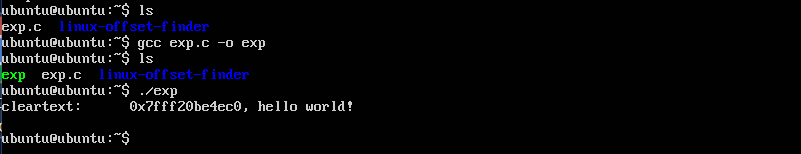
1.安装VirtualBox，并导入实验虚拟机的虚拟硬盘文件，进行相应的设置，然后运行该虚拟机。

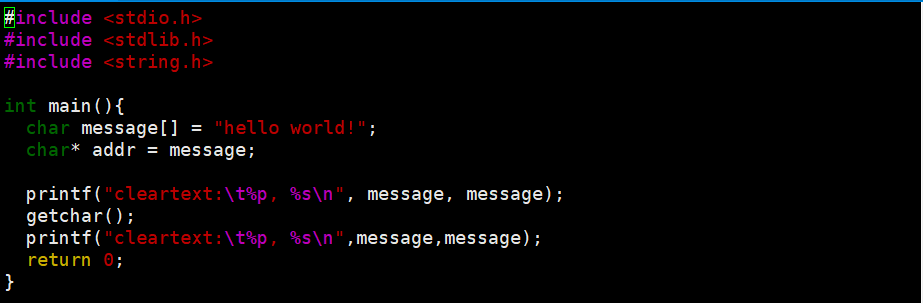
2.输入用户名vagrant和密码vagrant登录host虚拟机，在命令行输入virsh进行交互终端，在终端中输入list --all可以看到处于关机状态的guest虚拟机Ubuntu 16.04。输入start ubuntu16.04即可启动该虚拟机。



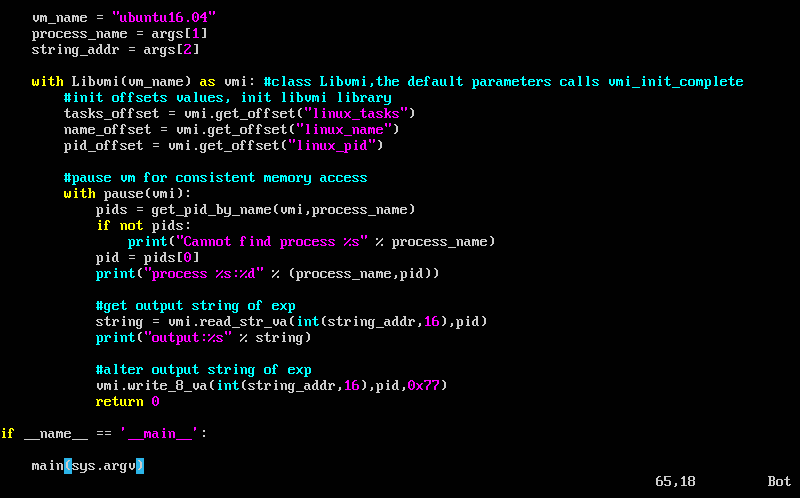
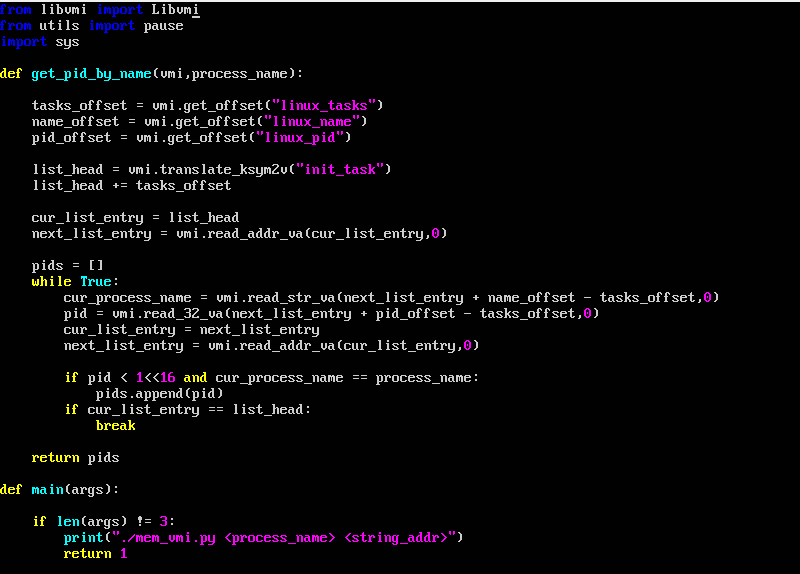
3.退出virsh终端，输入ssh ubuntu@192.168.122.160登录guest虚拟机，可以看到当前路径下存在一个exp.c文件，输入gcc exp.c -o exp将该文件编译，输入./exp运行该文件。该程序的功能是输出字符串在进程空间中的地址，然后等待用户输入并结束程序。



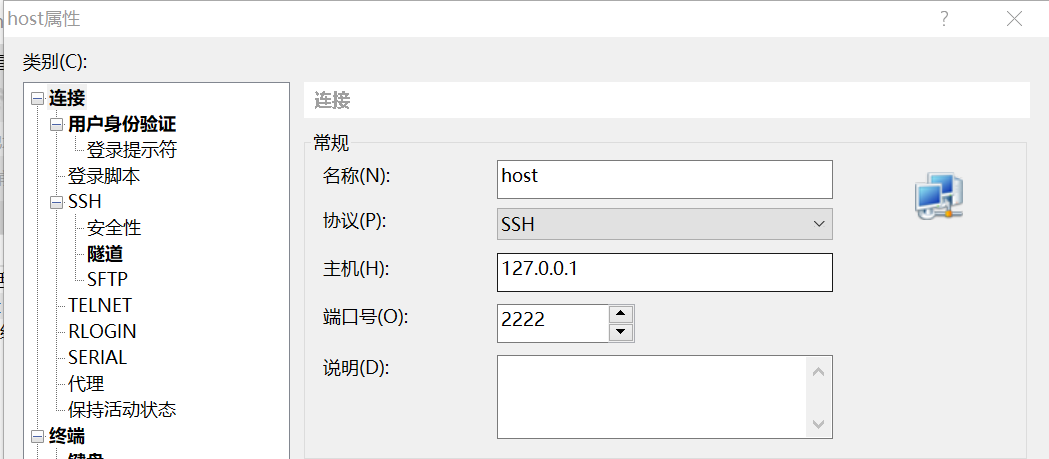
4.在guest虚拟机中输入vim exp.c做如下修改，该程序存储了message数组的起始地址，并在接收到用户的键盘输入后将该地址指向的数据再次输出，以验证host虚拟机是否修改成功，修改完成后重新编译并生成exp。



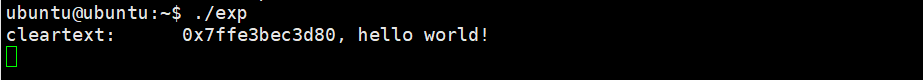
5.在host虚拟机中输入vim mem\_vmi.py，编写以下程序。该程序接收两个参数分别是guest虚拟机中的进程名process\_name和exp程序输出的字符串地址string\_addr，根据进程名找到对应的PID，然后根据PID和string\_addr读取并修改string\_addr指向的字符串内容。

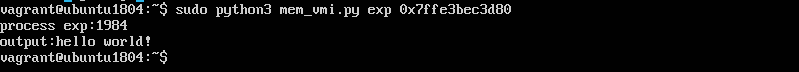


6.在VirtualBox中选择“设置”-“网络”-“端口转发”可以看到相应的端口转发规则。在Xshell中新建连接，设置主机ip地址为127.0.0.1，端口号为2222，即可远程连接到host虚拟机，然后再ssh登录到guest虚拟机，同时在VirtualBox中进入host虚拟机。



7.先在guest虚拟机中运行exp程序，输出如下所示



 然后在host虚拟机中运行mem\_vmi.py，输出如下所示，可以看到已经成功读取了exp输出的内容

在guest虚拟机中按任意键，输出如下所示，可以看到成功将0x7ffe3bec3d80处的数改成了0x77(w)，修改成功。

