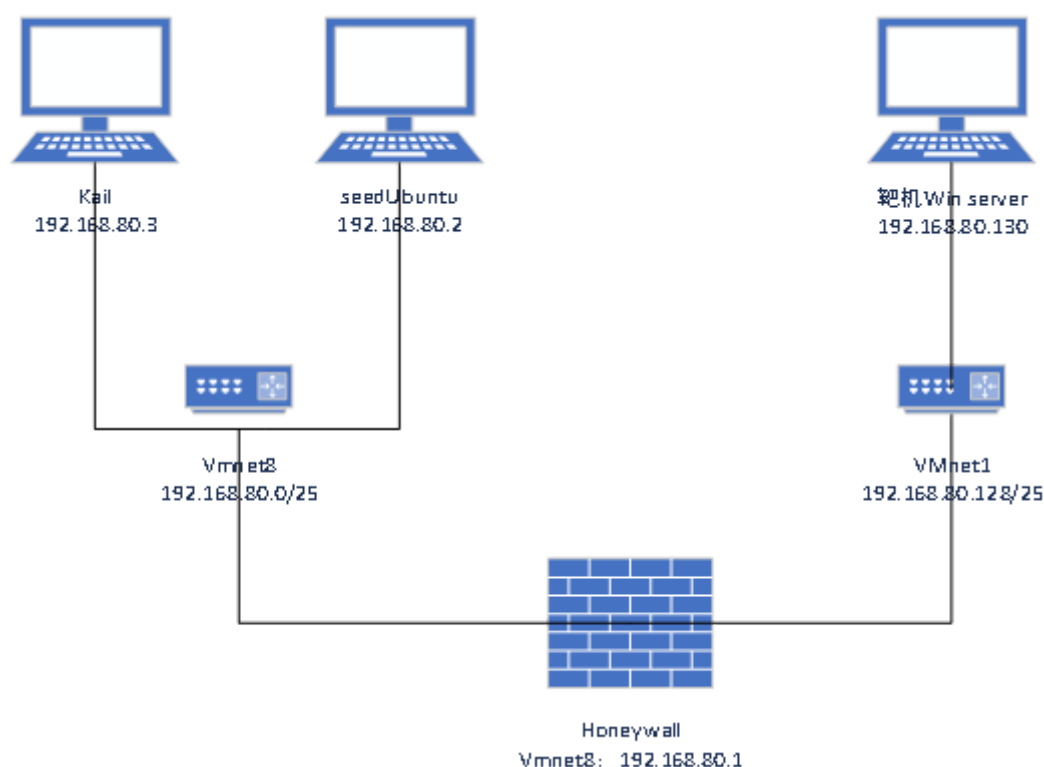


第1次作业-实践一 网络攻防环境的搭建

1、学习总结

本次实验是配置一个用于捕获攻击信息的蜜网。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。

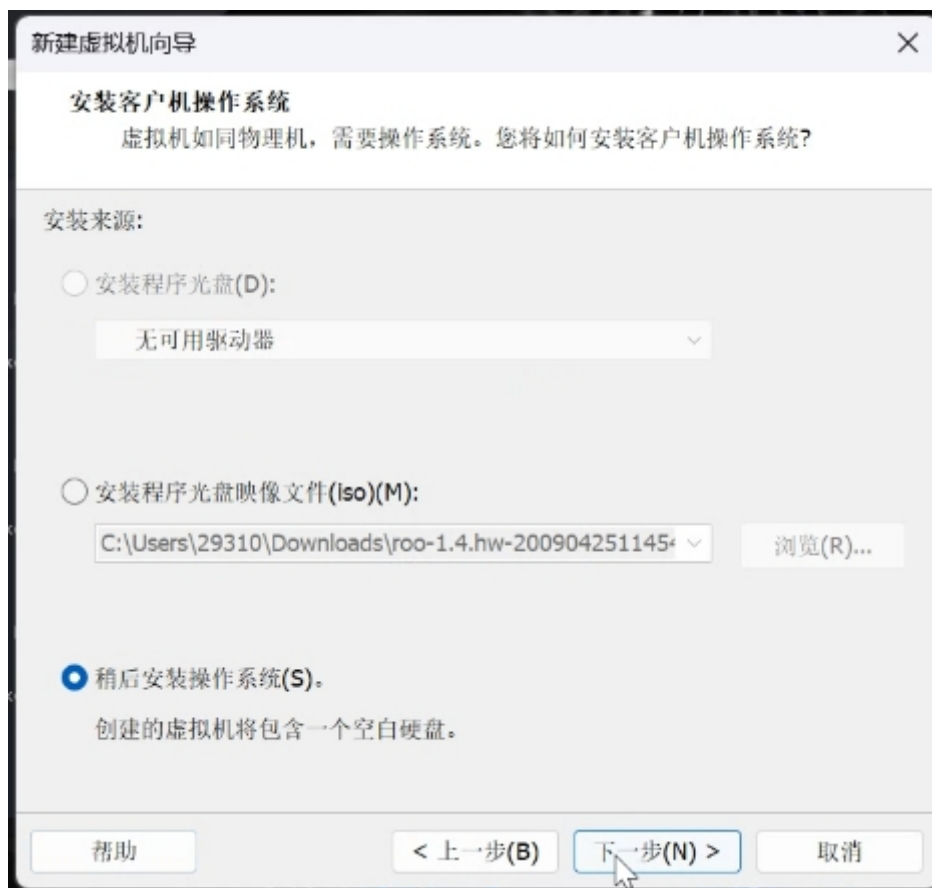
网络流量拓扑图如下（在该拓扑图中，存在攻击机、靶机和蜜罐）



2、搭建详细过程

1、安装honeywall

(1) 选择稍后安装操作系统



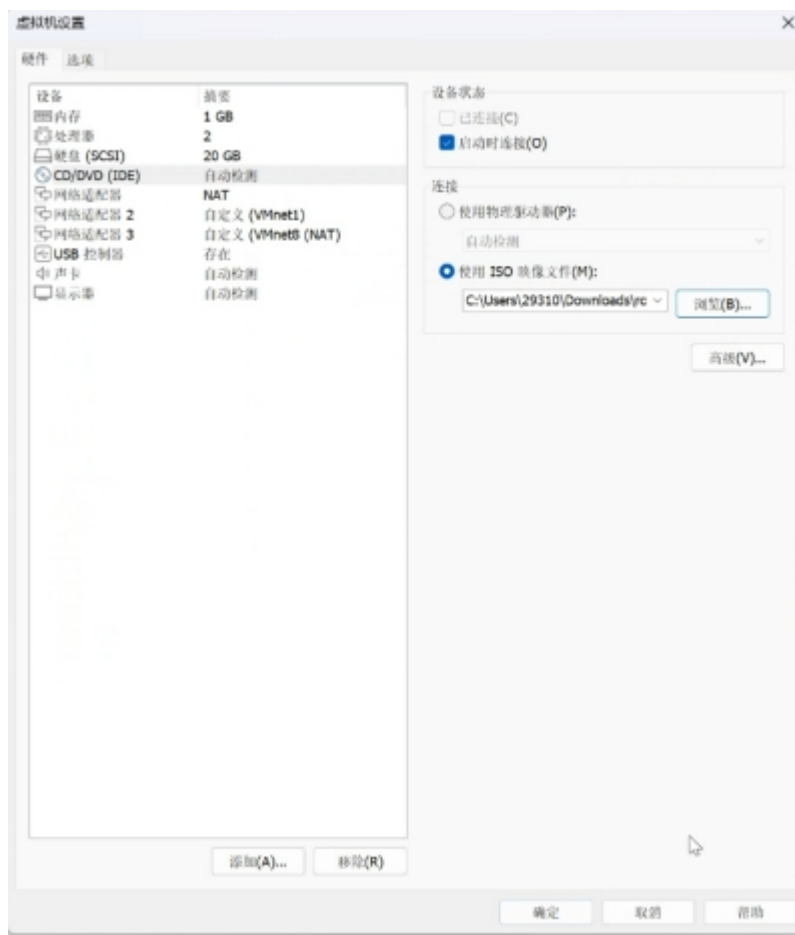
(2) 版本选择Centos5和更早版本



(3) 设置holleywall的网络适配器，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

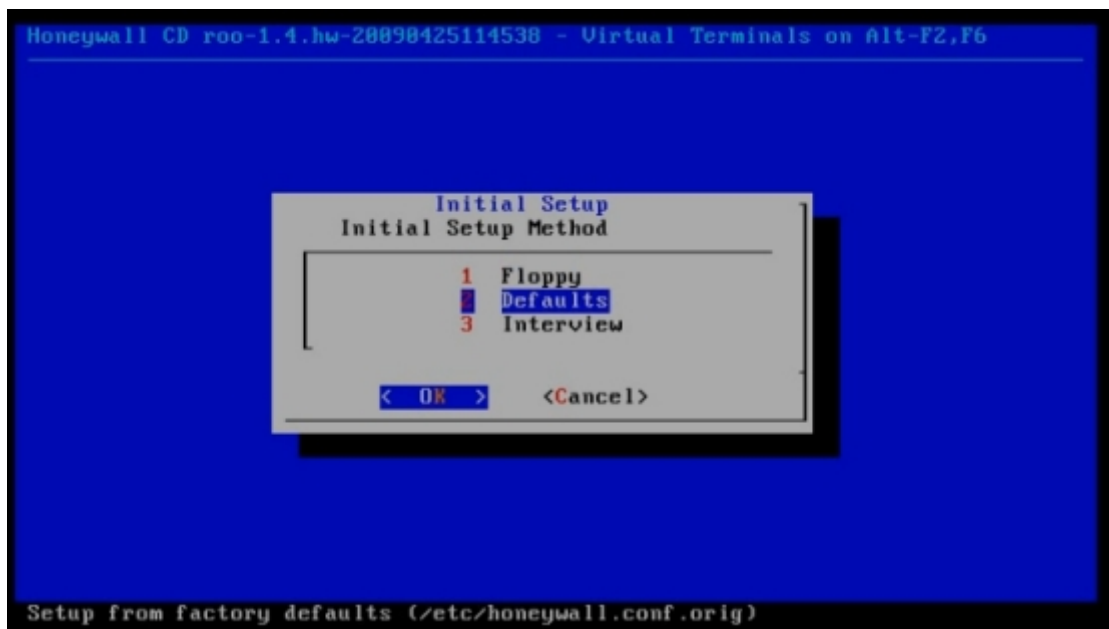


(1) 配置hollywall

- 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

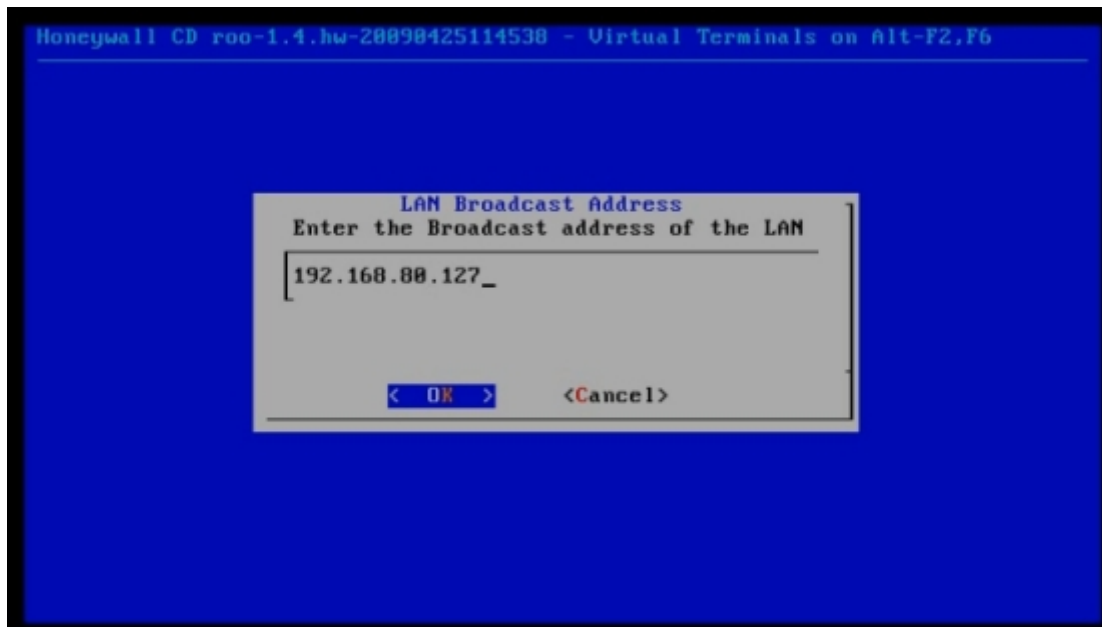


④ 选择第四项，然后开始配置靶机ip和honeywall在vmnet中的信息

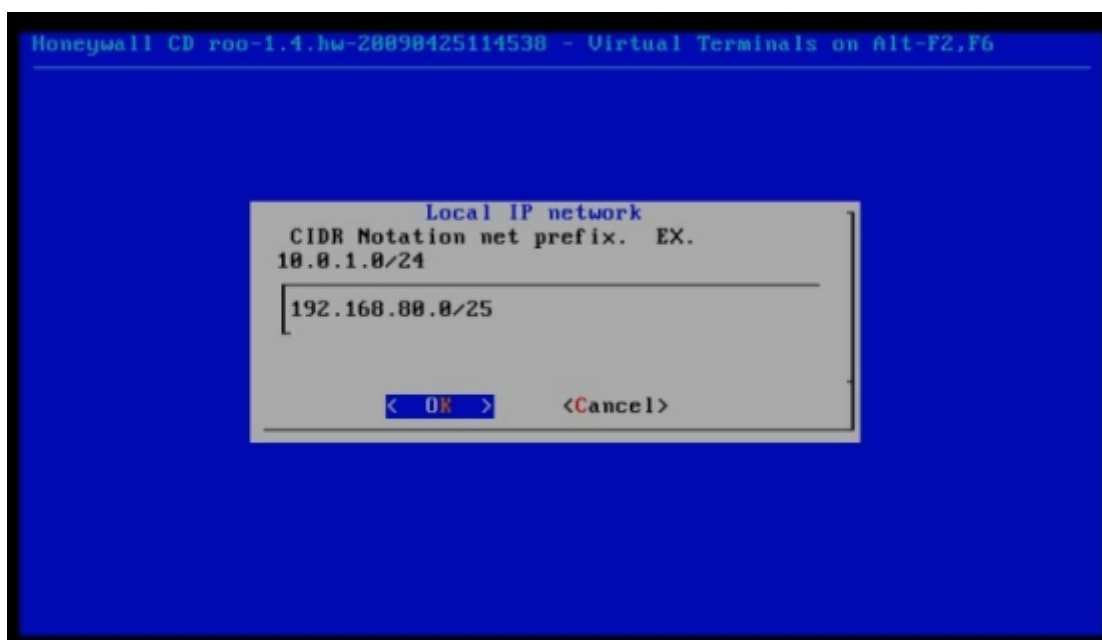
(1) 靶机ip配置



(2) Vmnet8广播地址设置

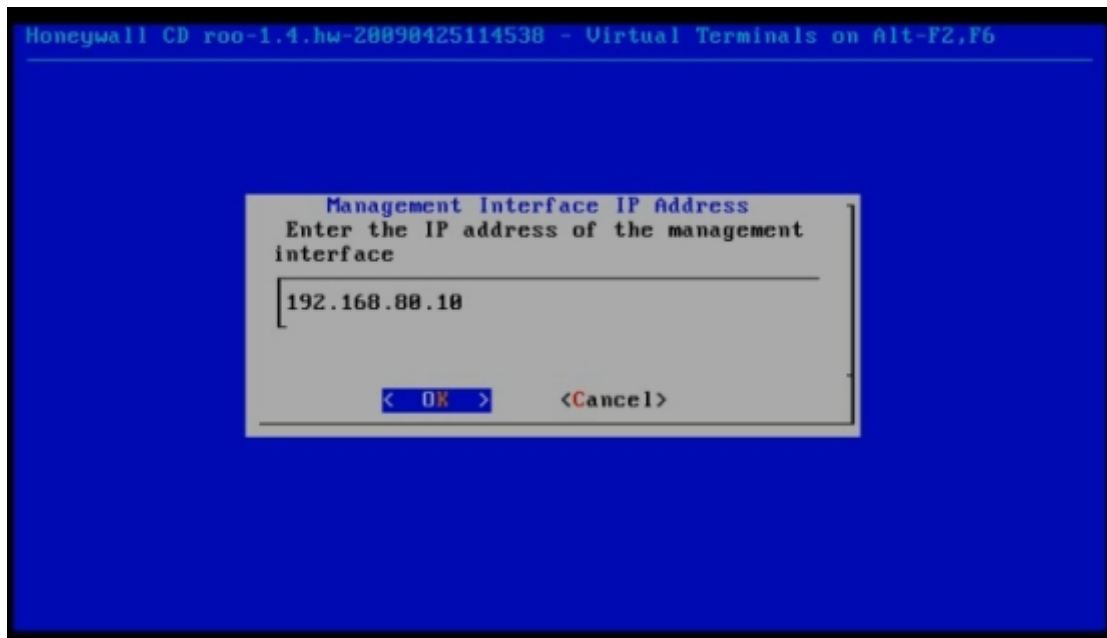


(3) VMnet网段设置

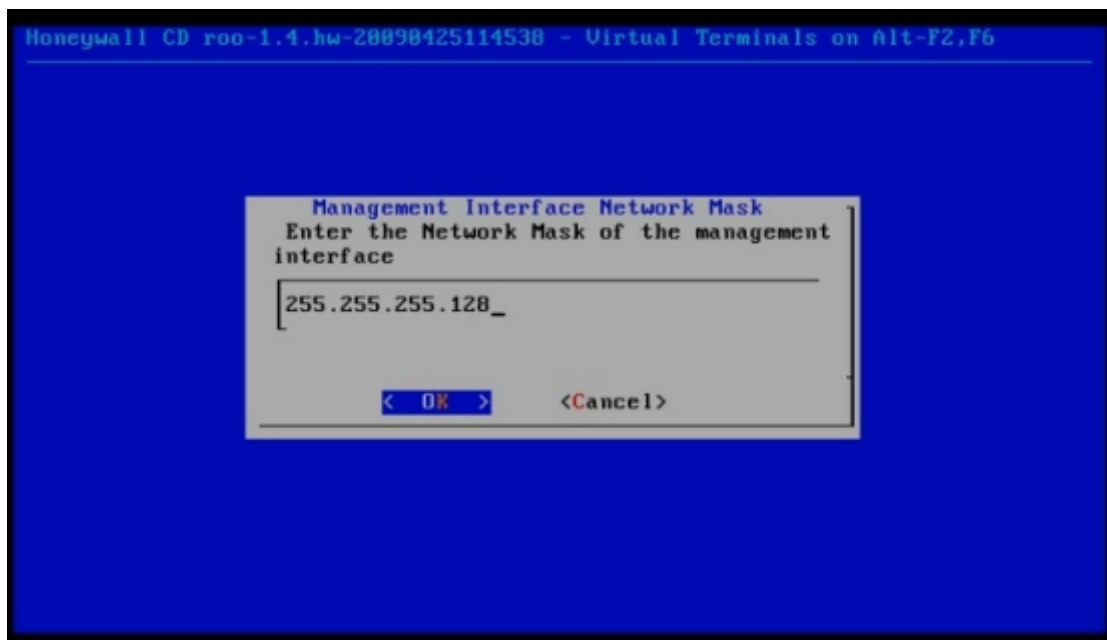


⑤ 远程IP地址设置

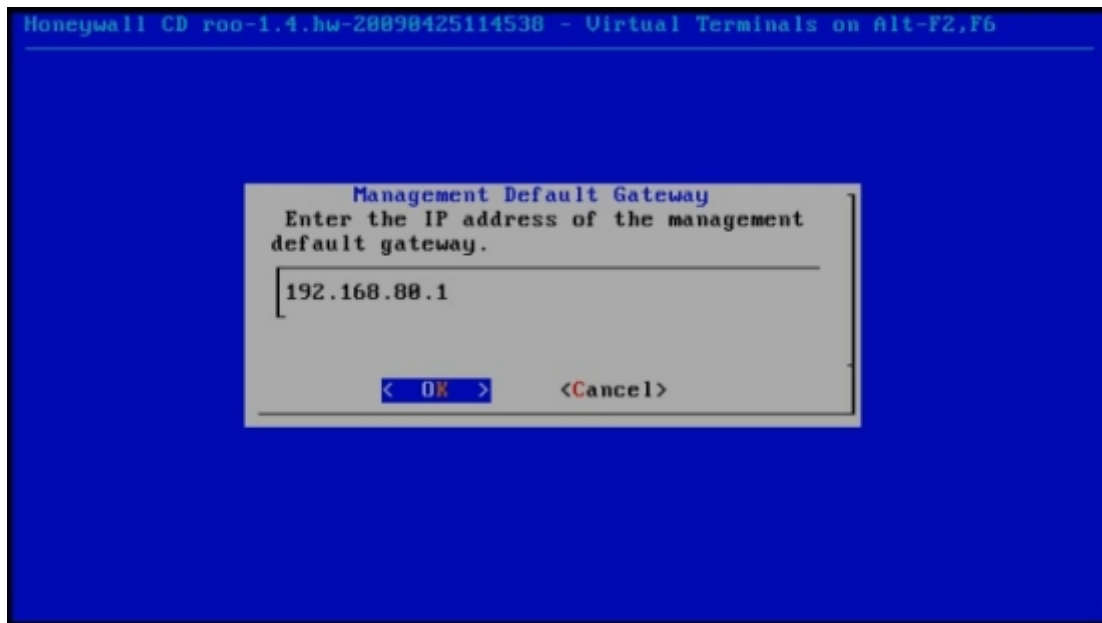
(1) Honeywall IP地址设置



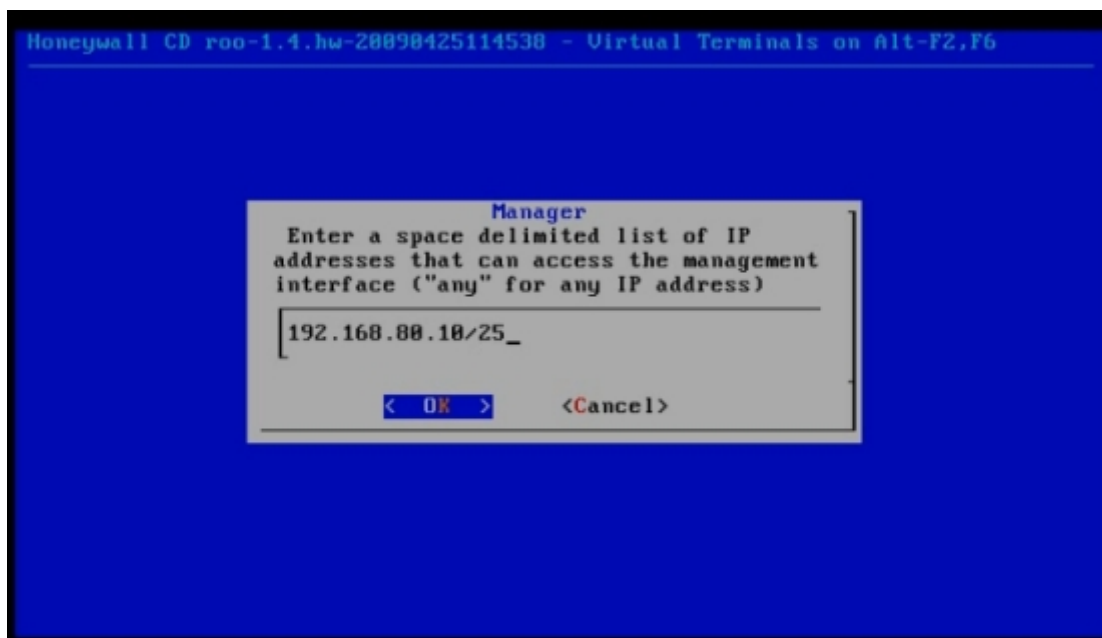
(2) 设置子网掩码



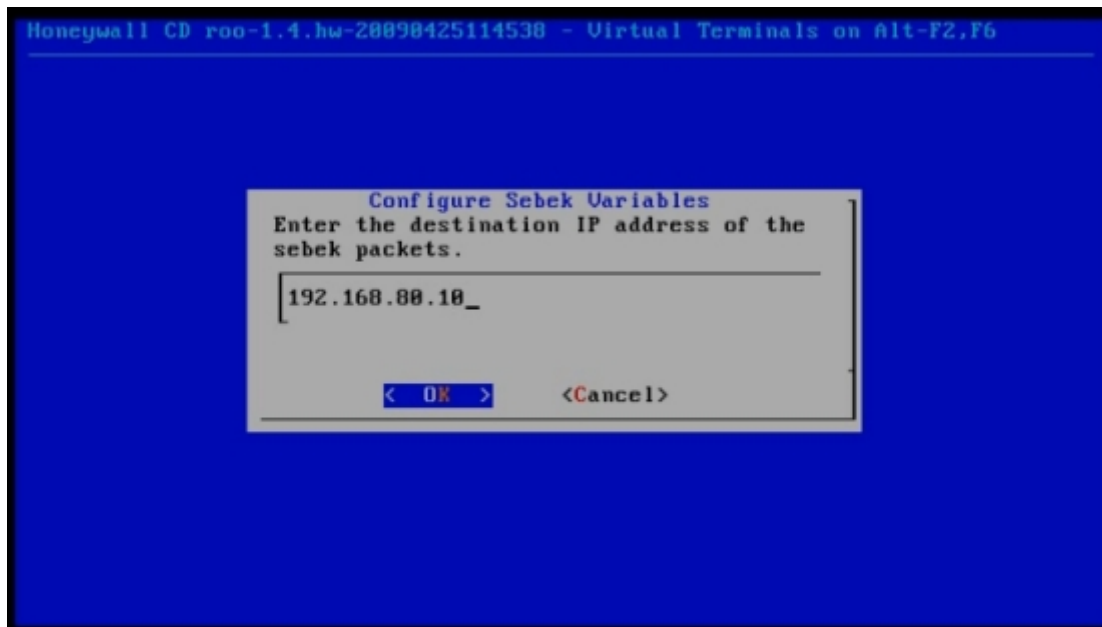
(3) 设置vmnet的网关



(4) 设置可通信的网段



(4) 设置sebek的ip地址



(6) 结束, 查看ip

```
UP BROADCAST RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1736 (1.6 KiB) TX bytes:1806 (1.8 KiB)
Interrupt:75 Base address:0x2080

eth2    Link encap:Ethernet HWaddr 00:0C:29:DD:72:A4
        inet addr:192.168.88.10 Bcast:192.168.88.127 Mask:255.255.255.128
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:60 (60.0 b) TX bytes:0 (0.0 b)
        Interrupt:67 Base address:0x2400

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

[root@localhost ~]# _
```

2、设置虚拟网络编辑器

(1) VMnet1设置

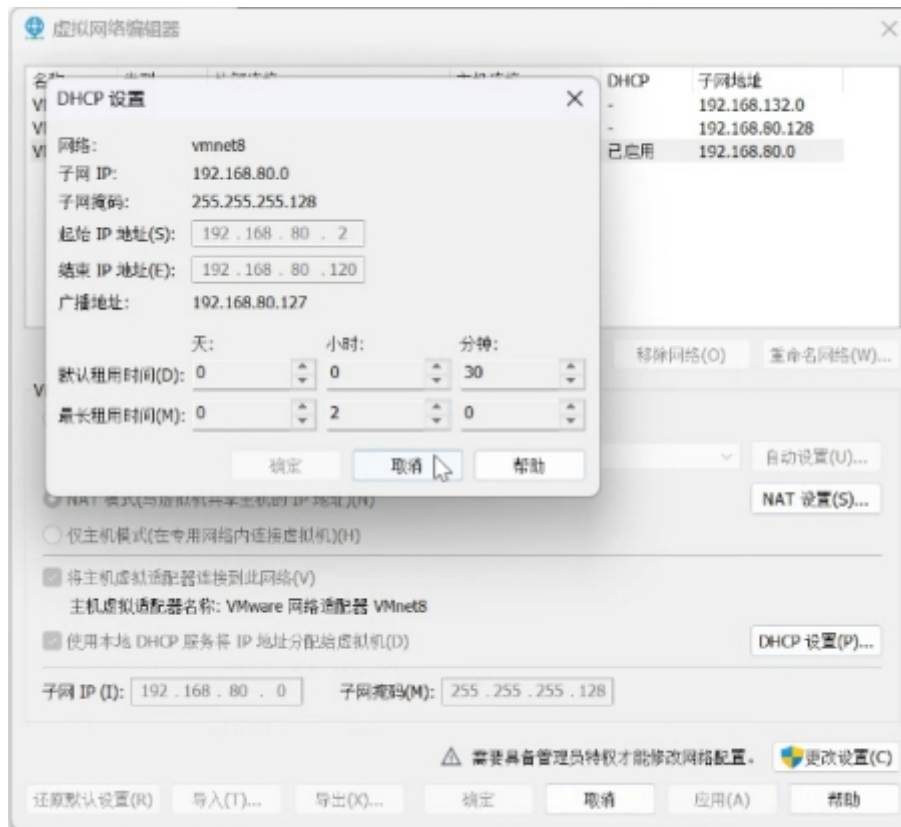


(2) 设置VMnet8设置

① 网关设置

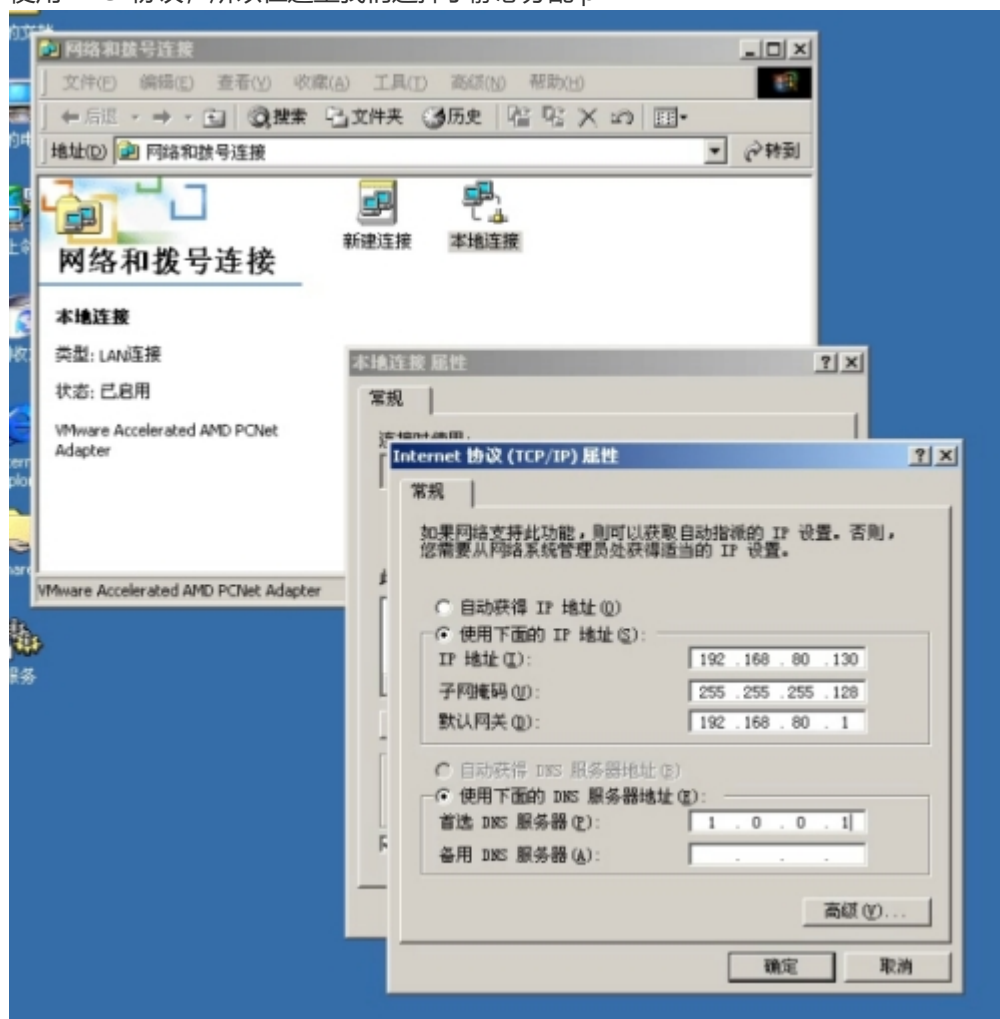


② DHCP分配地址设置



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



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.80.130
    Subnet Mask . . . . .             : 255.255.255.128
    Default Gateway . . . . .         : 192.168.80.1

C:\Documents and Settings\Administrator>
```

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

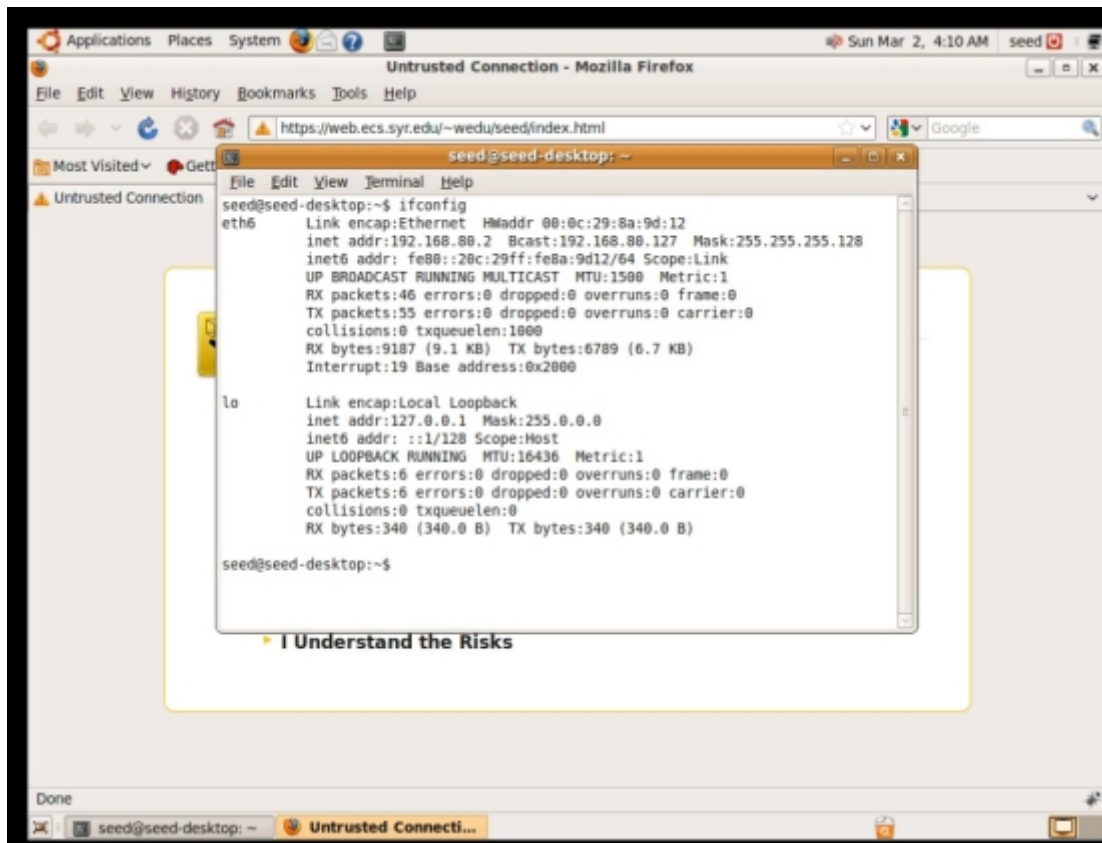
```
dky@kali: ~
文件 动作 编辑 查看 帮助

“hipconfig”命令来自 Debian 软件包 hipcc
“iwconfig”命令来自 Debian 软件包 wireless-tools
尝试 sudo apt install <deb name>

(dky@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.80.3 netmask 255.255.255.128 broadcast 192.168.80.127
    inet6 fe80::20c:29ff:fe2f:8e14 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:2f:8e:14 txqueuelen 1000 (Ethernet)
    RX packets 269 bytes 30327 (29.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2861 bytes 255125 (249.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

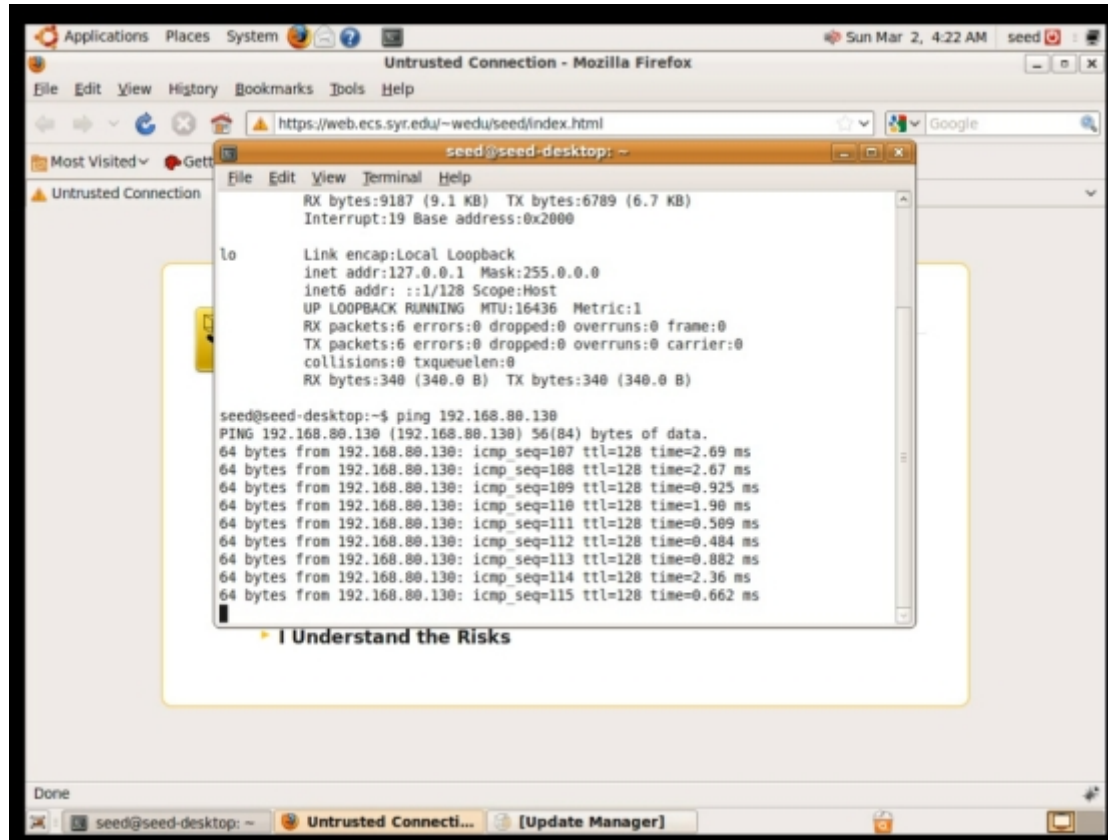
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 1152 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1152 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(dky@kali)-[~]
$
```



5、使用攻击机攻击靶机

(1) Seed ping win



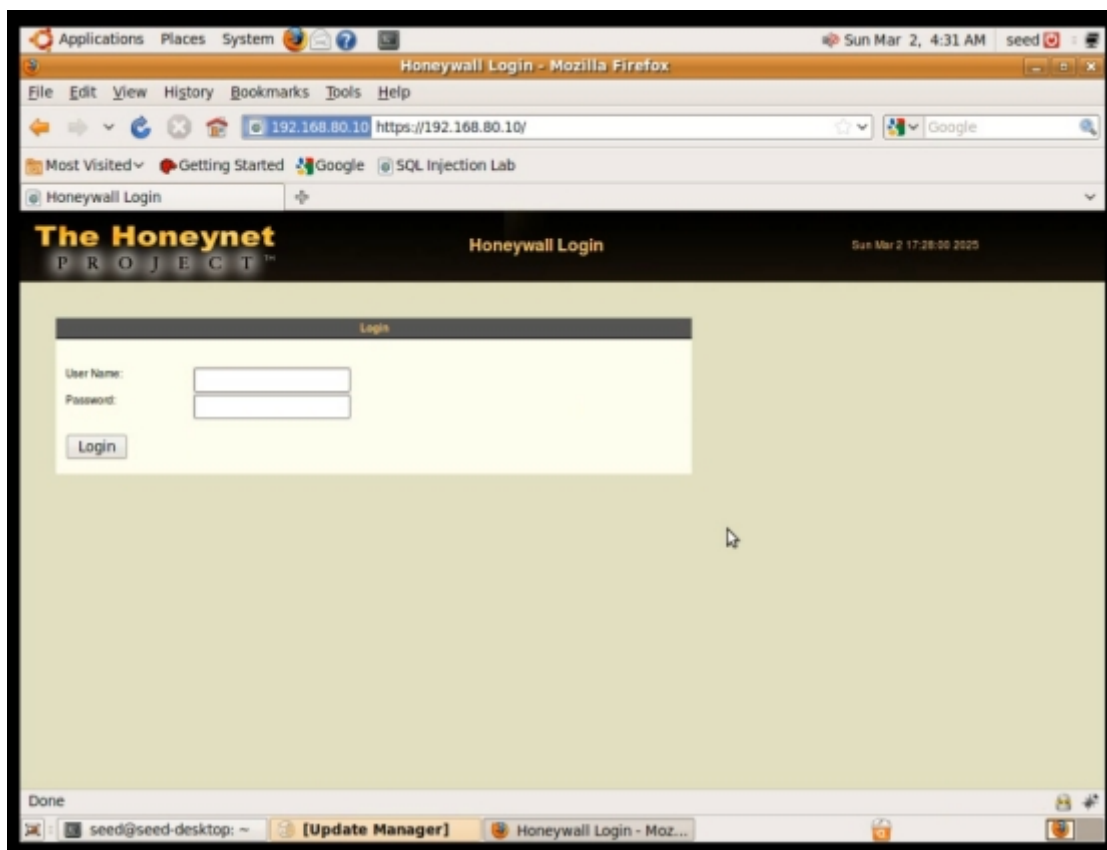
(2) Kail ping win

```
root@kali: ~  
文件 动作 编辑 查看 帮助  
RX packets 315  bytes 35424 (34.5 KiB)  
RX errors 0  dropped 0  overruns 0  frame 0  
TX packets 2987  bytes 266843 (260.5 KiB)  
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
inet 127.0.0.1  netmask 255.0.0.0  
inet6 ::1  prefixlen 128  scopeid 0<host>  
loop txqueuelen 1000  (Local Loopback)  
RX packets 16  bytes 1152 (1.1 KiB)  
RX errors 0  dropped 0  overruns 0  frame 0  
TX packets 16  bytes 1152 (1.1 KiB)  
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
  
(root@kali)-[~]  
# ping 192.168.80.130  
PING 192.168.80.130 (192.168.80.130) 56(84) bytes of data.  
64 bytes from 192.168.80.130: icmp_seq=1 ttl=128 time=0.869 ms  
64 bytes from 192.168.80.130: icmp_seq=2 ttl=128 time=0.570 ms  
^C  
— 192.168.80.130 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1012ms  
rtt min/avg/max/mdev = 0.570/0.719/0.869/0.149 ms  
  
(root@kali)-[~]  
#
```

(3) Honeywall所捕获的信息

```
17:26:51.596865 IP 192.168.80.3 > 192.168.80.130: ICMP echo request, id 52014, s  
eq 1, length 64  
17:26:51.597021 IP 192.168.80.130 > 192.168.80.3: ICMP echo reply, id 52014, seq  
1, length 64  
17:26:52.610638 IP 192.168.80.3 > 192.168.80.130: ICMP echo request, id 52014, s  
eq 2, length 64  
17:26:52.610684 IP 192.168.80.130 > 192.168.80.3: ICMP echo reply, id 52014, seq  
2, length 64  
17:26:53.613089 IP 192.168.80.3 > 192.168.80.130: ICMP echo request, id 52014, s  
eq 3, length 64  
17:26:53.613295 IP 192.168.80.130 > 192.168.80.3: ICMP echo reply, id 52014, seq  
3, length 64  
17:26:56.714247 IP 192.168.80.2 > 192.168.80.130: ICMP echo request, id 22031, s  
eq 1, length 64  
17:26:56.715459 IP 192.168.80.130 > 192.168.80.2: ICMP echo reply, id 22031, seq  
1, length 64  
17:26:57.715983 IP 192.168.80.2 > 192.168.80.130: ICMP echo request, id 22031, s  
eq 2, length 64  
17:26:57.716325 IP 192.168.80.130 > 192.168.80.2: ICMP echo reply, id 22031, seq  
2, length 64  
17:26:58.715238 IP 192.168.80.2 > 192.168.80.130: ICMP echo request, id 22031, s  
eq 3, length 64  
17:26:58.715467 IP 192.168.80.130 > 192.168.80.2: ICMP echo reply, id 22031, seq  
3, length 64
```

(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。