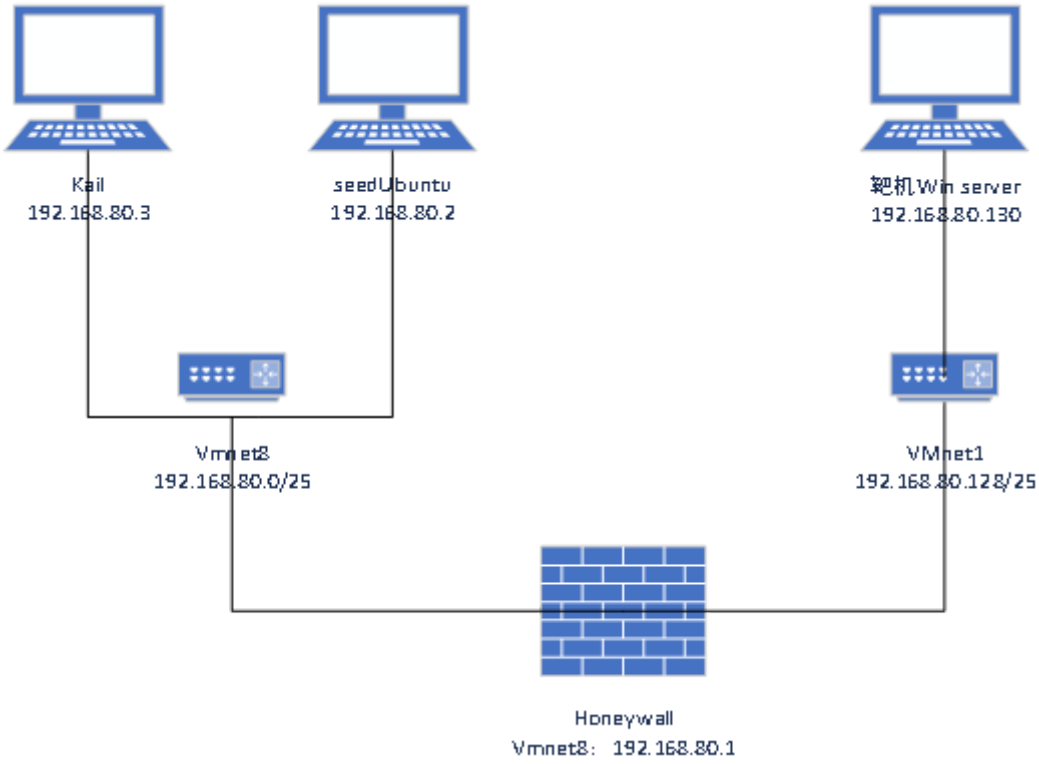
第1次作业-实践一 网络攻防环境的搭建

1、学习总结

本次实验是配置一个用于捕获攻击信息的密网。其中，honeywall作为一个蜜罐，他对于外网应该是不可见的（所以无法ping），win server作为诱饵，吸引kail和seedUbuntu攻击，而攻击流量必然要通过honeywall。在本实验中，如果没有honeywall的话，kail和seedubuntu是无法与win server通信的，因为一个在NAT网络，一个在仅主机网络。

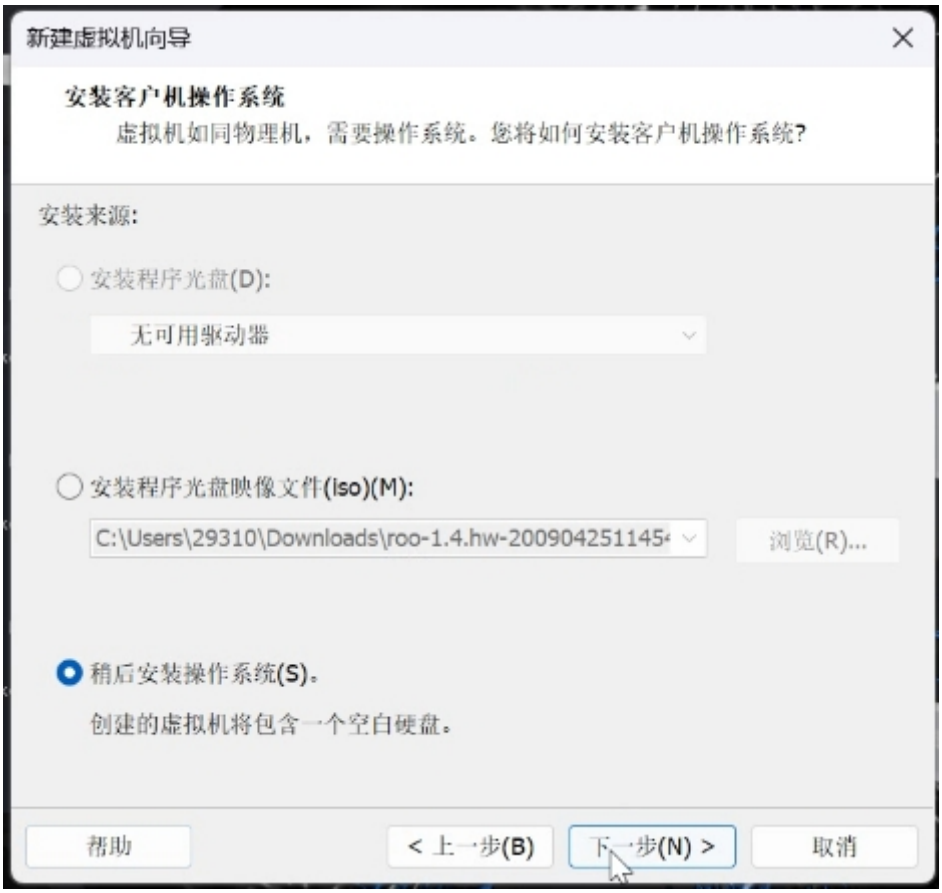
网络流量拓扑图如下（在该拓扑图中，存在攻击机、靶机和蜜罐）



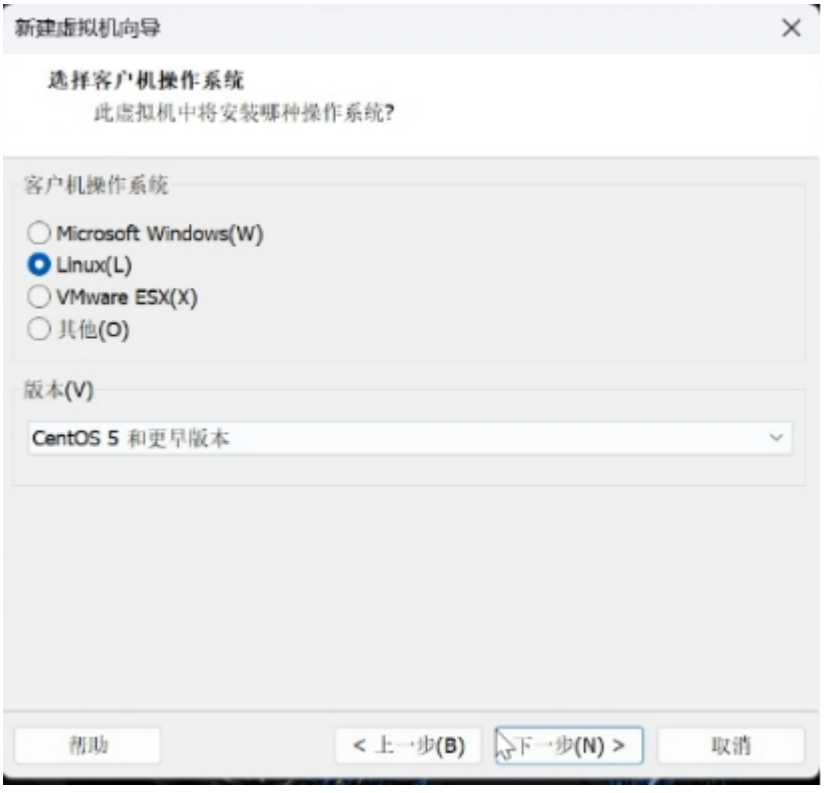
2、搭建详细过程

1、安装honeywall

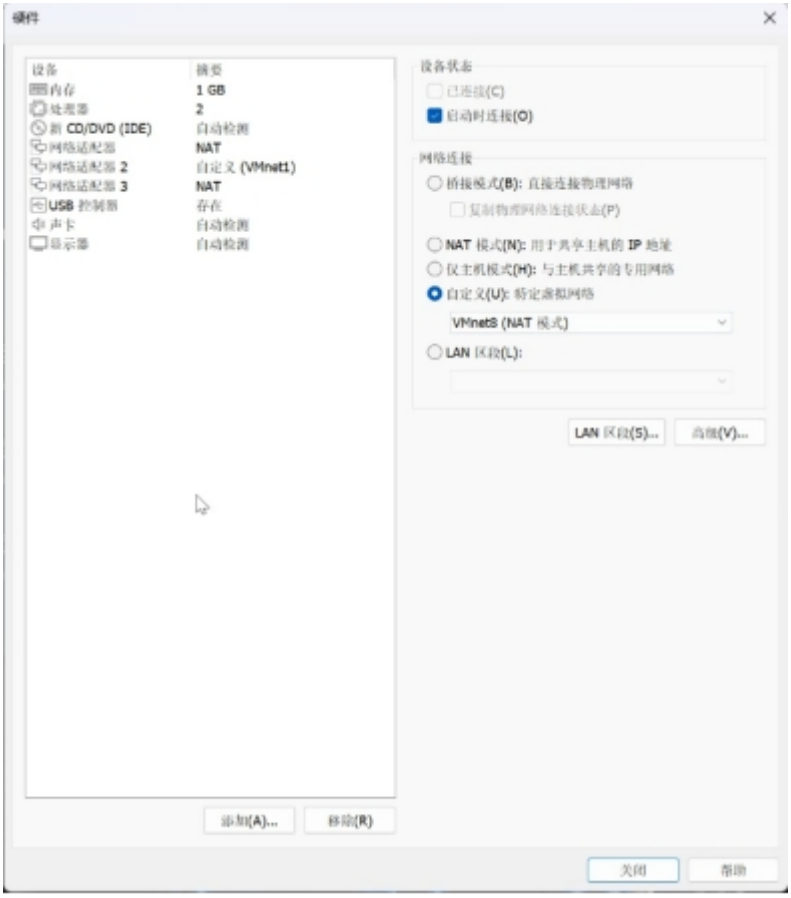
(1) 选择稍后安装操作系统



(2) 版本选择Centos5和更早版本



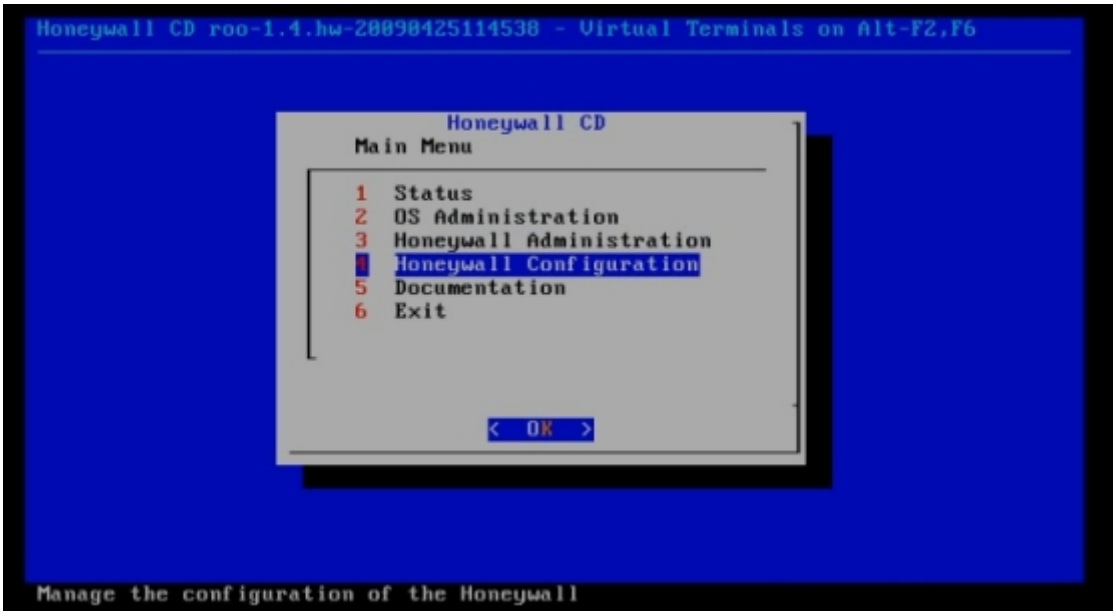
(3) 设置holleywall的网络设配器，其中一个设置为仅主机网络，一个设置为NAT



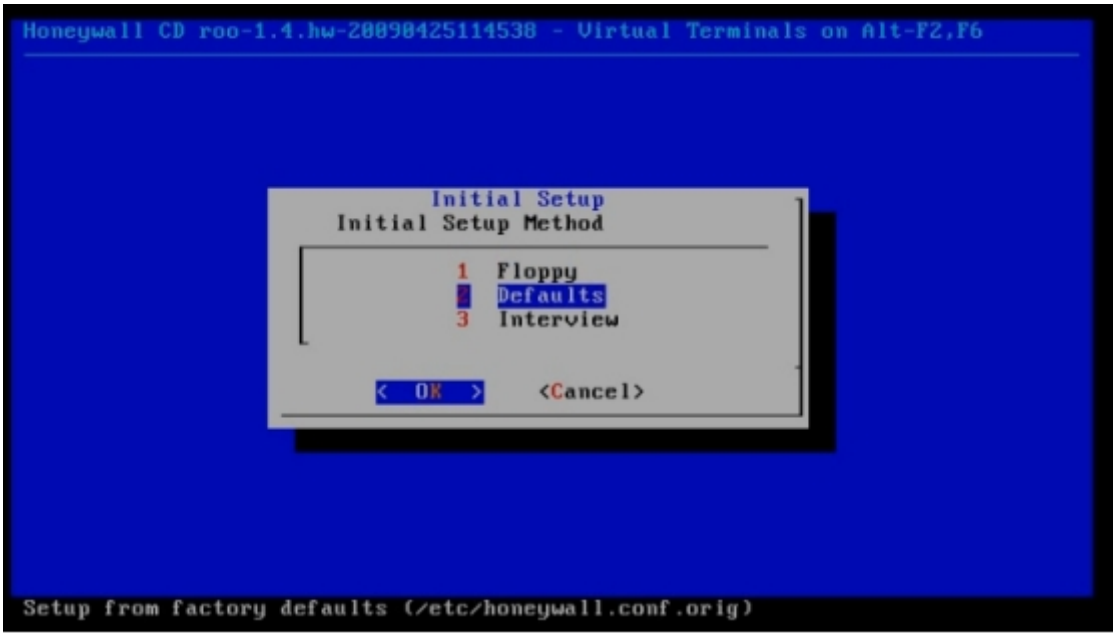
(4) 加载ISO映像文件

(1) 配置hollywall

① 登陆后输入su -，开始配置



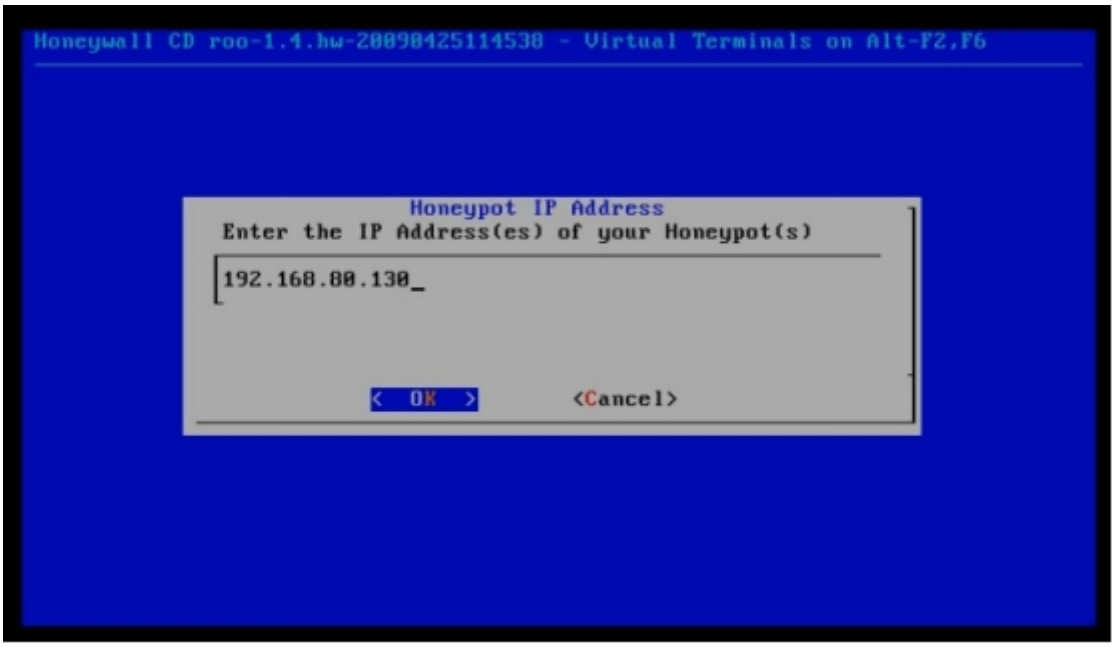
② yes后，选择默认安装



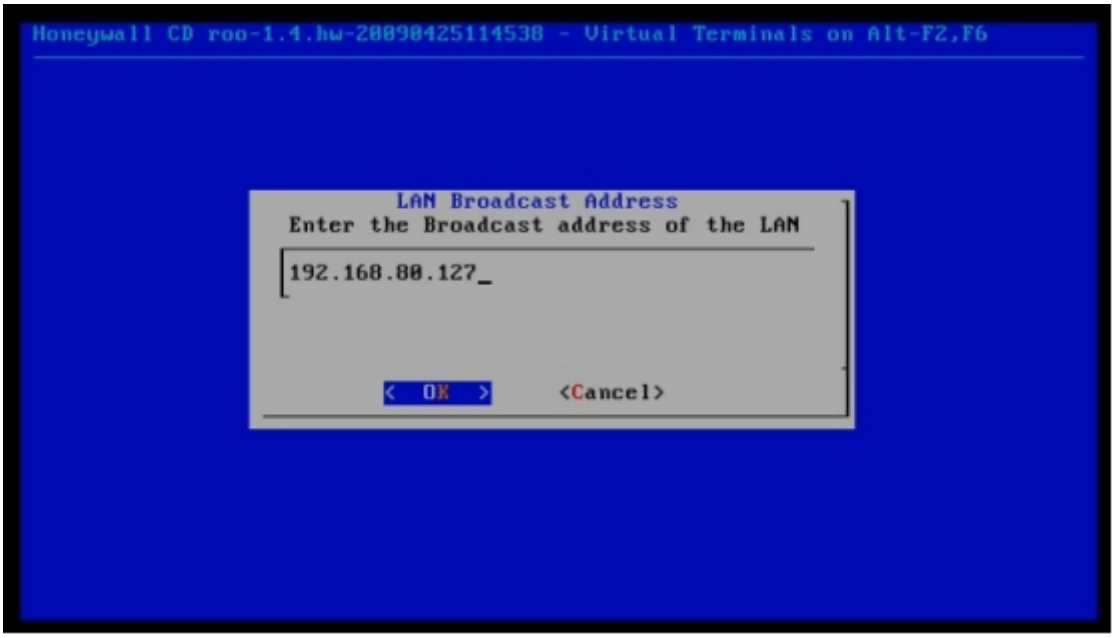
③ 经过自动安装的进程后，将进入以下界面

④ 选择第四项，然后开始配置靶机ip和honeywall在vmnet中的信息

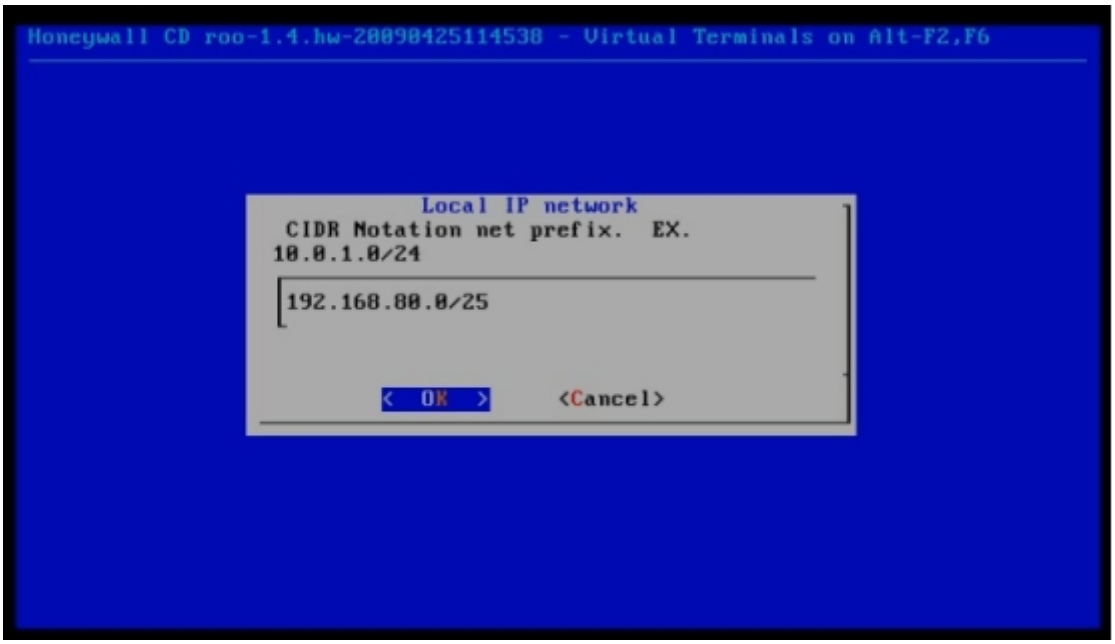
(1) 靶机ip配置



(2) Vmnet8广播地址设置

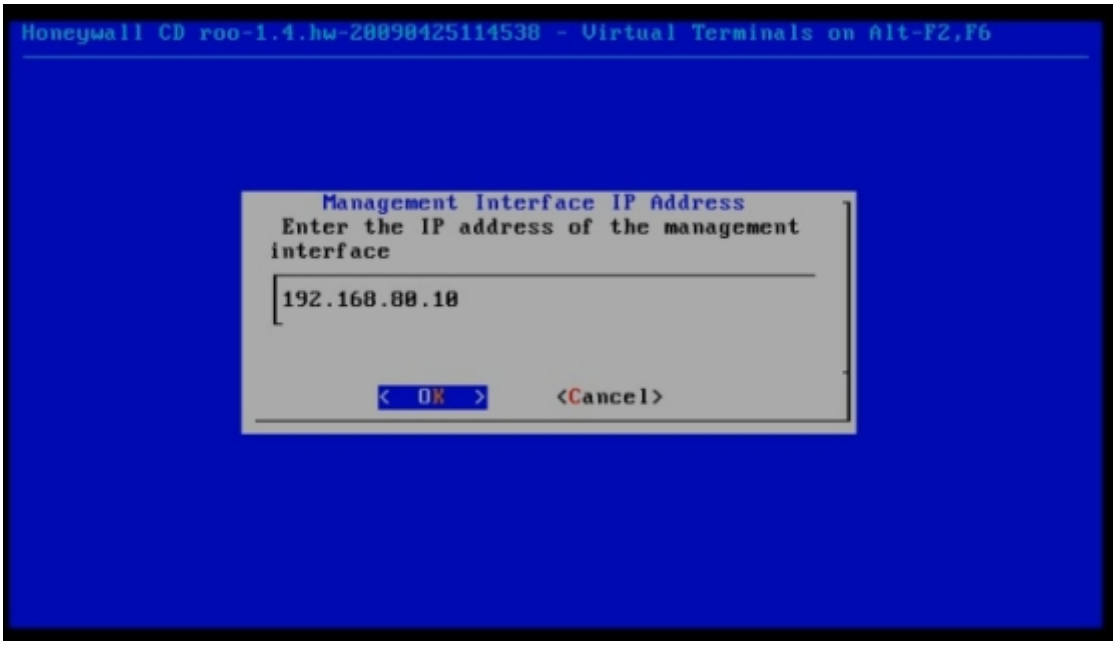


(3) VMnet网段设置

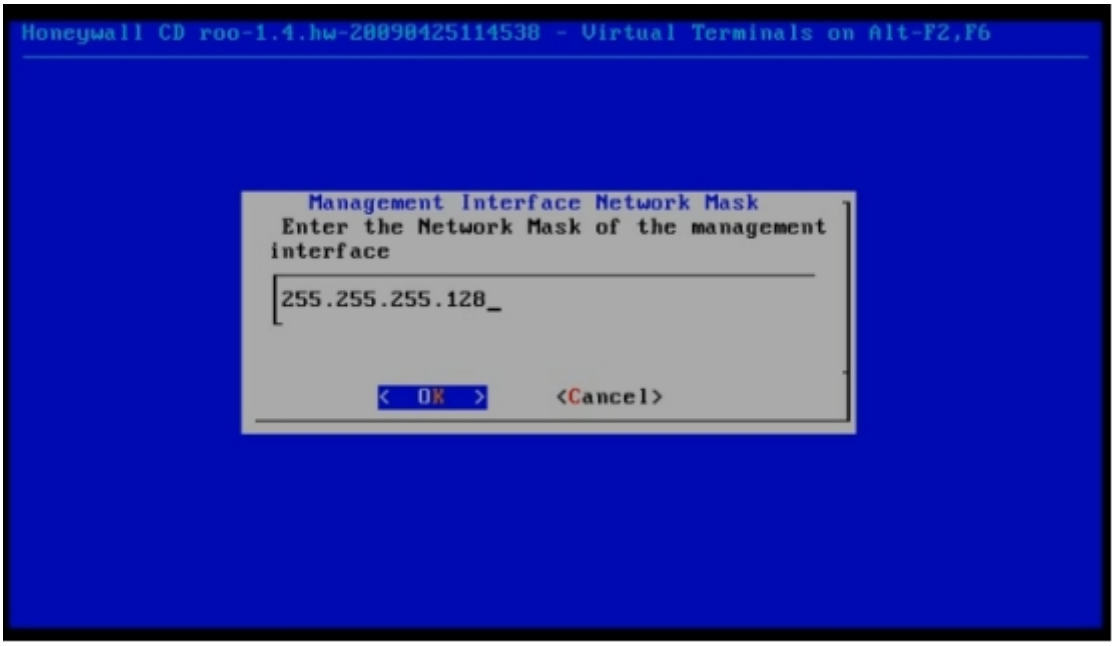


⑤ 远程IP地址设置

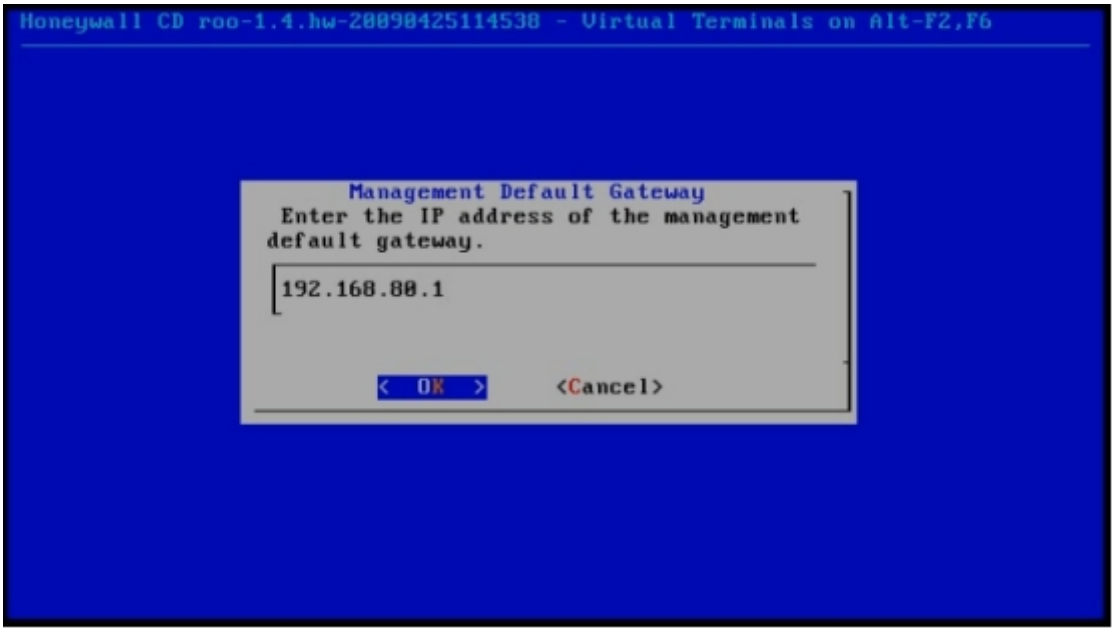
(1) Honeywall IP地址设置



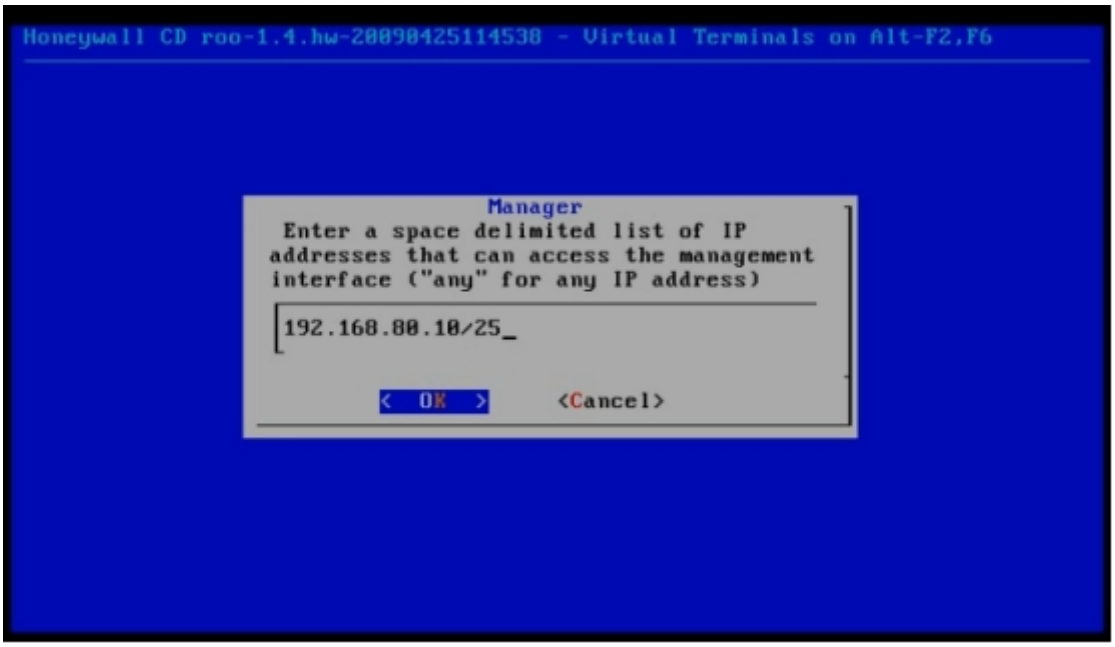
(2) 设置子网掩码



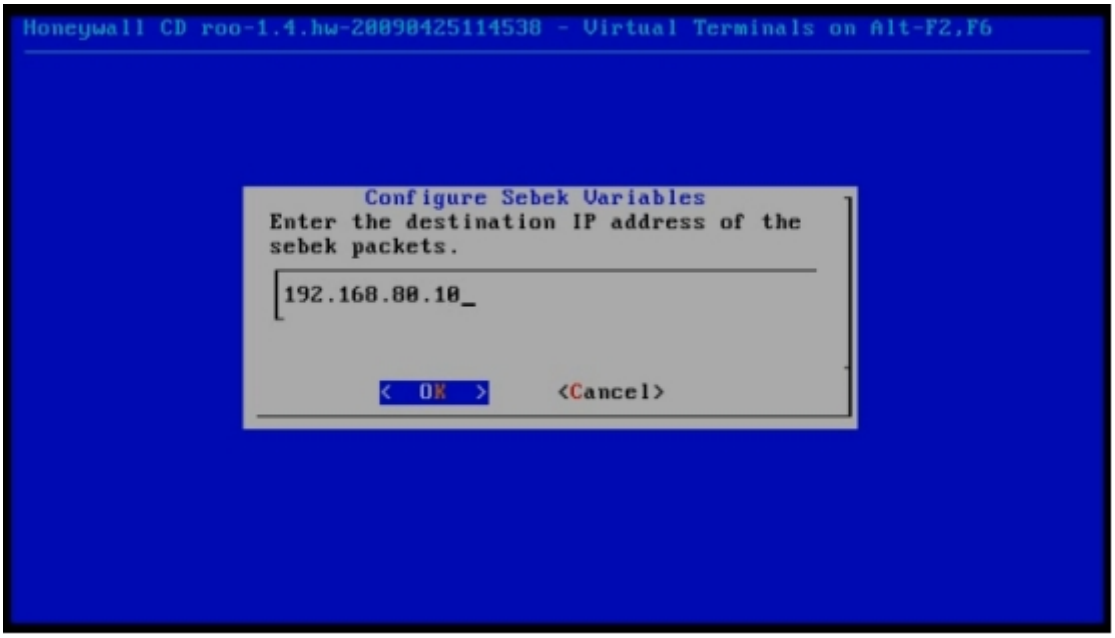
(3)设置vmnet的网关



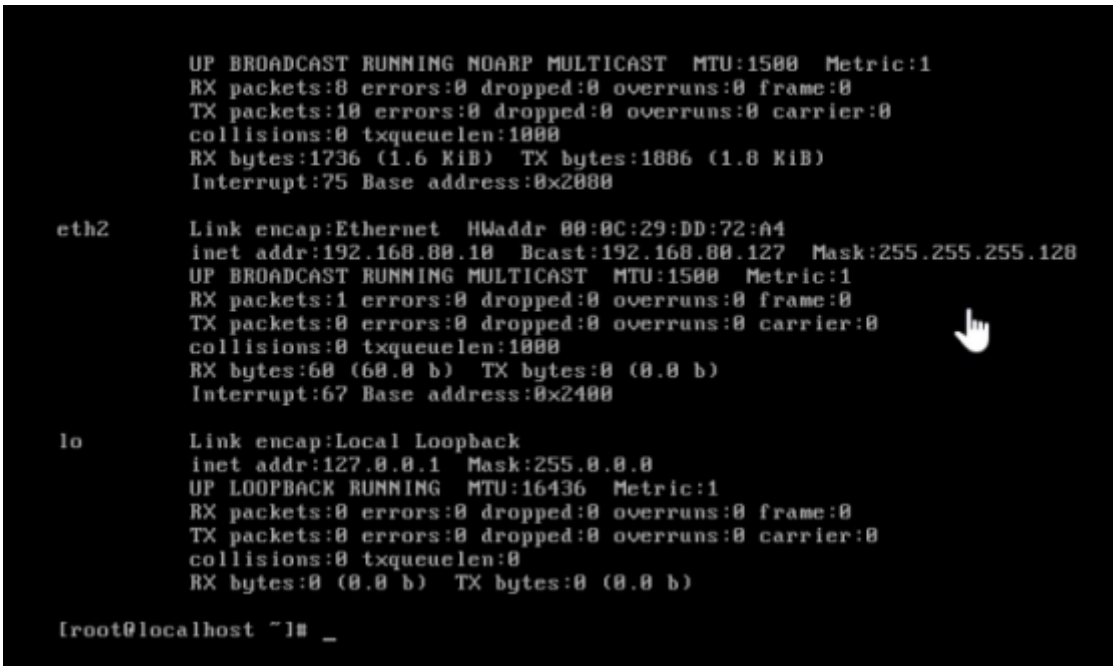
(4) 设置可通信的网段



(4) 设置sebek的ip地址



(6) 结束，查看ip



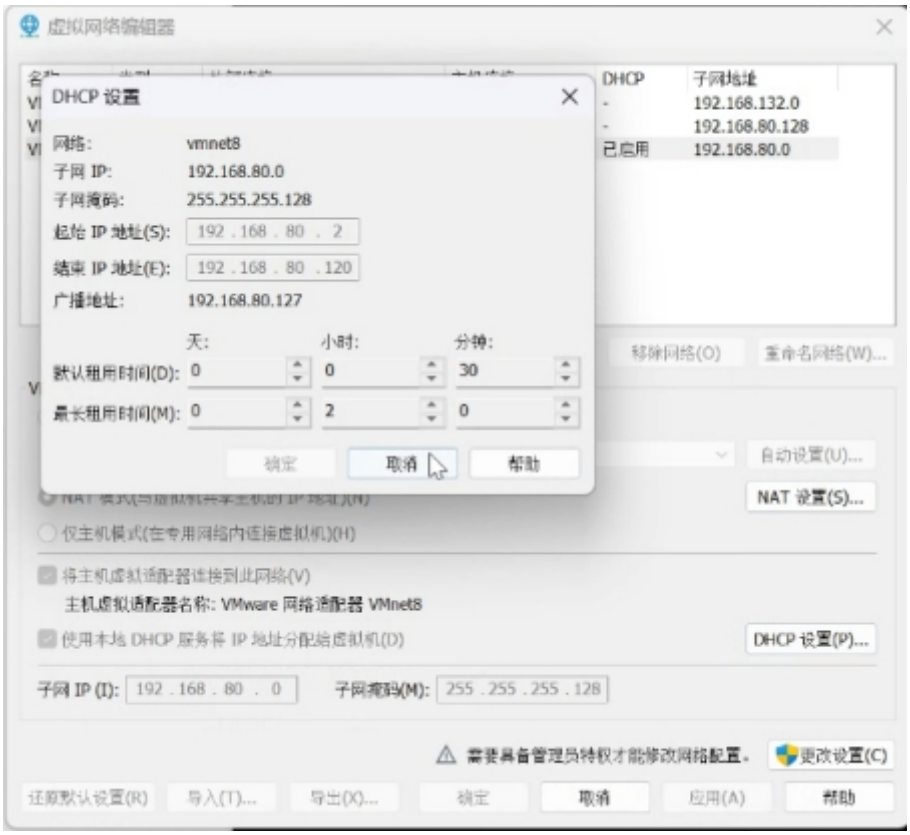
2、设置虚拟网络编辑器

(1) VMnet1设置

(2) 设置VMnet8设置

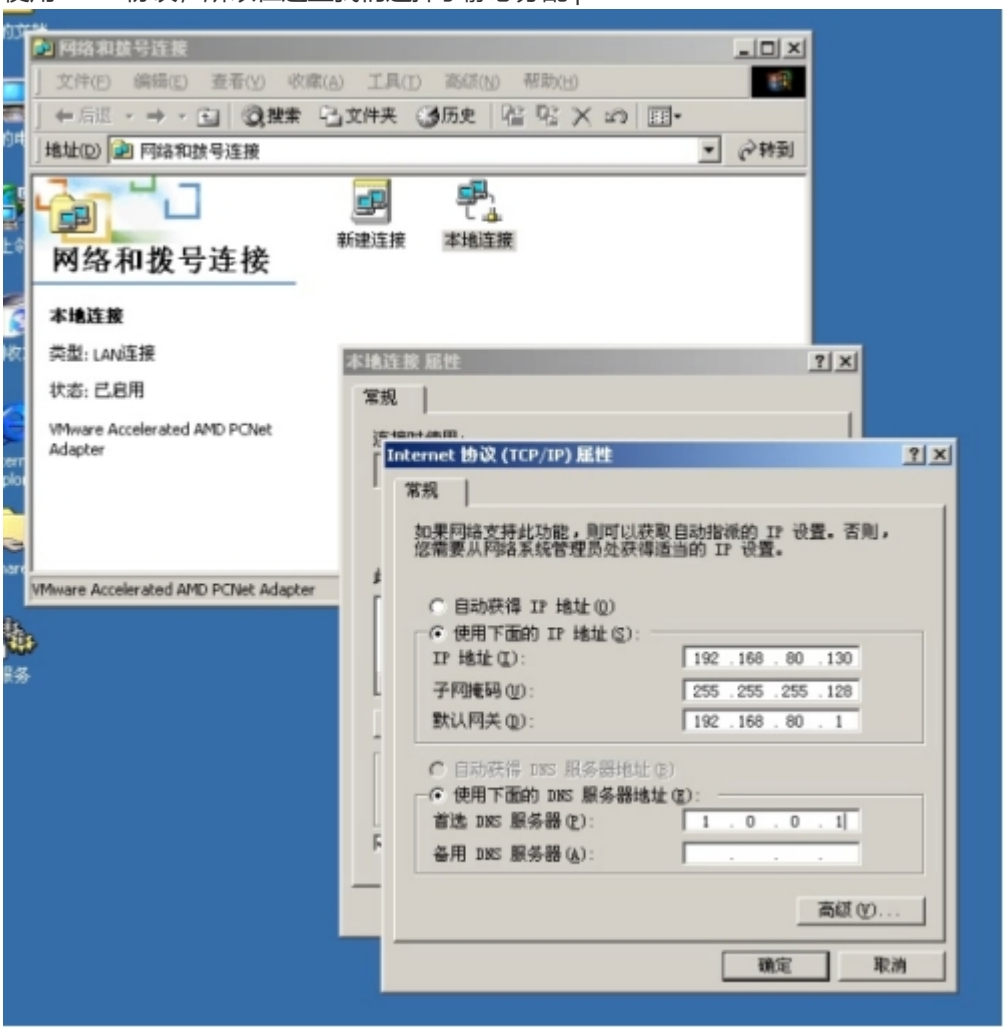
① 网关设置

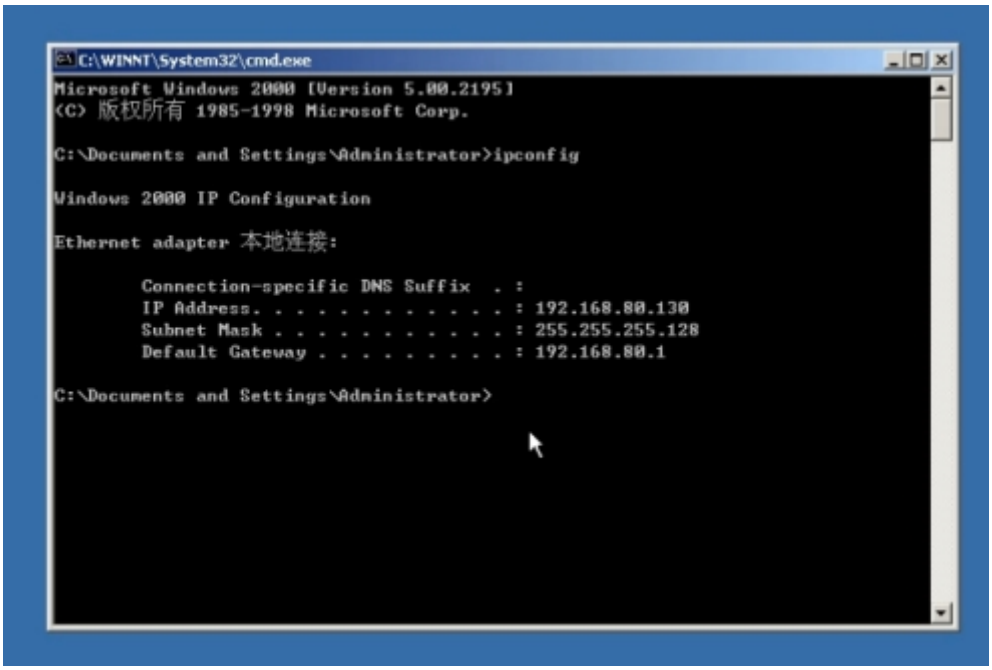
② DHCP分配地址设置



3、设置靶机网络配置（win server）

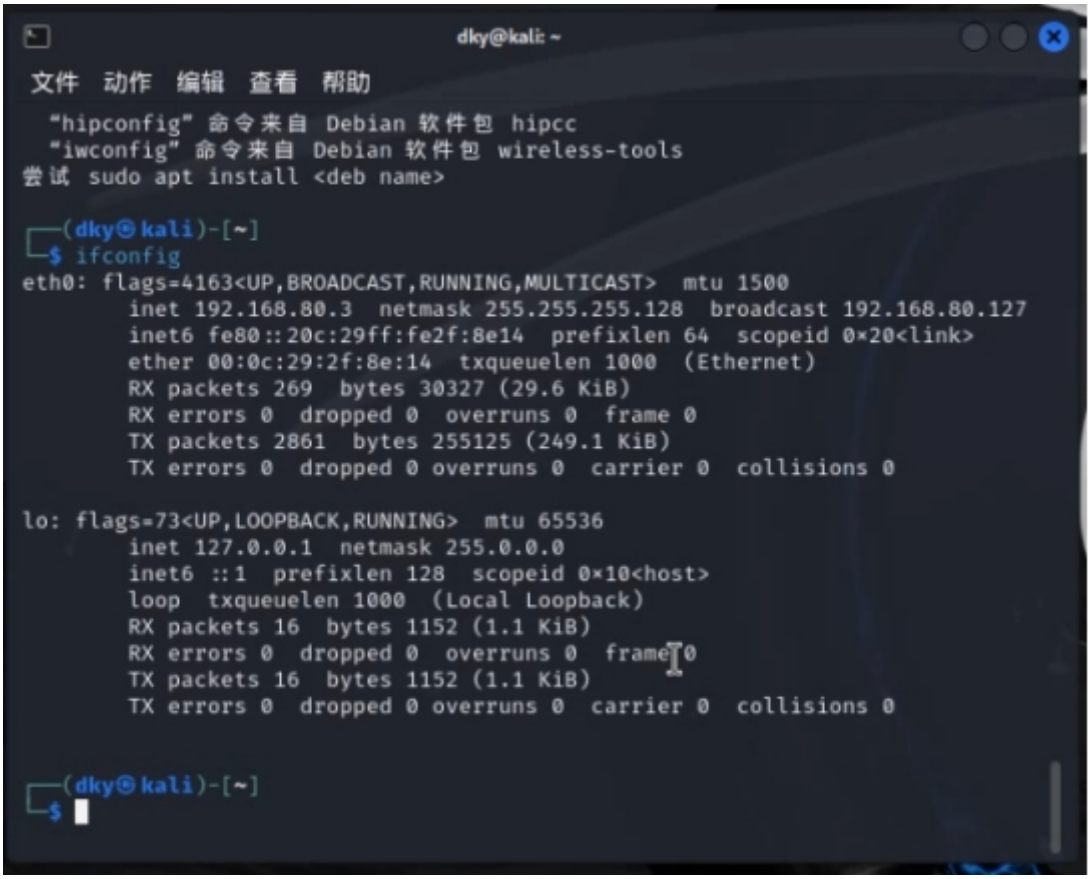
由于靶机位于VMnet1（仅主机网络） 并且因为需要后续固定ip地址（hollywall设置），从而没有使用DHCP协议，所以在这里我们选择了静态分配ip

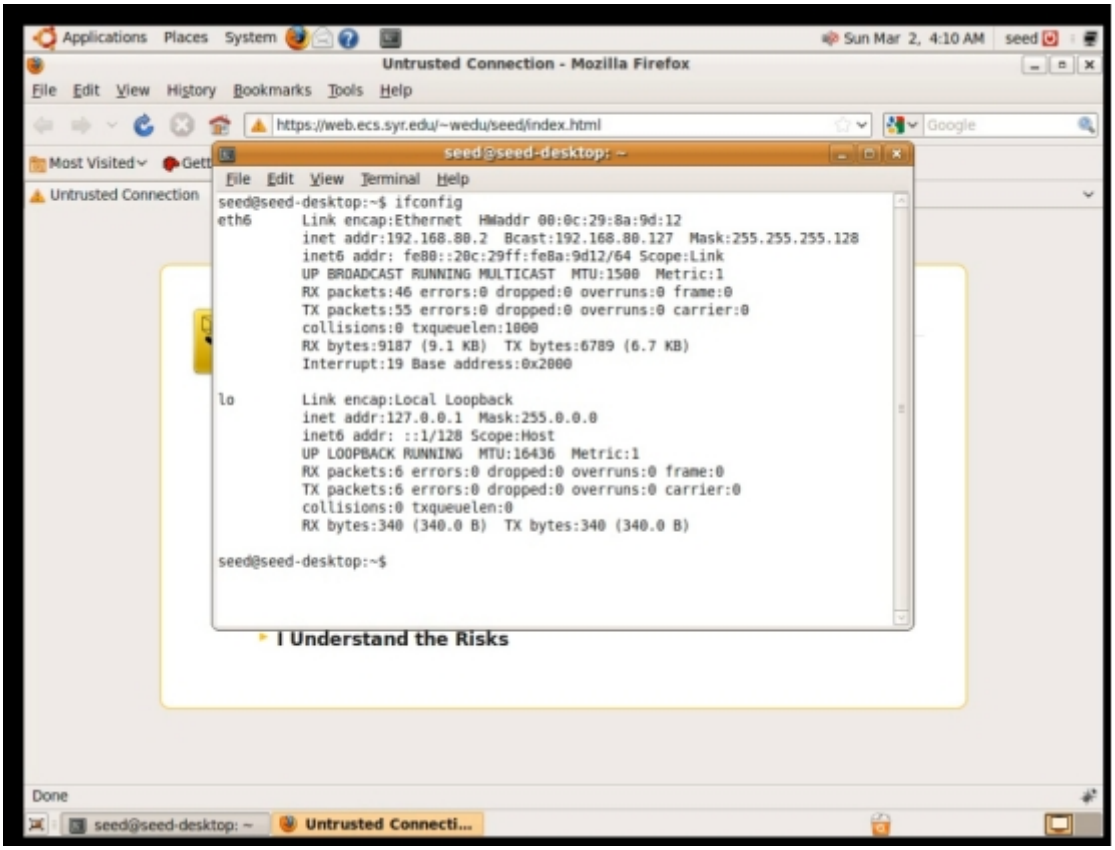




4、攻击机设置（kail和seedubuntu)

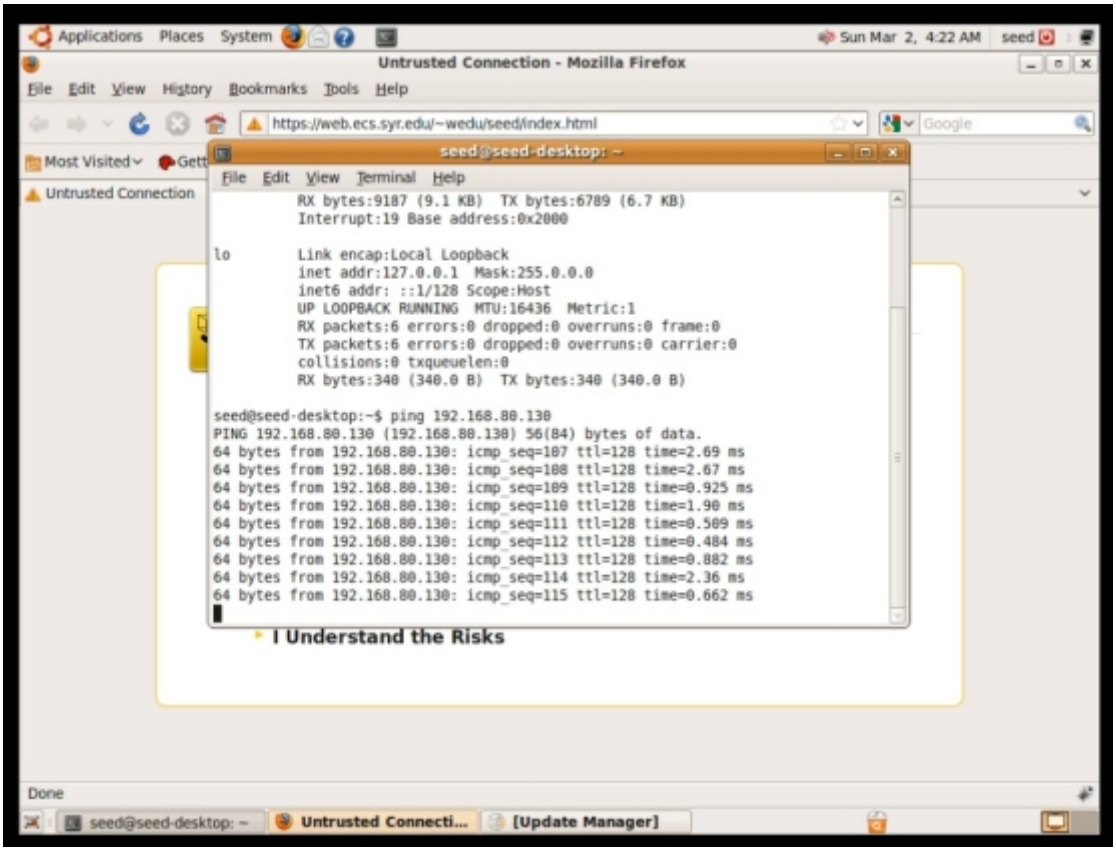
这两台机器都位于vmnet8中，并且选择了dhcp协议，所以我们只需要确定下两台的ip正确分配了即可



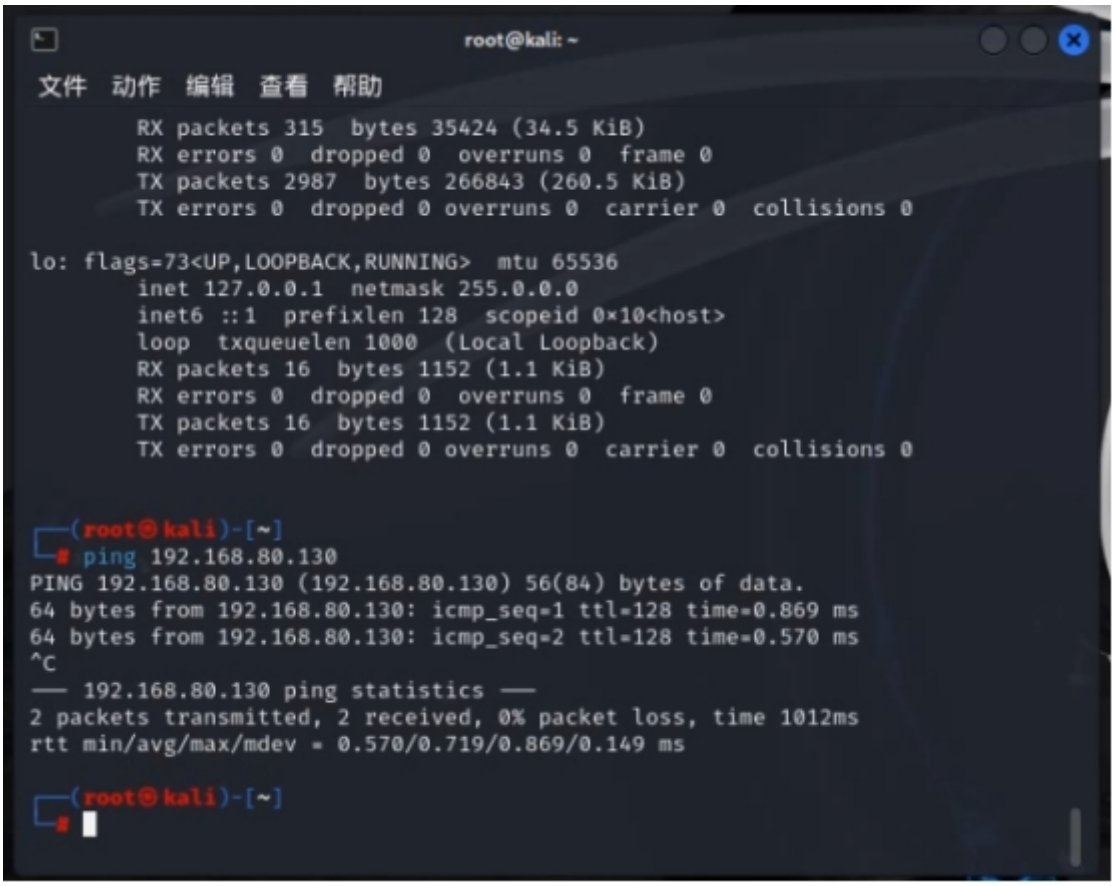


5、使用攻击机攻击靶机

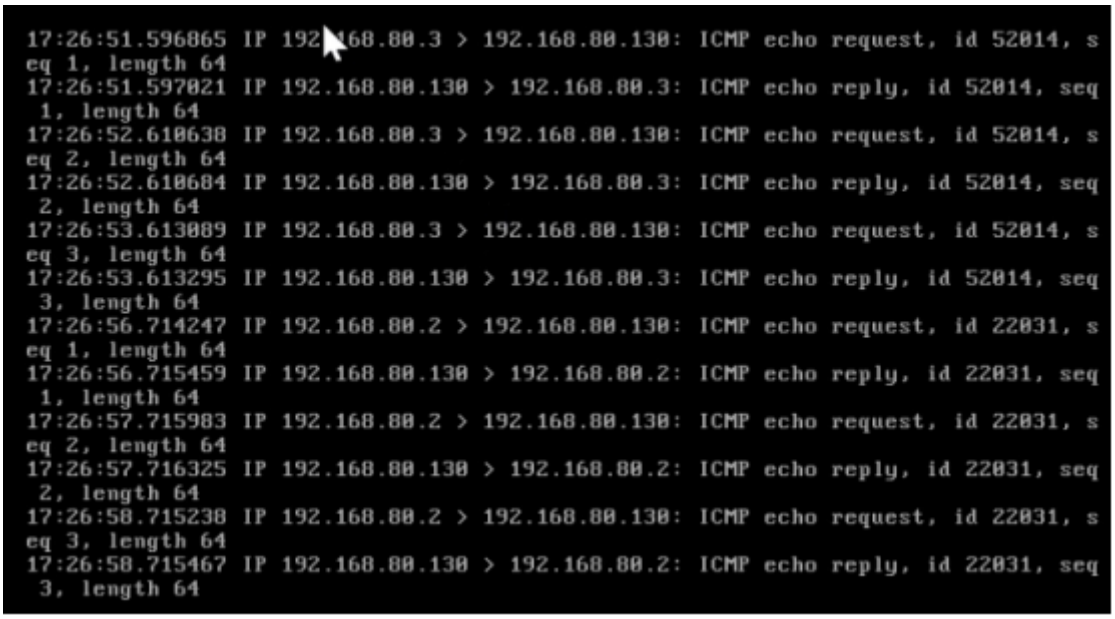
(1) Seed ping win



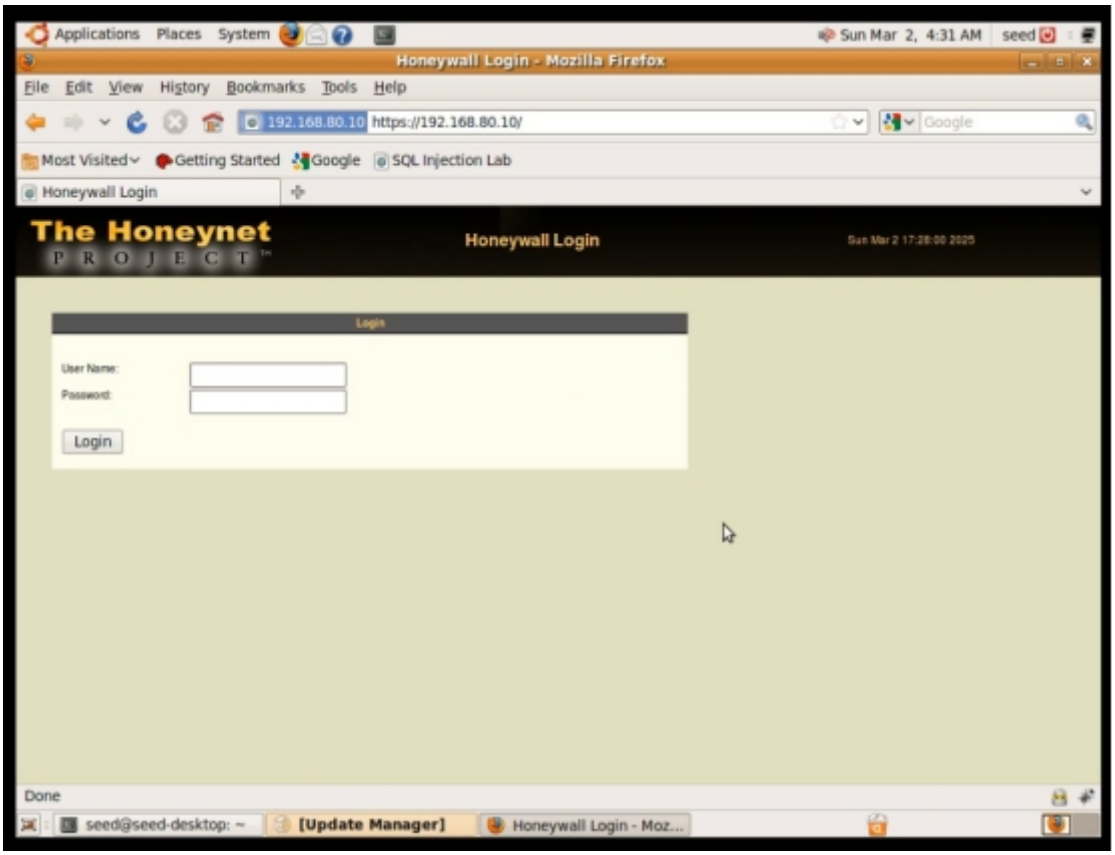
(2) Kail ping win



(3) Honeywall所捕获的信息



(4) Honeywall页面访问



3、总结反思

(1) 学习了桥接模式、NAT模式和仅主机模式的作用和区别，桥接模式可以认为是将虚拟机和物理主机处于相同地位，NAT模式是将虚拟机挂在主机下面，外界看不到虚拟机的ip；仅主机模式比NAT更加封闭，仅主机网络中的主机无法访问外界

(2) 重温了网段相关的知识。

(3) 开始实验的时候在自己电脑vmware上做，做了四五遍一直不通，得出我电脑的vmware workstation可以有问题，遂使用同学的电脑做，成功了。

(4) 全部都设置好后，发现攻击机无法ping通靶机，但在honeywall中发现直接攻击机向靶机的请求icmp，而没有回应icmp，所以我认为问题出现在靶机，检查后发现靶机的网络适配器变成了桥接模式，将其改为仅主机问题，就能成功ping通了。