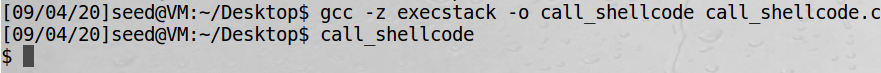
**实验二：**

**Buffer Overﬂow Vulnerability Lab**

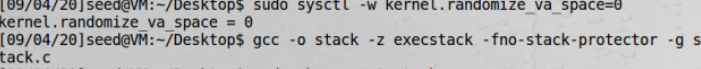
**57117101 焦典**

**Task1：Running Shellcode**

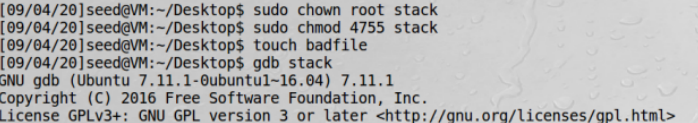


**Task 2: Exploiting the Vulnerability**

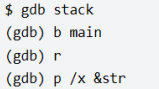
1.编译程序



2.调试gdb



3.获取shellcode地址，shellcode地址为0xbfffe94b

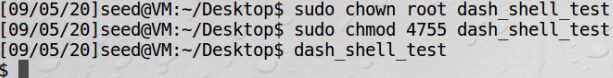


4.编译程序exploit.c，得到root shell



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

1.将程序设置为Set-uid程序，运行得到shell



2.取消注释后，重新编译程序，运行得到root权限的shell



3.连接dash后，也得到root权限的shell



**Task 4: Defeating Address Randomization**

1.地址随机化

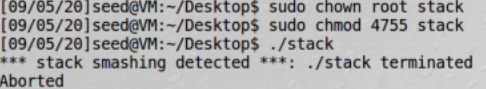


2.攻击失败后，暴力破解



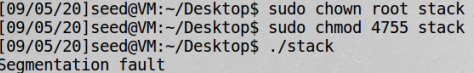
**Task 5: Turn on the Stack Guard Protection**

关闭地址随机化，编译时不关闭栈，程序终止执行。



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

关闭地址随机化，编译时打开可执行栈，攻击失败。

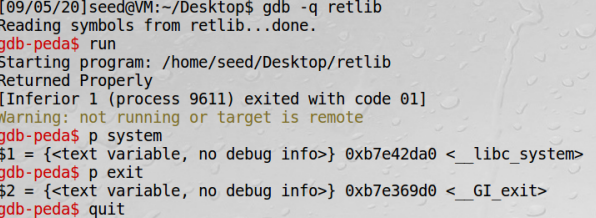


**Task 1: Finding out the addresses of libc functions**

**1.编译程序**



2.得到地址如图



**Task 2: Putting the shell string in the memory**

**1.定义环境变量**



2.获取环境变量地址为bffffdae

