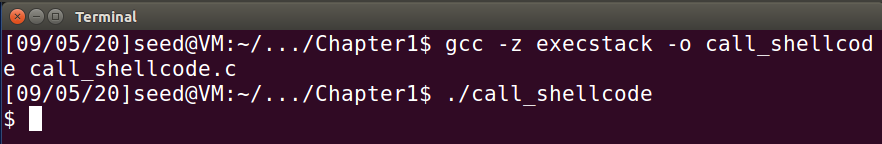
**网络空间安全实训Lab[2]**

**实验报告**

**57118117 谌雨阳**

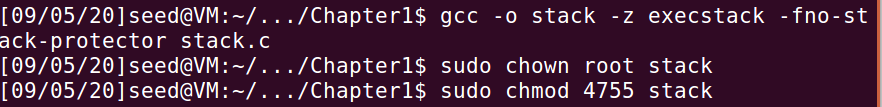
**Task1: Running Shellcode**

1、编译题目所给的程序：



结果：成功调用了一个shell

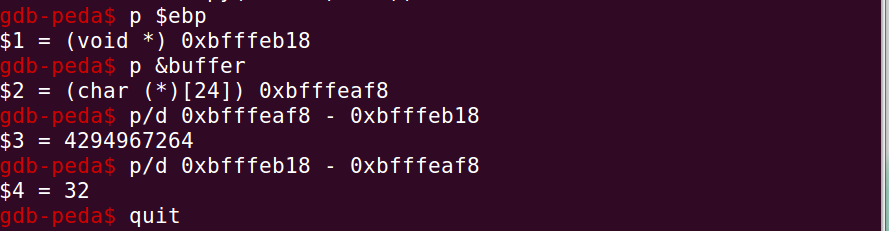
2、编译stack.c并将其设置成SET-UID root程序：



总结：Stack.c文件的编译和设置是重要的准备工作，在后面每一个Task当中都会用到。

**Task 2: Exploiting the Vulnerability**

1、获取ret和计算offset：



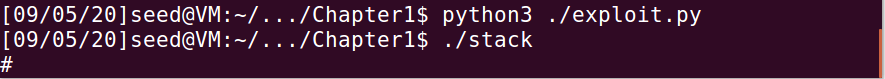
Offset=32+4=36

Ret=0xbfffeb18

2、将值设置在.py文件中：



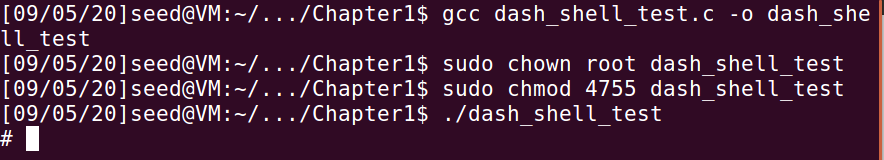
3、运行结果：



结果：得到了root权限，攻击成功。

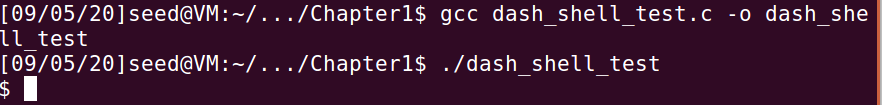
**Task 3: Defeating dash’s Countermeasure**

1、编译原始代码并修改其权限：



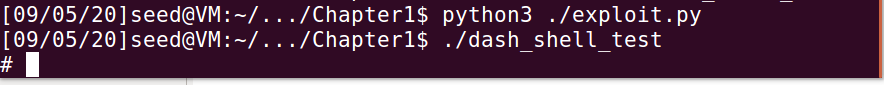
结果：得到了root权限

2、取消注释setuid代码后编译运行：



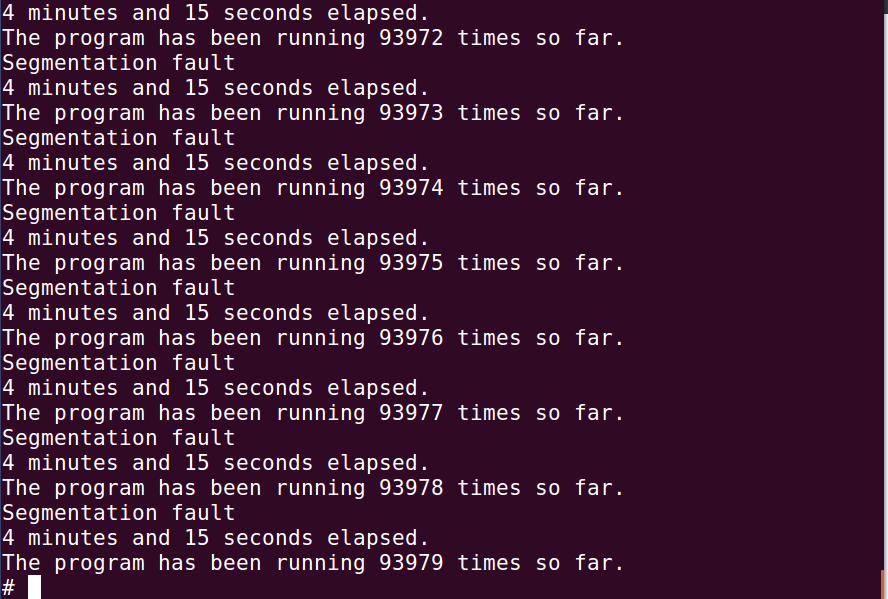
结果：未获得root权限。

3、添加代码后重新进行task2的攻击：



结果：得到了root权限。

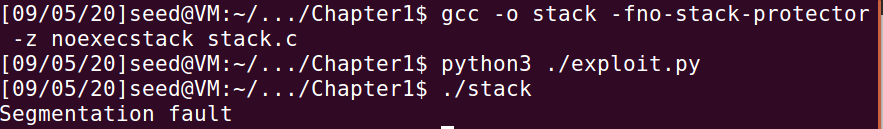
**Task 4: Defeating Address Randomization**



结论描述：运行4分15秒后停止，获得了root权限。

**Task 5: Turn on the StackGuard Protection**

1、去掉-fno-stack-protector重新编译后进行attack：

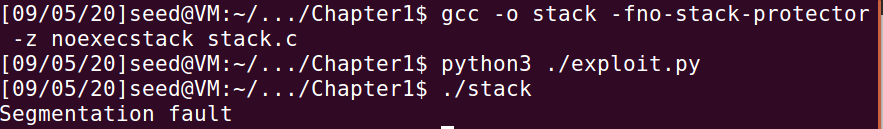


结果：attack失败。

总结：通过与Task2实验对比得知，StackGuard对缓冲区溢出攻击有良好的保护作用。

**Task 6: Turn on the Non-executable Stack Protection**

1、打开Non-executable Stack Protection后进行attack：



结果：attack失败。

总结：同样与Task2实验对比可以得知，Non-executable Stack Protection的开关也会影响缓冲区溢出攻击的效果。