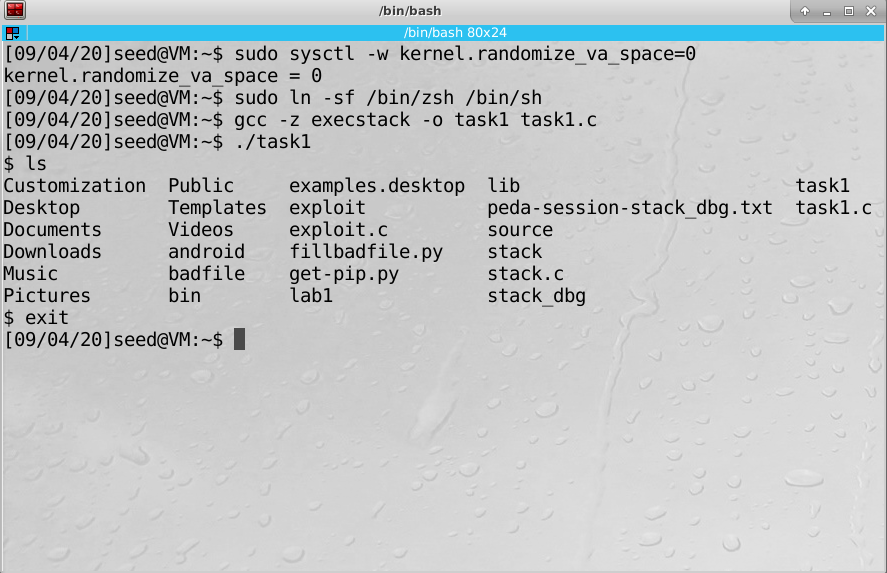
Lab 2

姓名：郭雅琪 学号：57118104

Task1:Running Shellcode



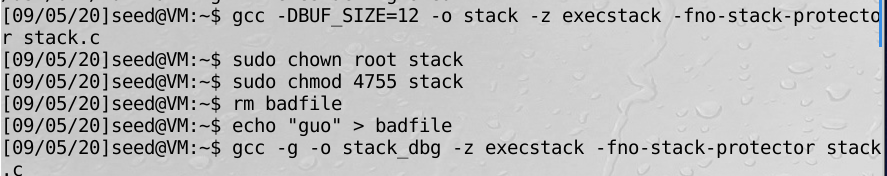
发现通过调用shellcode，/bin/sh被成功打开，表明攻击成功。

Task2: Exploiting the Vulnerability

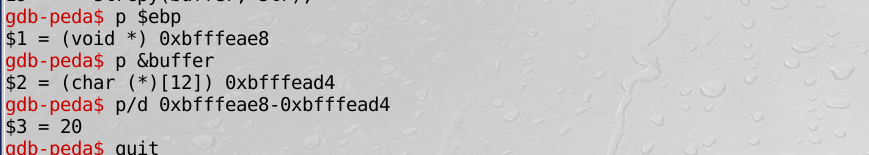
关闭随机堆栈，检查shell。



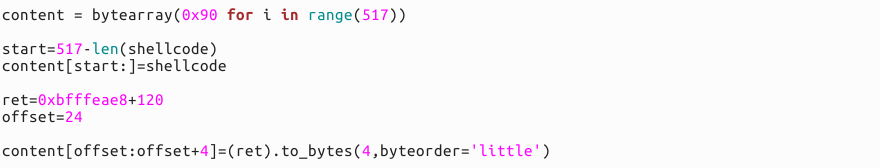
编译stack文件，把buffer\_size设置为12。



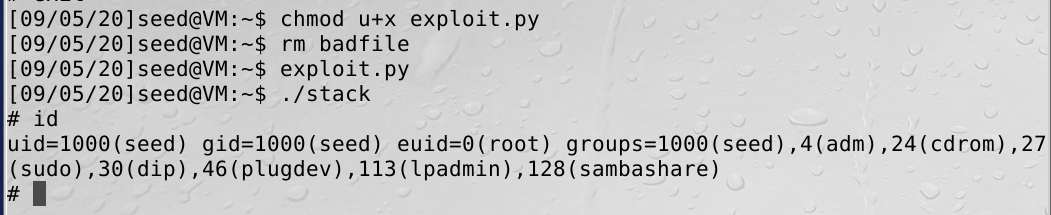
利用gdb查看ebp地址，以及buffer和ebp的距离。



利用实验手册中给出的python脚本，编写shellcode。Ret=ebp+4;offset=ebp-&buffer+4。在地址号为ret的内存中放入shellcode开始的地址（最小为ebp+8,这里取ebp+120）。

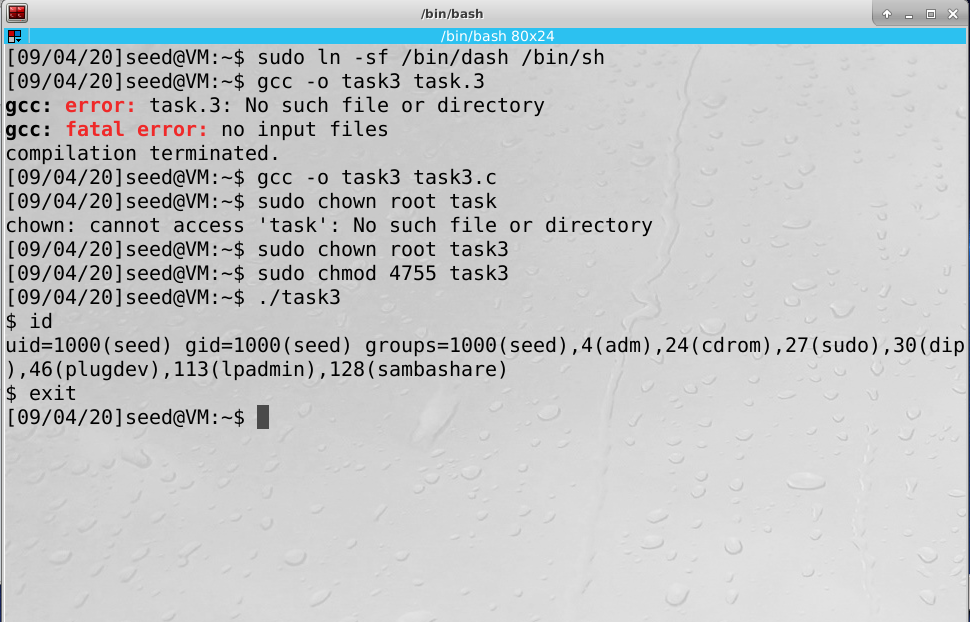


对python进行编译后运行，得到badfile之后运行stack。发现成功调用shell并且获得root权限，攻击成功。

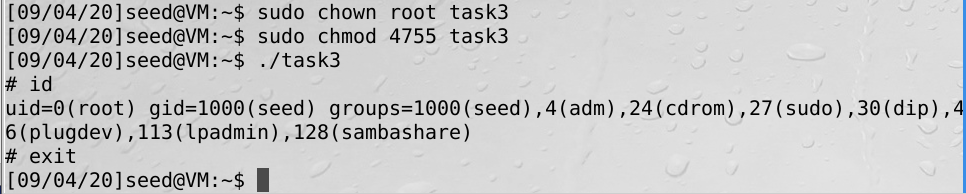


Task3:Defeating dash’s Countermeasure

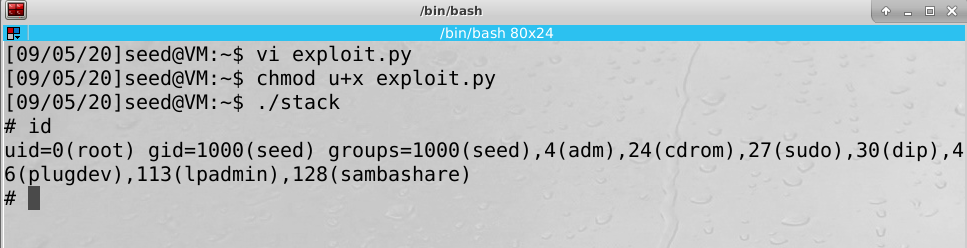
把setuid(0)注释时，uid和euid的值相同，表示进程被降级。



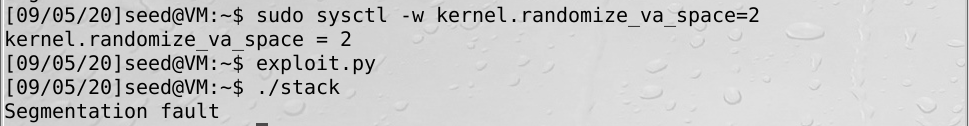
取消注释后运行，uid被成功置为0，表明绕过成功。



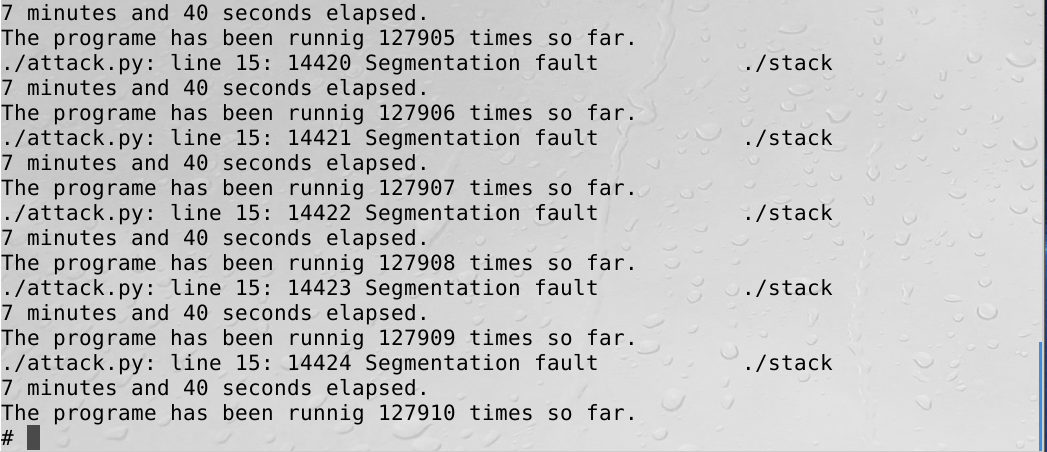
我们再使用task2的代码进行测试，发现成功绕过。



Task4:Defeating Address Randomization

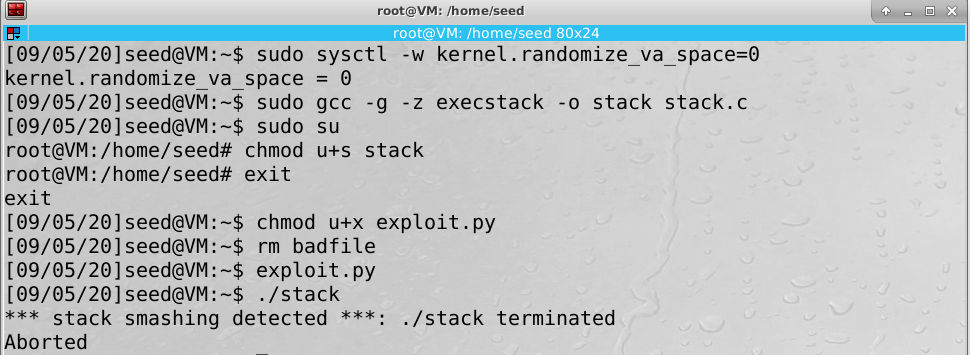


因为地址随机化，所以运行stack后无法成功。利用python程序进行暴力破解，最终结果如下：



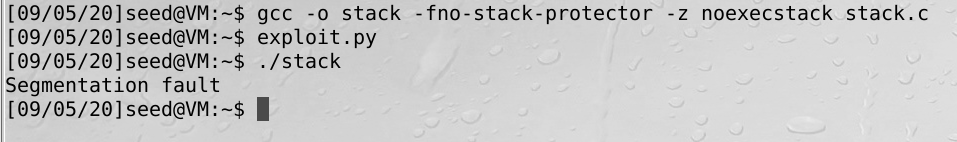
花费7分40秒，运行12万次，最后成功。

Task5:Turn on the StackGuard Protection



开启stack guard之后，发现攻击失败。

Task6: Turn on the Non-executable Stack Protection



关闭可执行栈之后，攻击失败。