可执行文件名长度,由于更改了环境变量中system的地址，因此无法攻击成功。

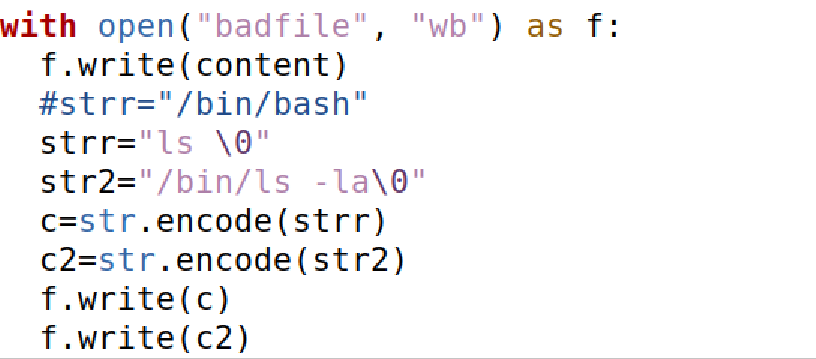


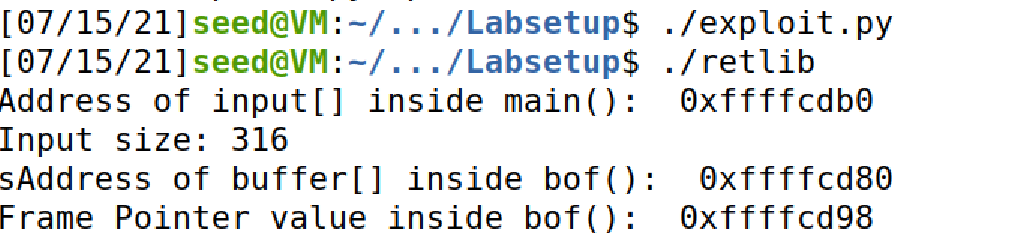
Task4

将参数放置在input文件中，返回input地址查找，但不明原因攻击未成功；









System调用/bin/ls -la

