Lab2

57117140 庞乃瑜

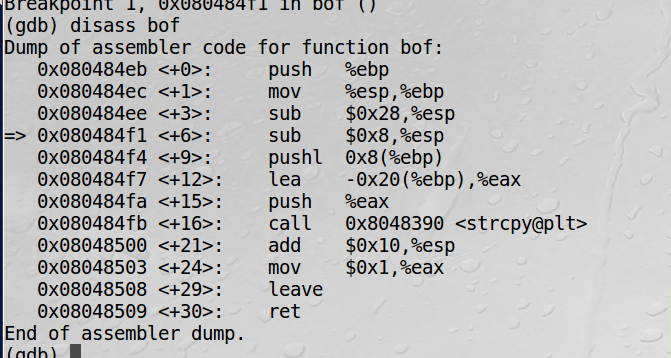
Lab21

Task1:

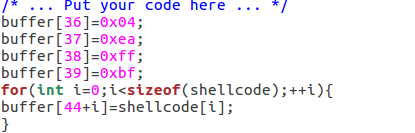
启动了一个新的shell

Task2:

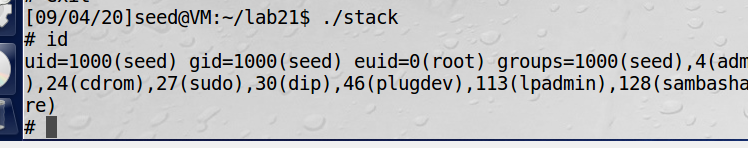
用GDB反汇编bof函数



可以看到ebp和buffer地址距离为32个字节，为了防止出现0终止复制，在shellcode地址之后加4个nop，所以badfile构造为32NOP+shellcode地址+4NOP+shellcode；由于GDB中看到的地址不是真实的地址，利用执行stack段错误时的core文件找到esp地址，可知esp地址即为shellcode地址，得shellcode地址为0xbfffea04,小端填入，添加代码如下

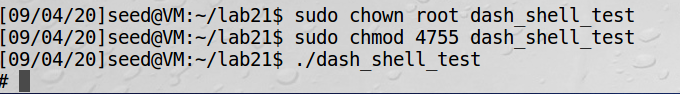


结果如下：



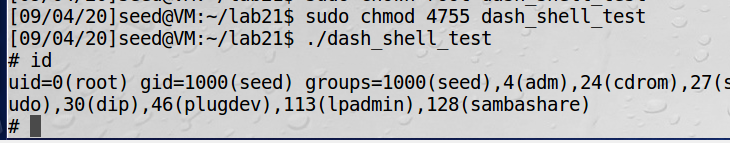
Task3:

Setuid(0);被注释时



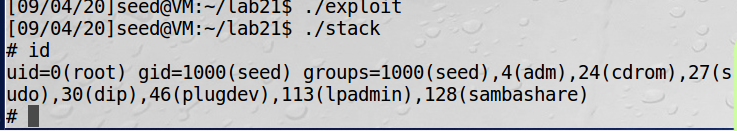
获得的shell没有root权限

没有被注释时



有root权限

添加后task2：



因为系统检测到real uid为0,认为是一个真的root用户，所以没有进行降权处理，获得了一个root权限的shell

Task4:

Task5:

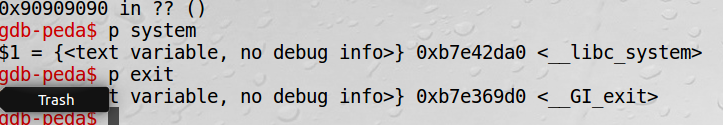
检测到栈溢出，程序被终止

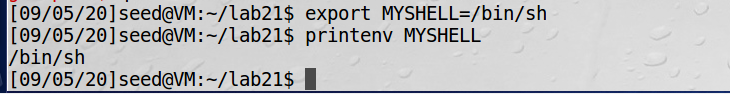
Task6:

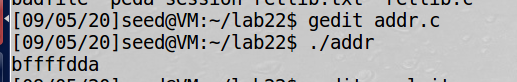
不能，栈不能执行，shellcode不能执行，不能获得shell，会发生段错误

Lab22

Task3:

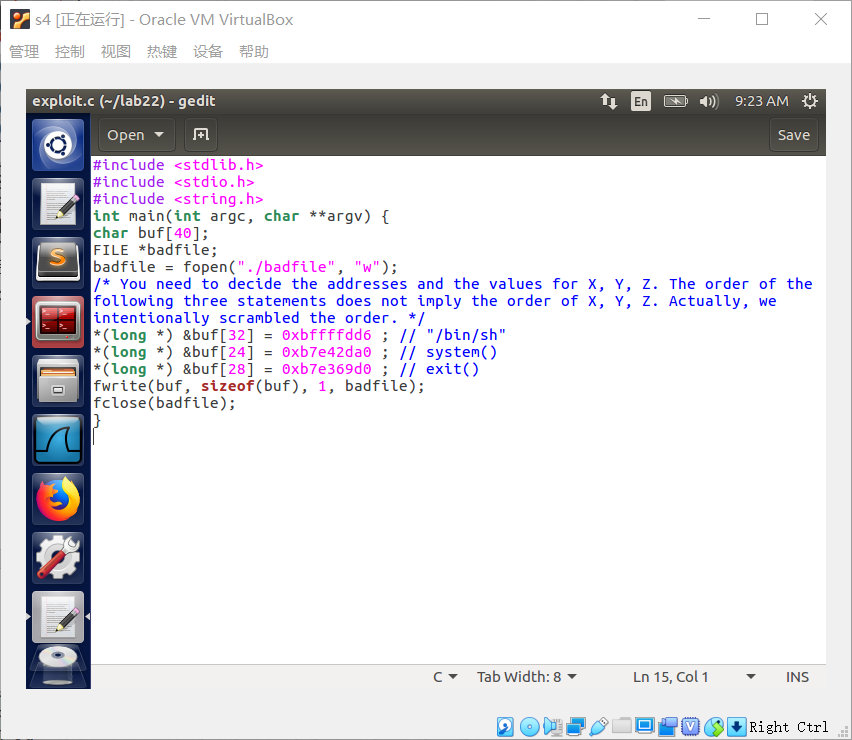


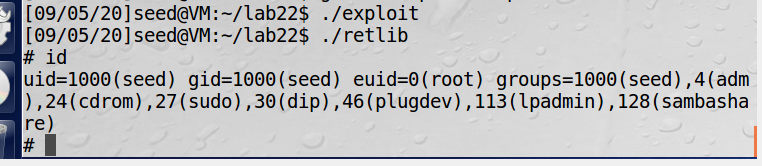




最后猜出来地址为0xbffffd6

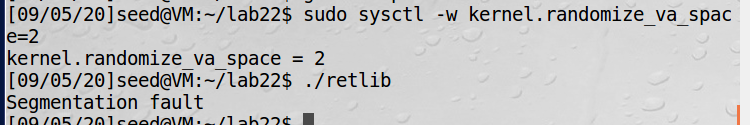
所以exploit.c如下



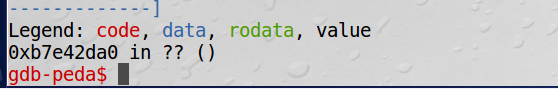


成功提权

Task4:



发生段错误



System()的地址不正确