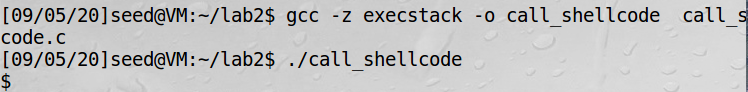
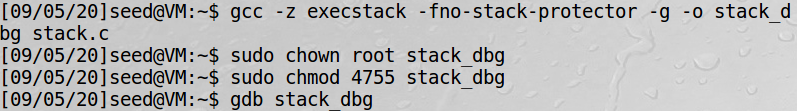
**学号57118127 姓名 孙博**

**Task1，2**

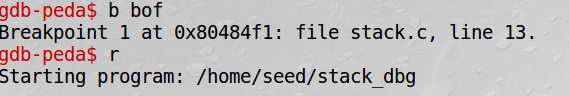
创建并编译call\_shellcode.c程序，运行结果如下

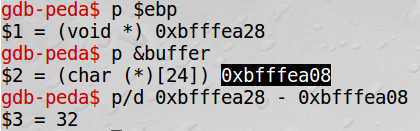


创建并编译stack.c, 通过代码可以知道，程序会读取一个名为“badfile”的文件，并将文件内容装入“buffer”，编译该程序，并设置SET-UID程序。

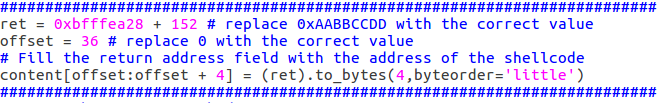


通过gdb中在bof处设置断点找buffer的地址

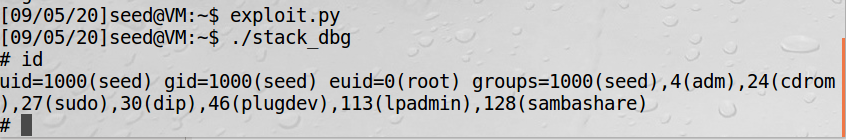




在exploit.py中输入buffer位置和偏移量

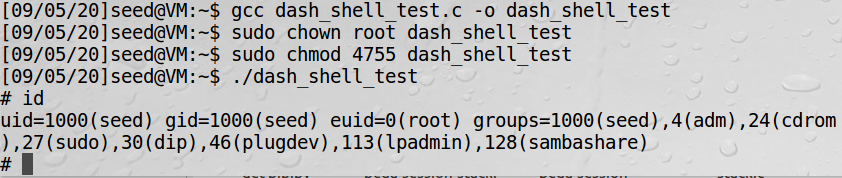


给exploit.py权限 再运行exploit.py和stack\_dbg,获得root权限

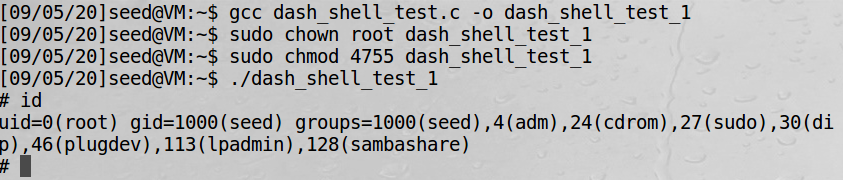


**Task3**

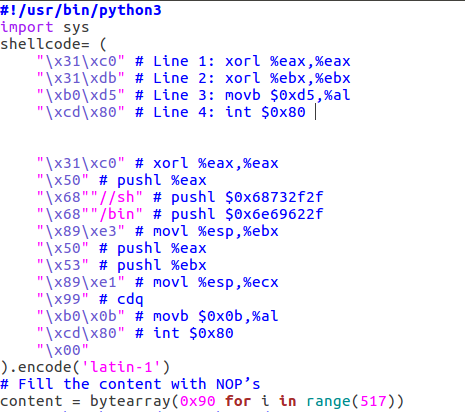
我们首先注释掉行A，并以Set-UID程序的形式运行程序，所有者是root，发现获得了管理员权限

****

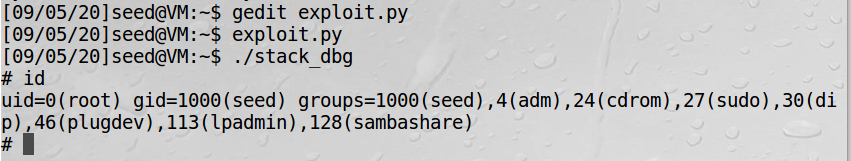
取消掉注释，并再次运行程序，发现仍然获得了root权限，但uid为0



在exploit.py中加入该段代码后

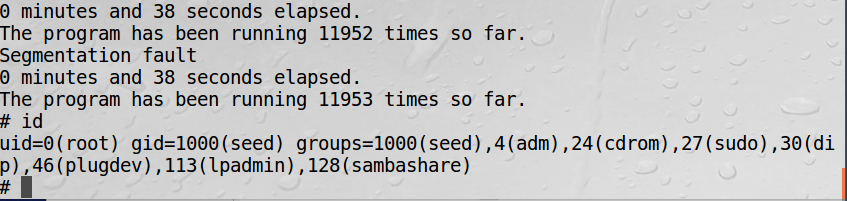


运行后获得root权限，但调用系统调用后uid变为0



**Task4**

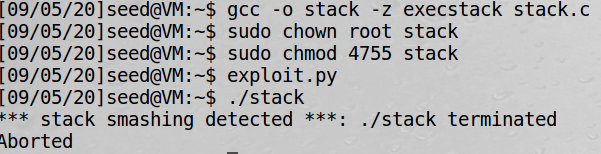
开启随机化 然后输入命令，有概率找到badfile地址而运行stack成功



如图，在11953次时运行成功

**Task5**

使用栈保护选项之后运行程序，发现被栈保护终止



**Task6**

开启堆栈不可执行之后，不能获得管理员权限

