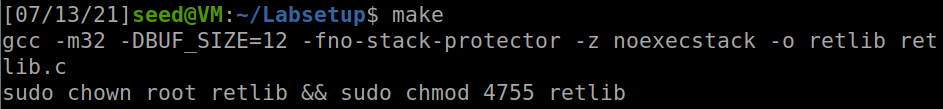
**操作系统实验三**

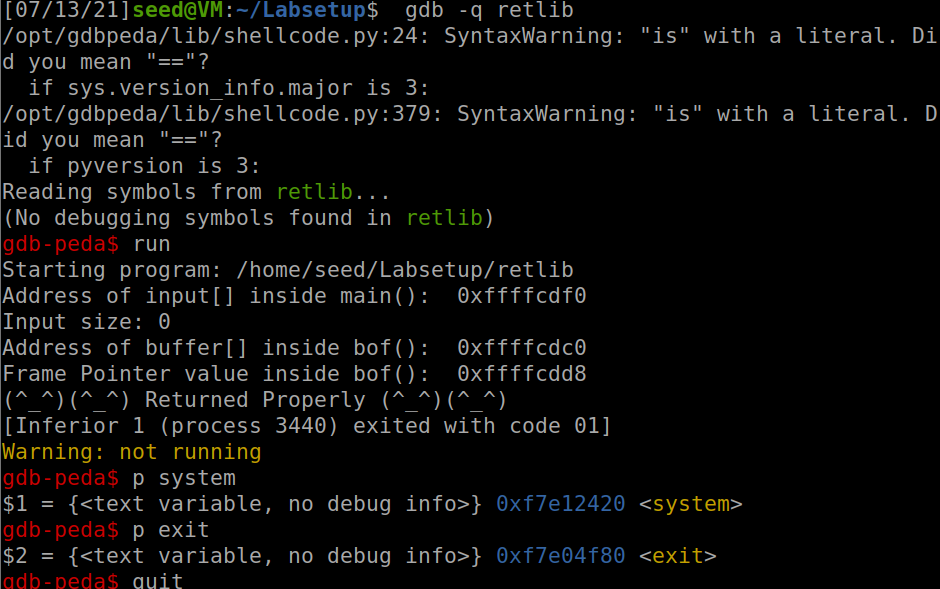
高昂 57119123

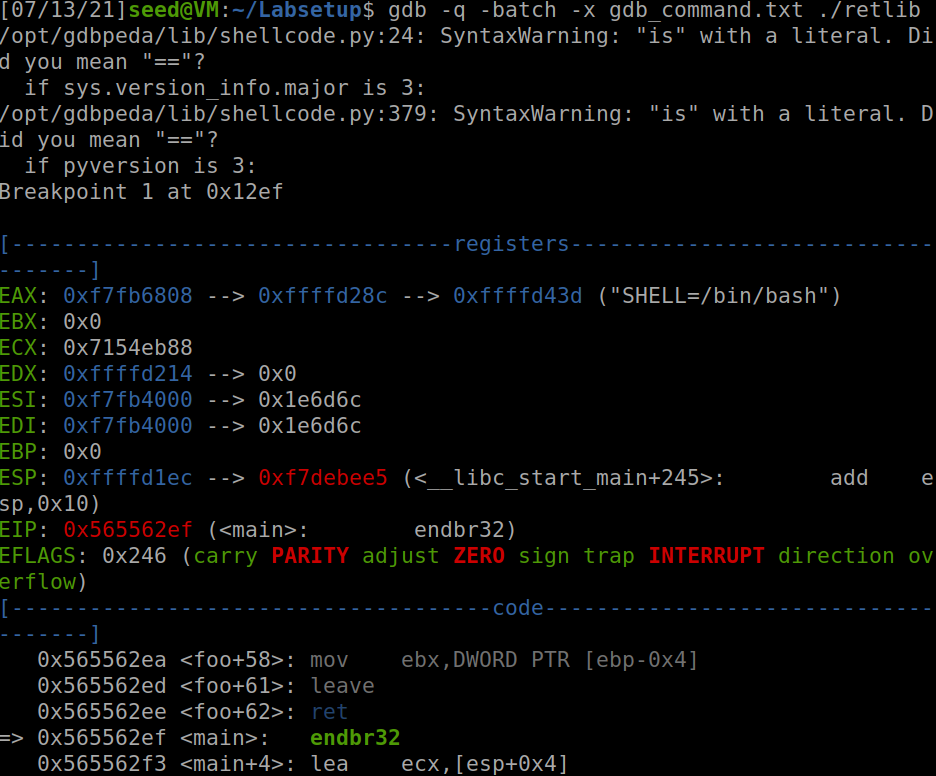
Task 1

使用 make编译程序



通过 gdb 调试获得 system 和 exit 函数地址

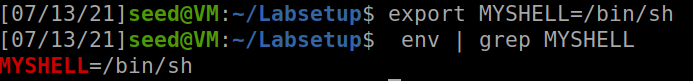




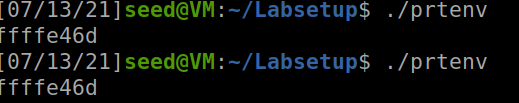
得到system（）和exit（）的地址:

Task 2

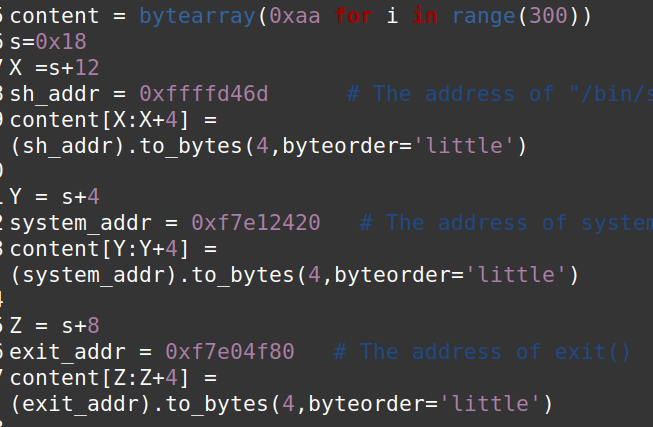
添加环境变量

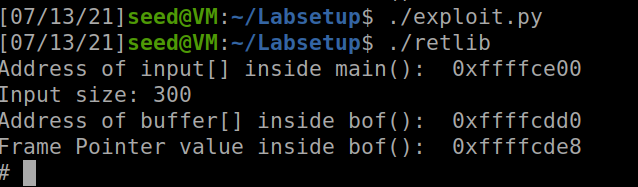


得到”/bin/sh”的地址:



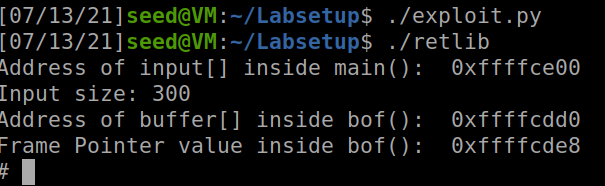
Task 3





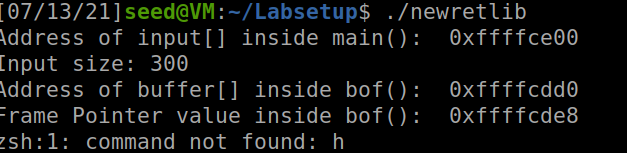
攻击成功

Attack variation 1



成功

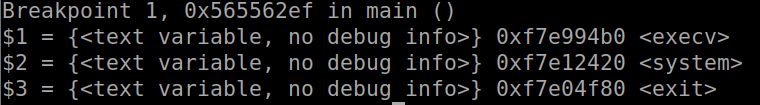
Attack variation 2：



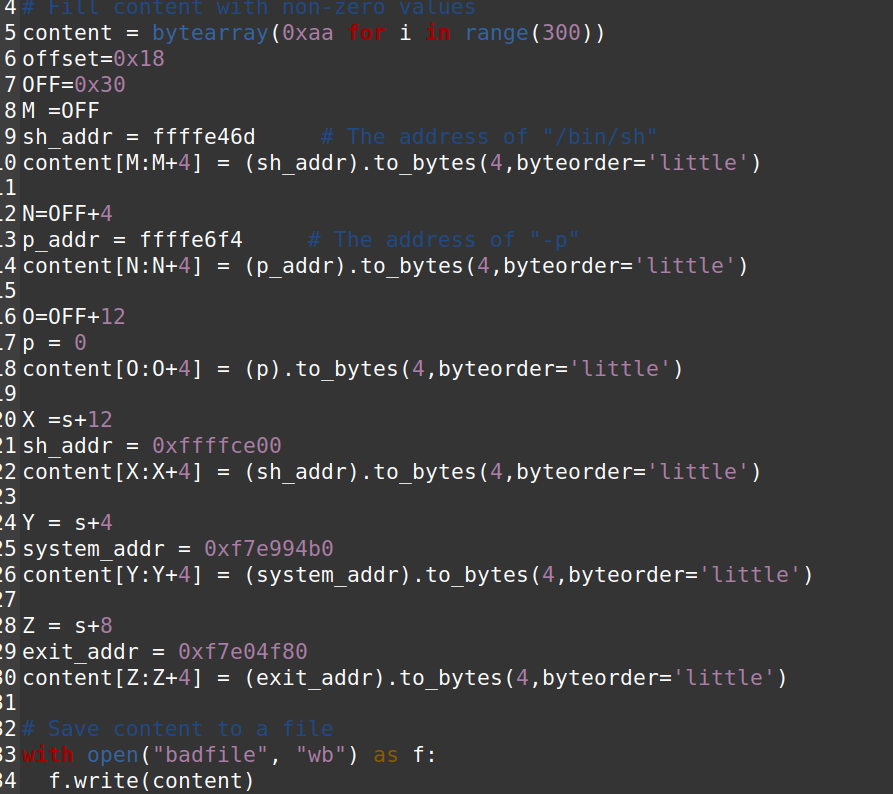
MYSHELL 的地址已经改变，攻击失败

Task 4

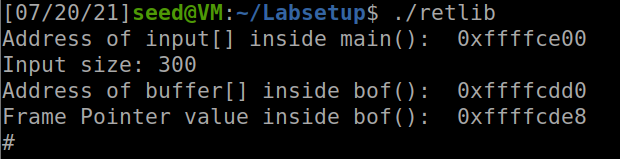
获得程序对应的地址



攻击代码：：



编译后进行攻击



攻击成功！