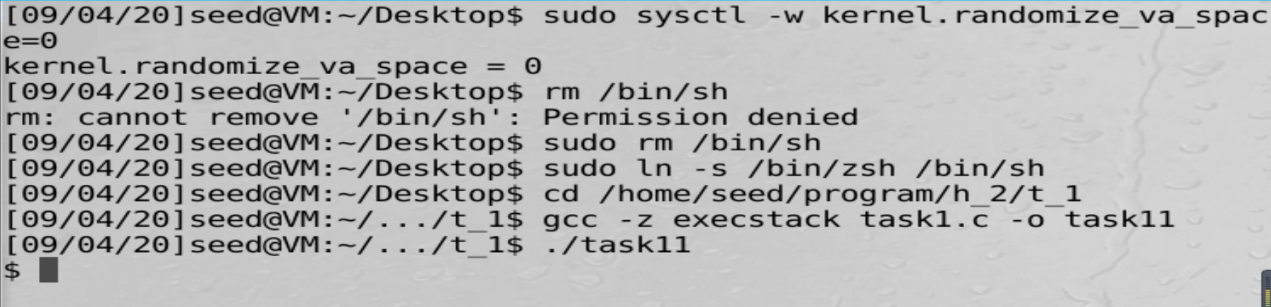
实验报告

Task1

过程



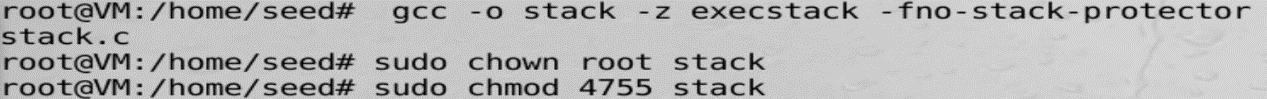
可以观察到

Task2

关闭countermeasures



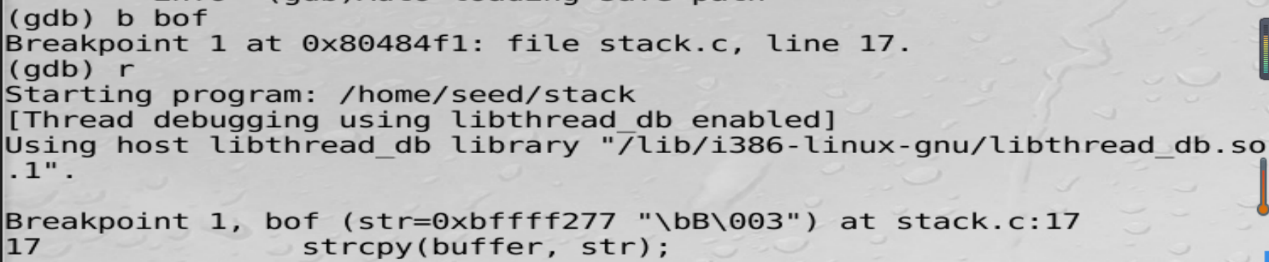
编译stack.c文件，关闭栈保护并设置栈可行



建立badfile文件，并用gdb对stack进行调试



在bof函数处设置断点，并运行程序



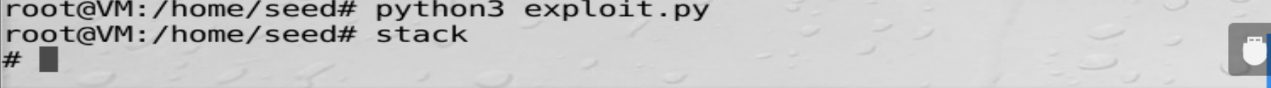
查看ebp和buffer的地址



得到两个地址相差32个字节，所以offset设置为36，ret地址设置为ebp地址

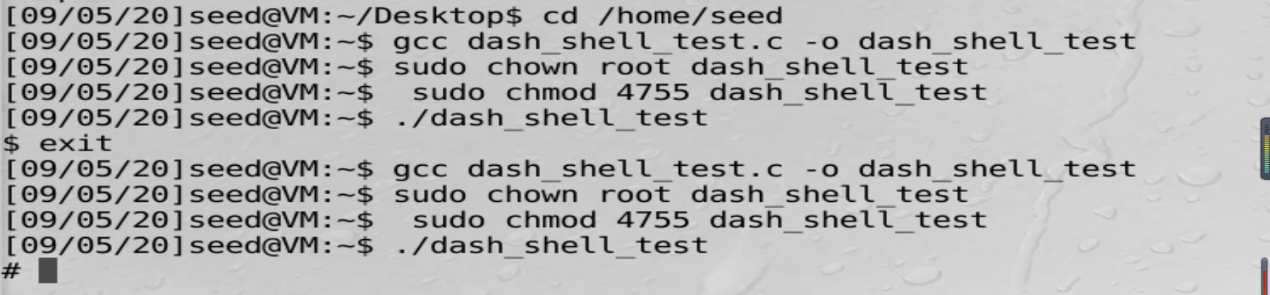


运行stack，获得root权限

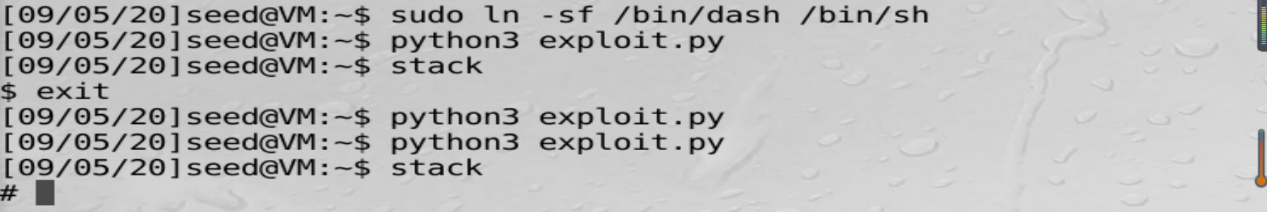


Task3

复制代码并编译执行，发现注释掉之后无法获得root权限，解除注释后可以获得root权限

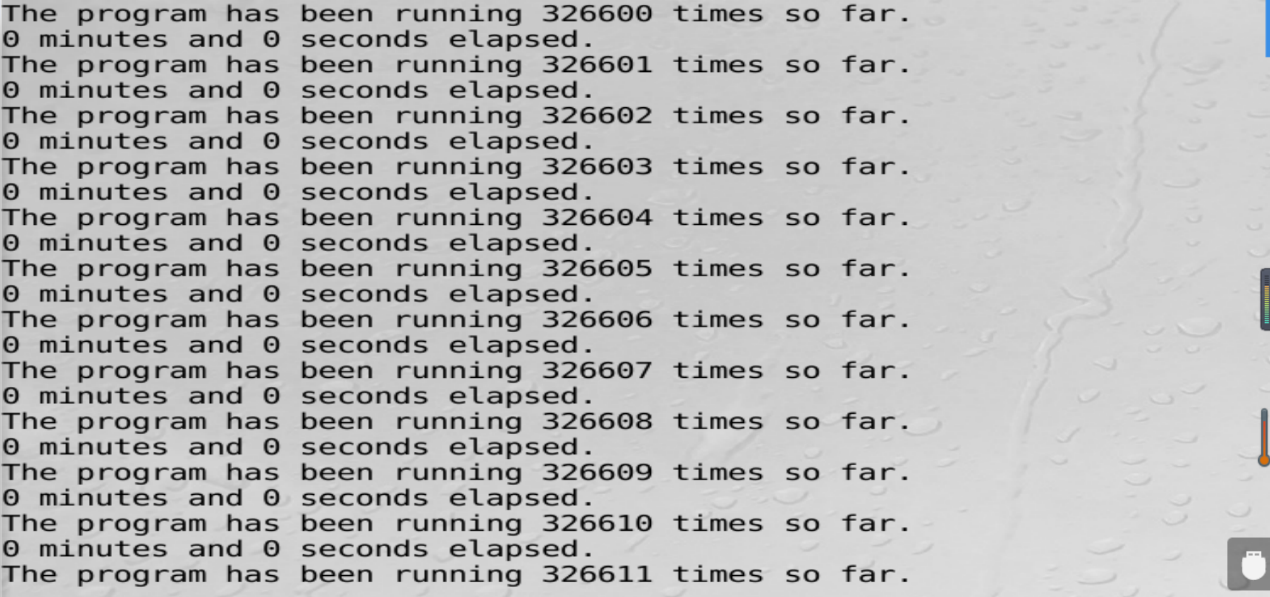


比较更改前后的task2中的攻击，可以看出添加前无法获得root权限，添加后可以获得



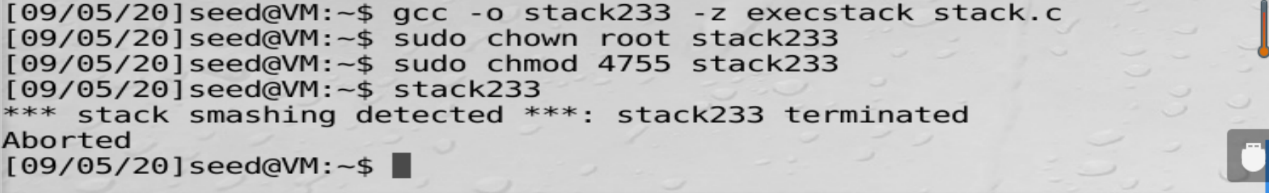
Task4

暴力破解



Task5

程序异常退出



Task6

栈不可执行，出现段错误

