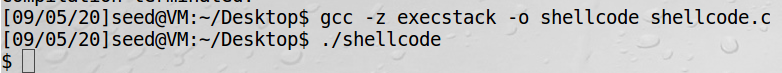
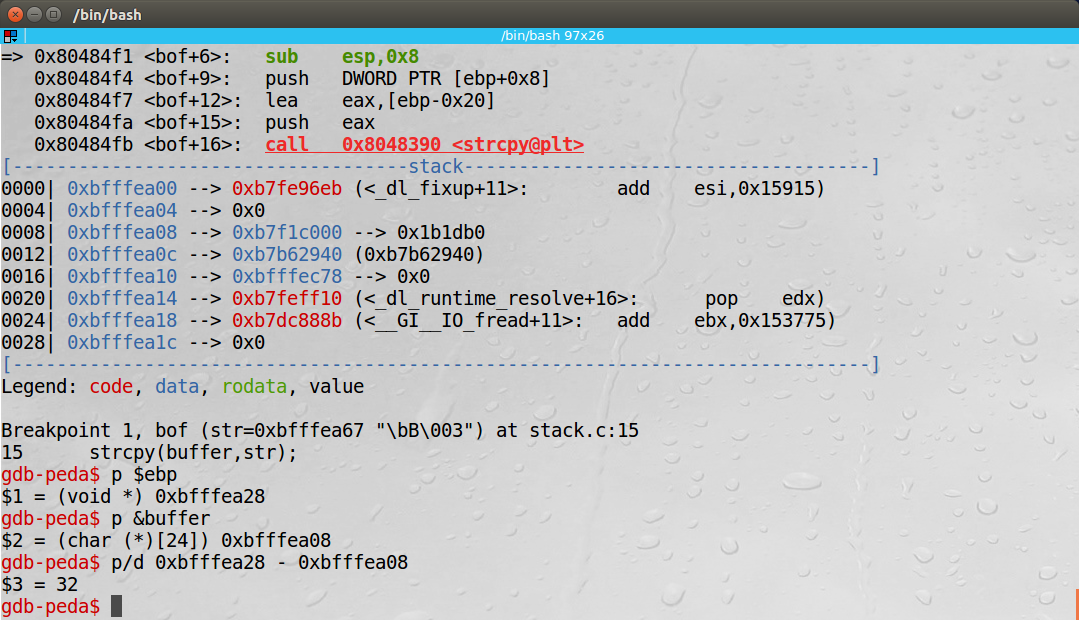
**Task 1**

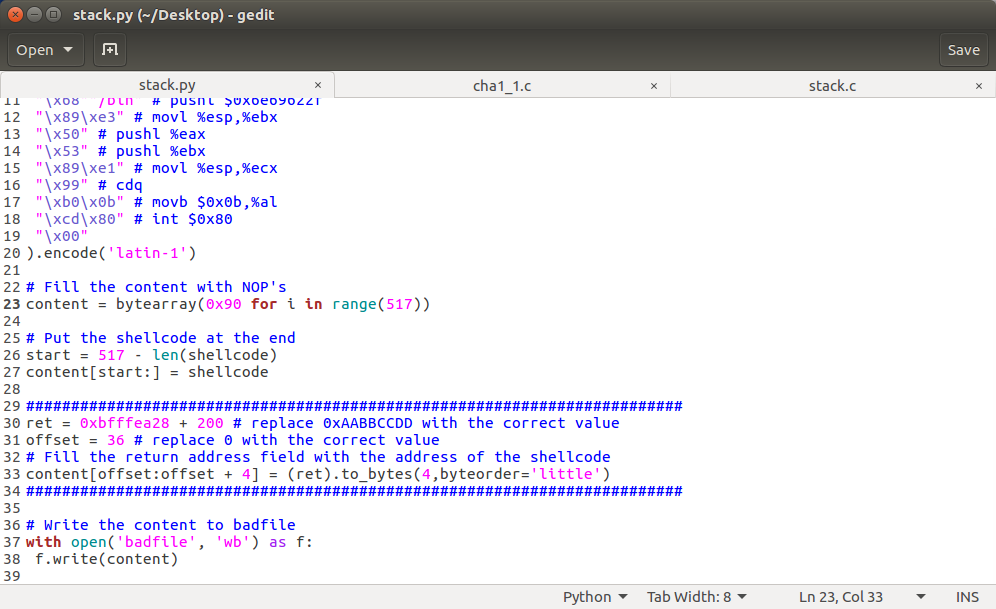


Shellcode启动了一个shell，可以在其中输入命令行。

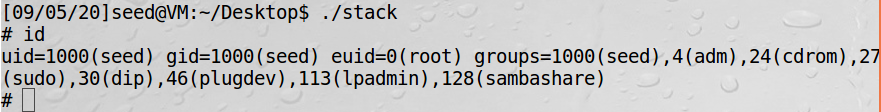
**Task 2**



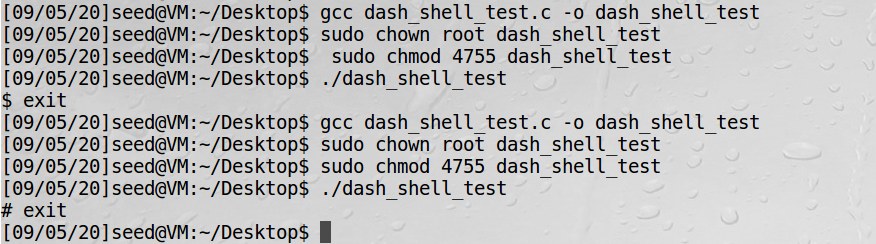
通过gdb，获得ebp位置为0xbfffea28，ebp和buffer地址之差为32，python程序内容输入如下：



运行stack程序，成功获得euid为root的shell

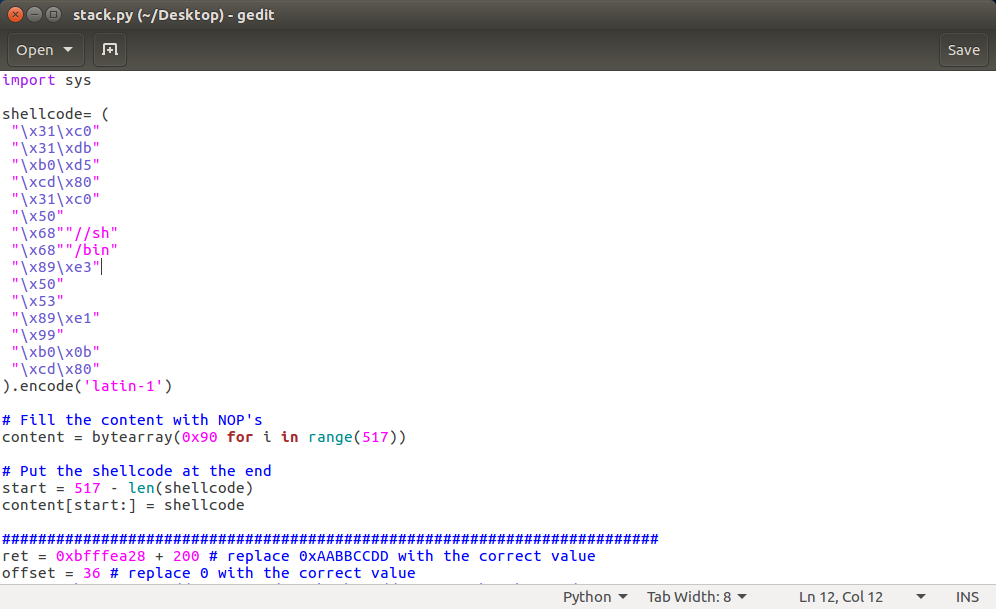


**Task 3**

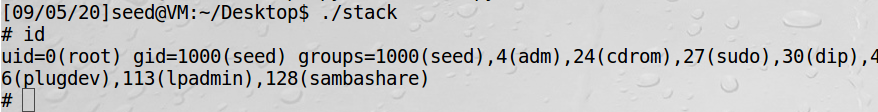


Setuid(0)可以改变uid为root，从而dash也不会进行反制。

Shellcode改变为如下：



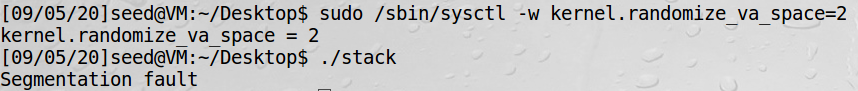
运行stack：

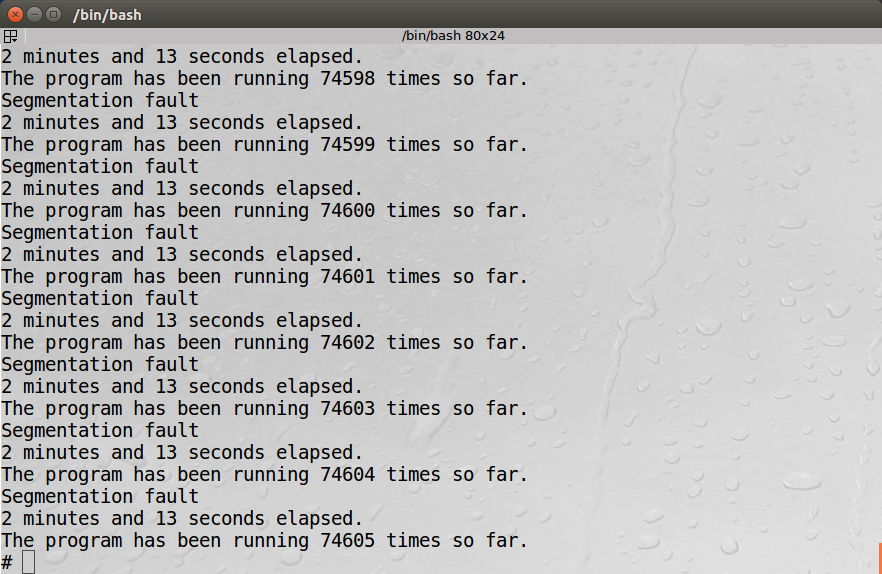


获得了uid=0的shell

**Task 4**

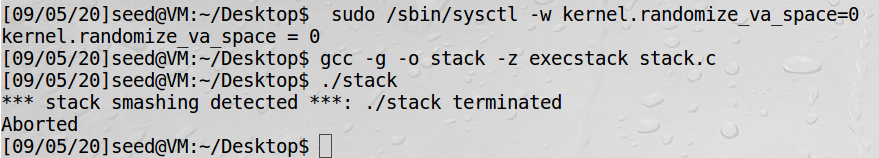
地址随机化开启后，stack运行失败：





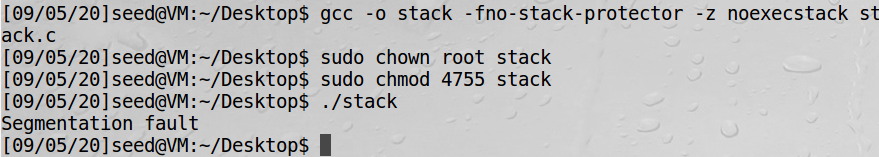
在历遍了74605次后，stack成功获得了root shell。

**Task 5**



开启StackGuard后，stack攻击失败。

**Task 6**



启用不可执行的堆栈保护后，stack攻击失败。