

**入侵检测与数字取证**

**黄雨卓 57117205**

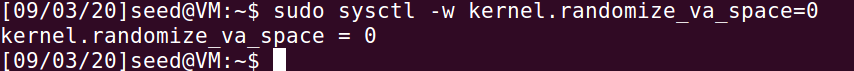
**LAB2**

2020年9月5日

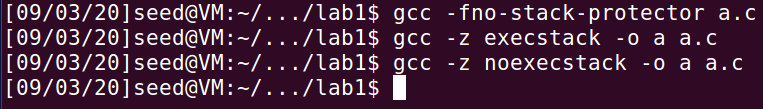
Buffer Overflow Vulnerability Lab

Task1

2.1Turning Off Countermeasures

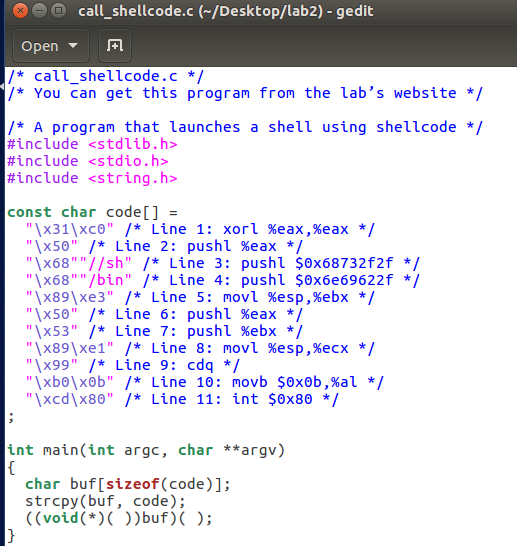
地址空间随机化，StackGuard保护方案，不可执行的堆栈。

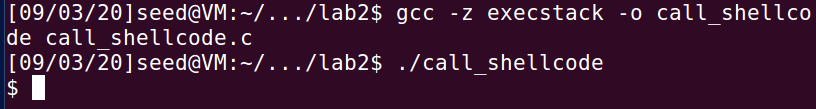




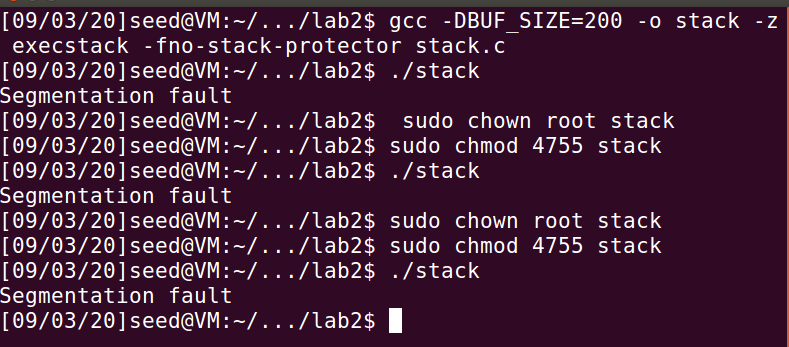
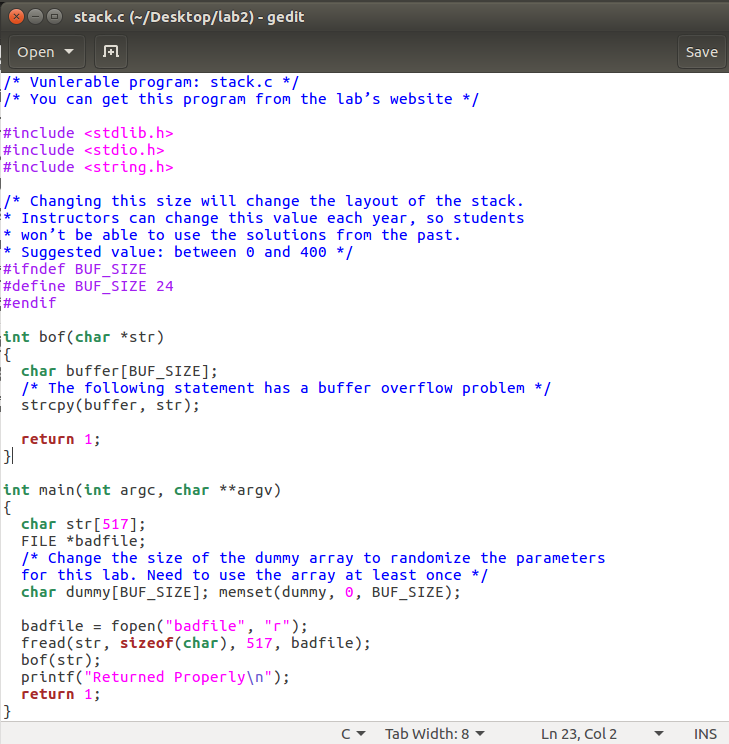


2.2Running Shellcode



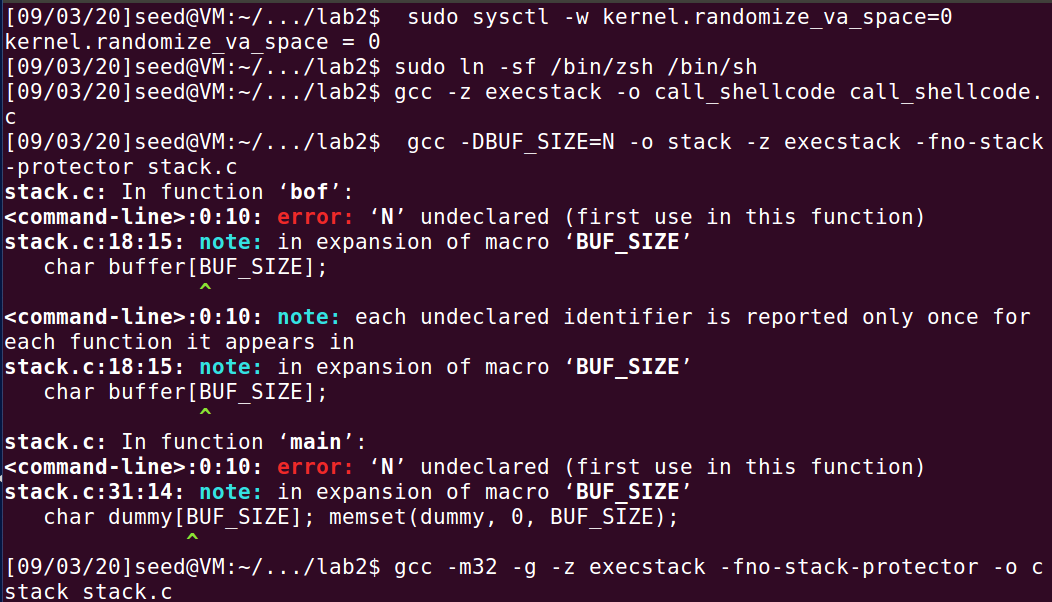


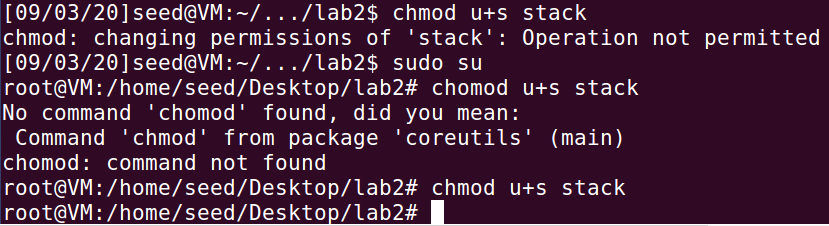
2.3 The Vulnerable Program

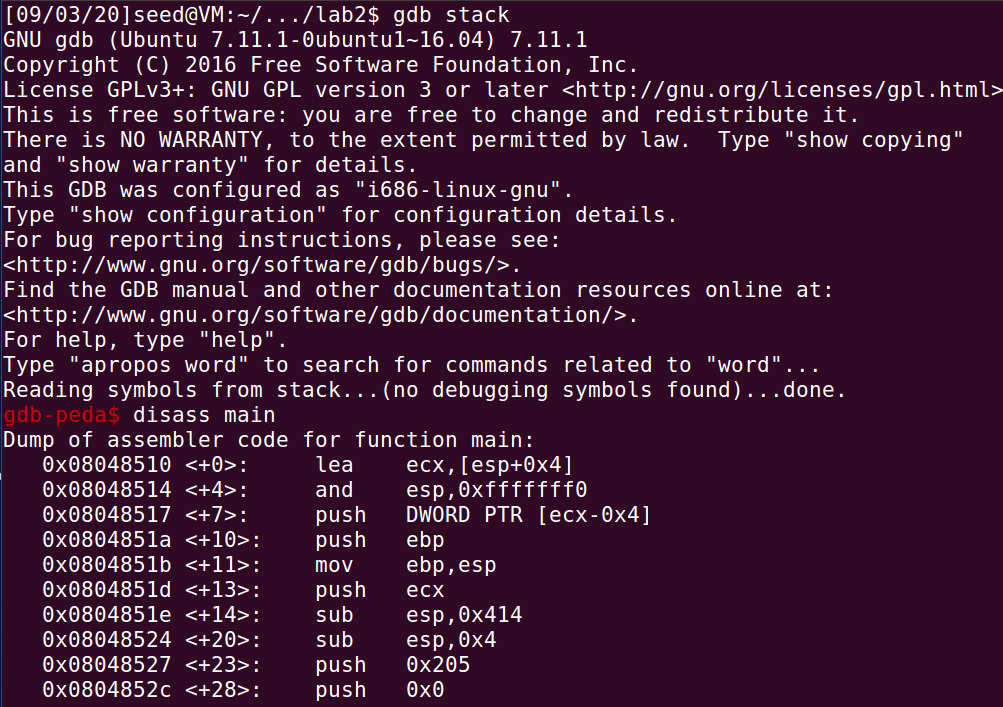


Task 2

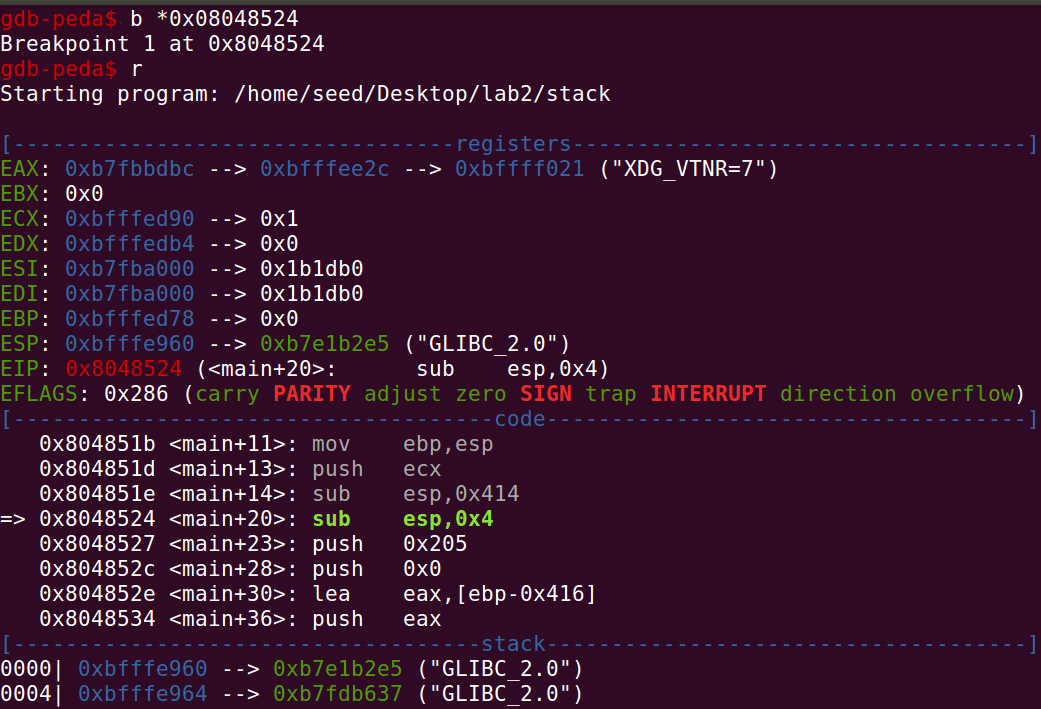
2.4 Exploiting the Vulnerability

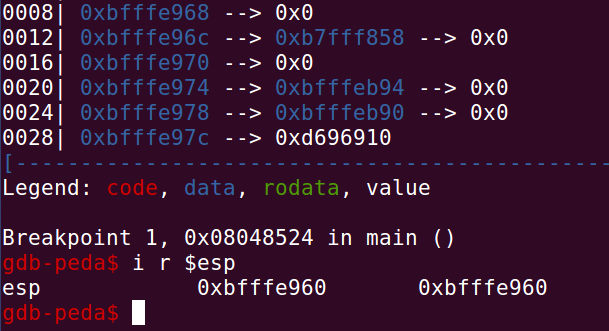


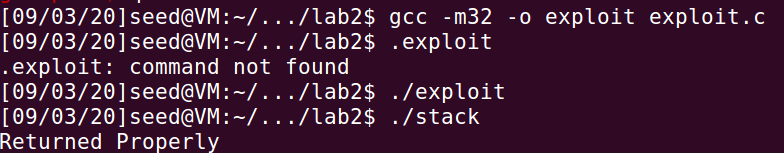








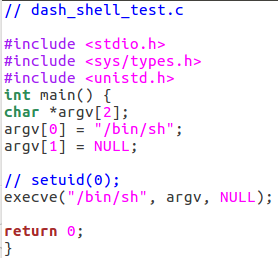


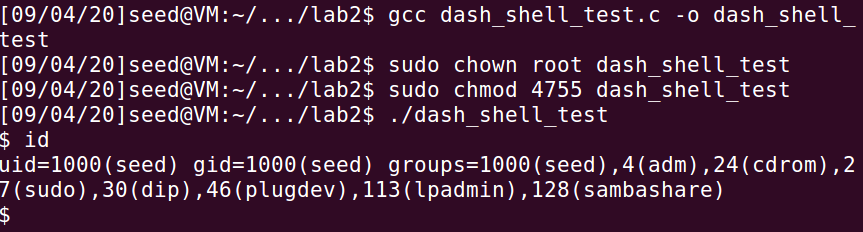


Task 3

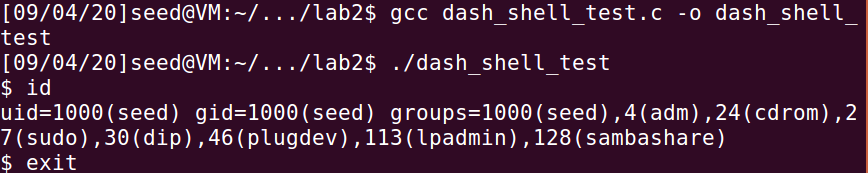
2.5 Defeating dash’s Countermeasure

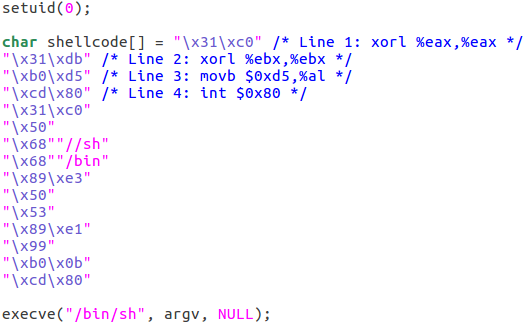


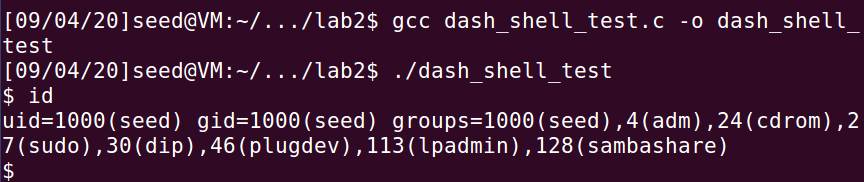
注销掉setuid(0)，发现可以绕过：



取消注销再次运行：可以绕过

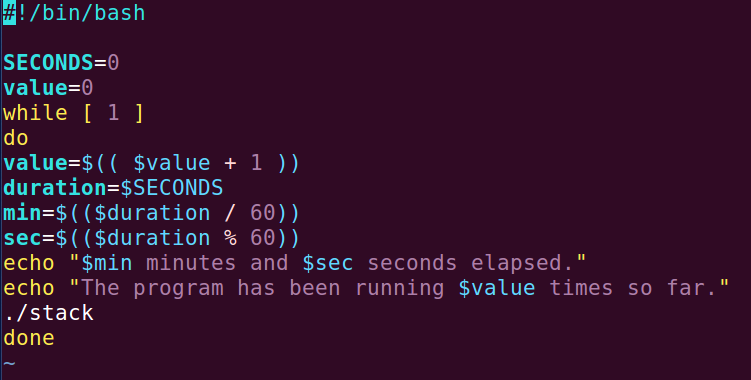


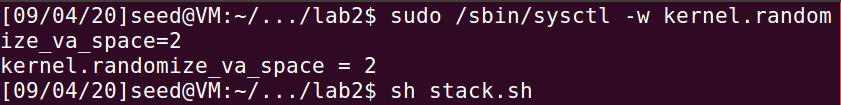




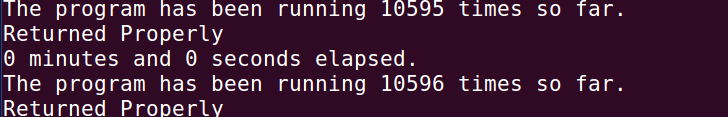
Task 4

2.6 Defeating Address Randomization



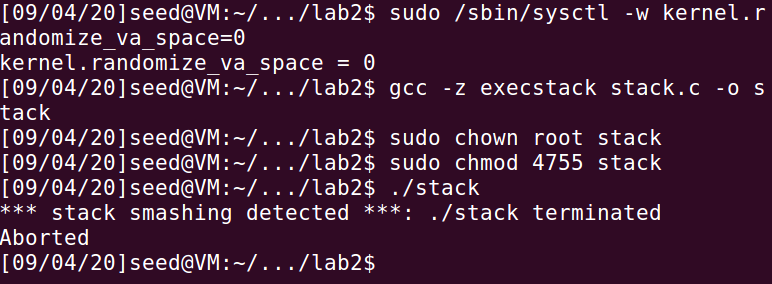


攻击失败



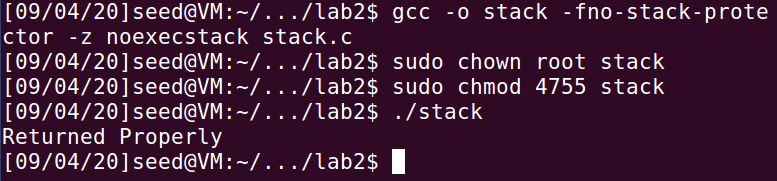
Task 5

2.7 Turn on the Stack Guard Protection



Task 6

2.8 Turn on the Non-executable Stack Protection

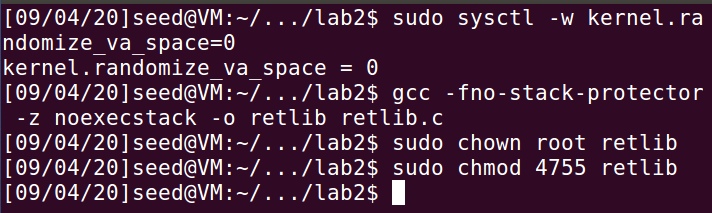


Return-to-libc Attack Lab

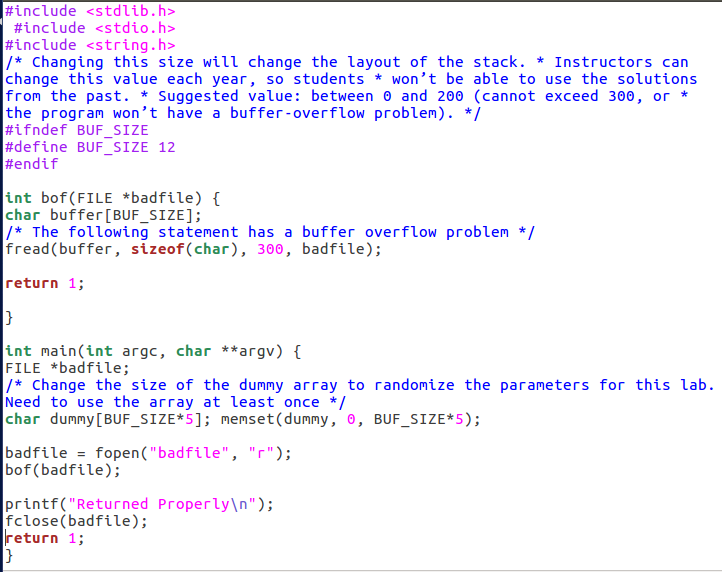
Task1

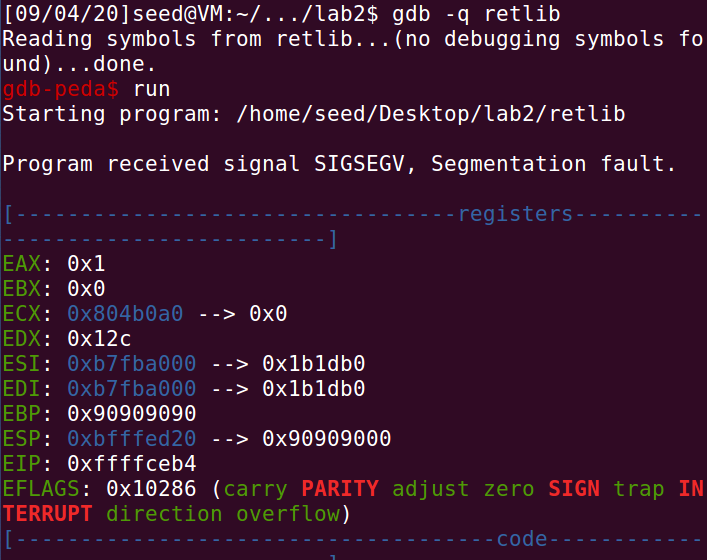
2.3 Finding out thead dresses of libc functions

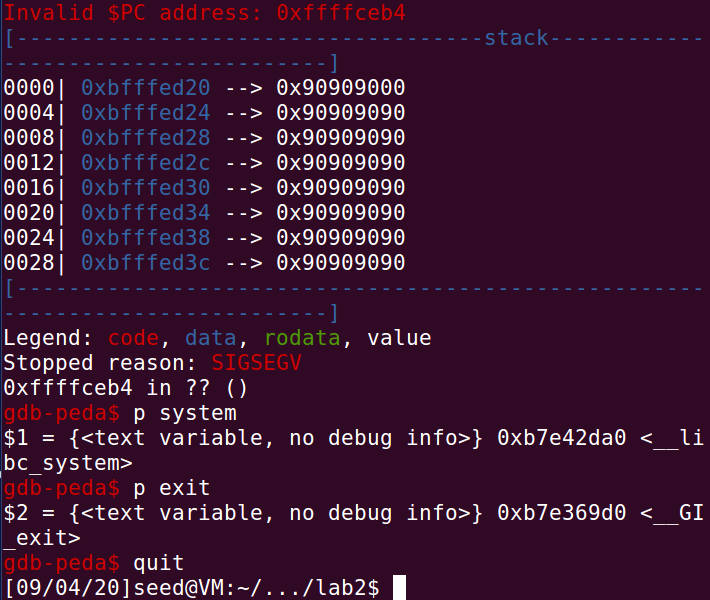
Turning off counter measures



The Vulnerable Program

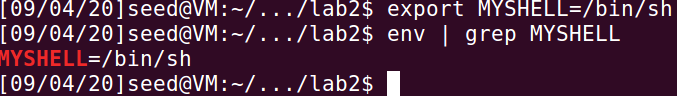


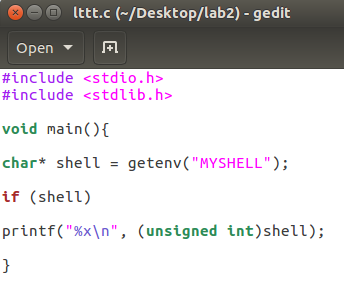


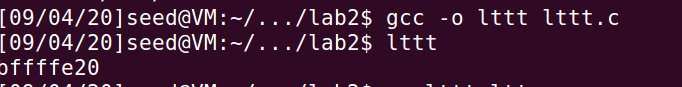


Task2

2.4 Putting the shell string in the memory

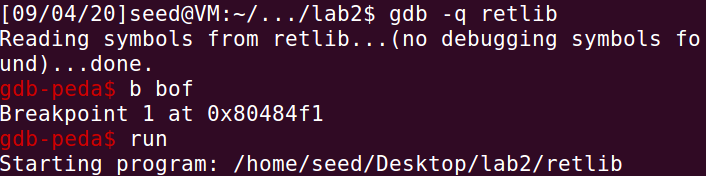


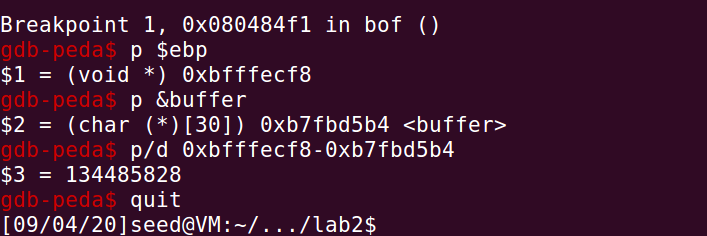


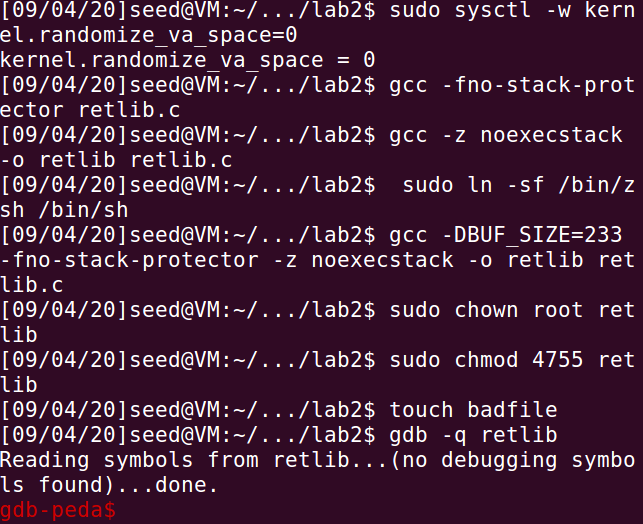


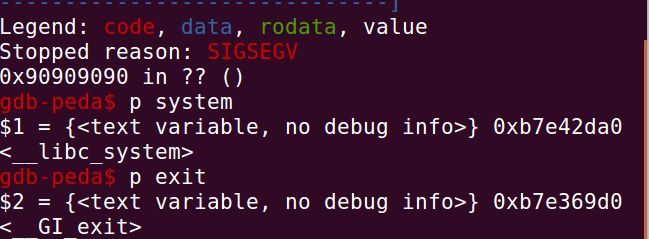
Task3

2.5 Exploiting the buffer-overﬂow vulnerability





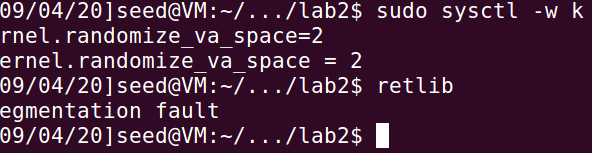




Task4

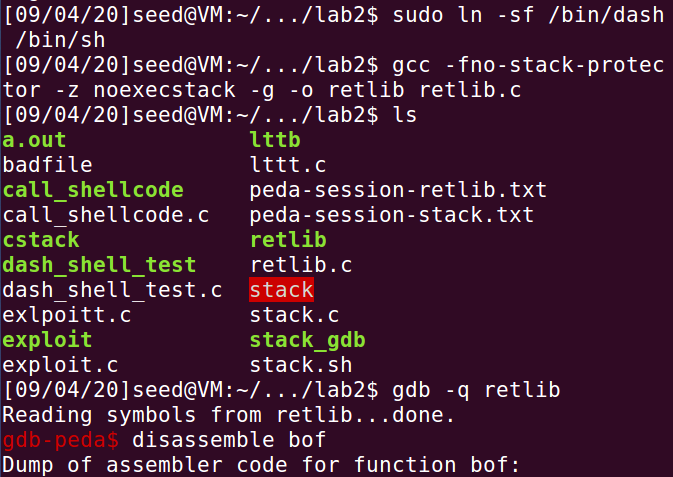
2.6 Turning on address randomization

报错，段错误



Task5

2.7 Defeat Shell’s counter measure



Task6

2.8 Defeat Shell’s counter measure without putting zeros in input

