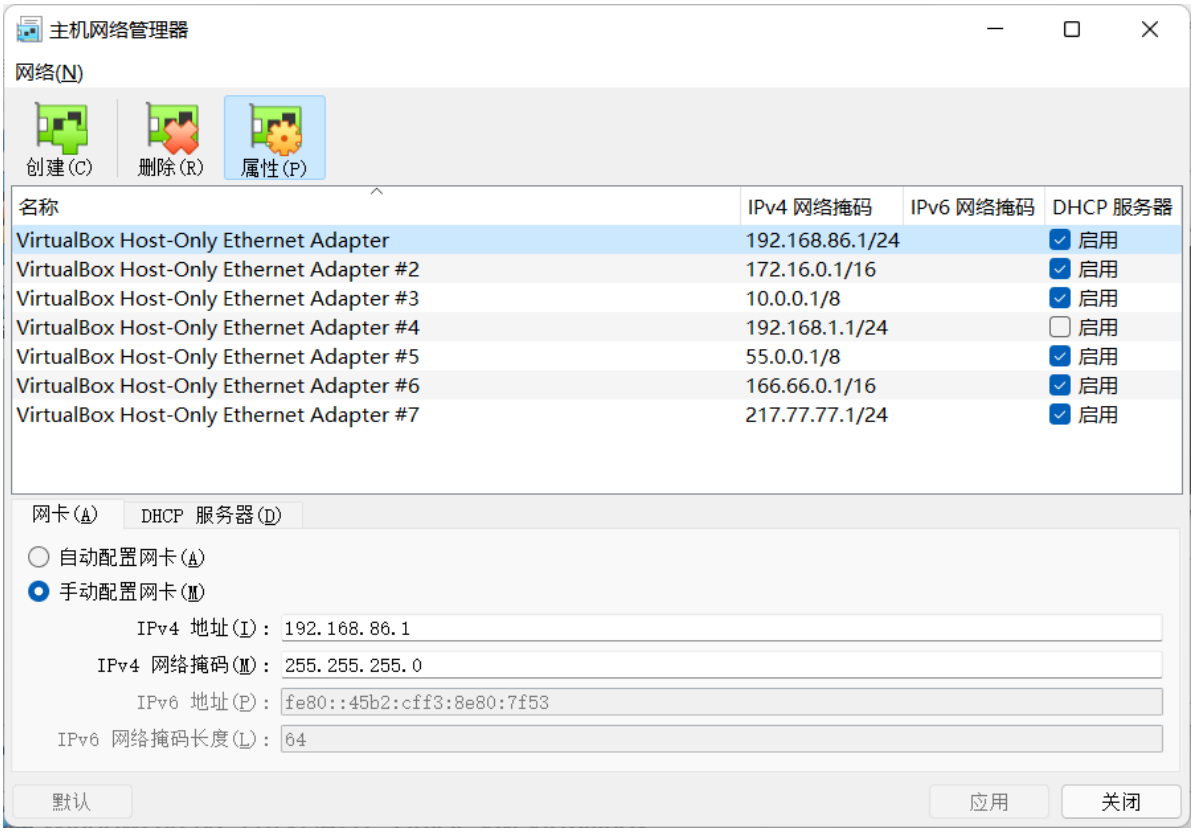
信息安全导论第一次实验

PB19051183 吴承泽

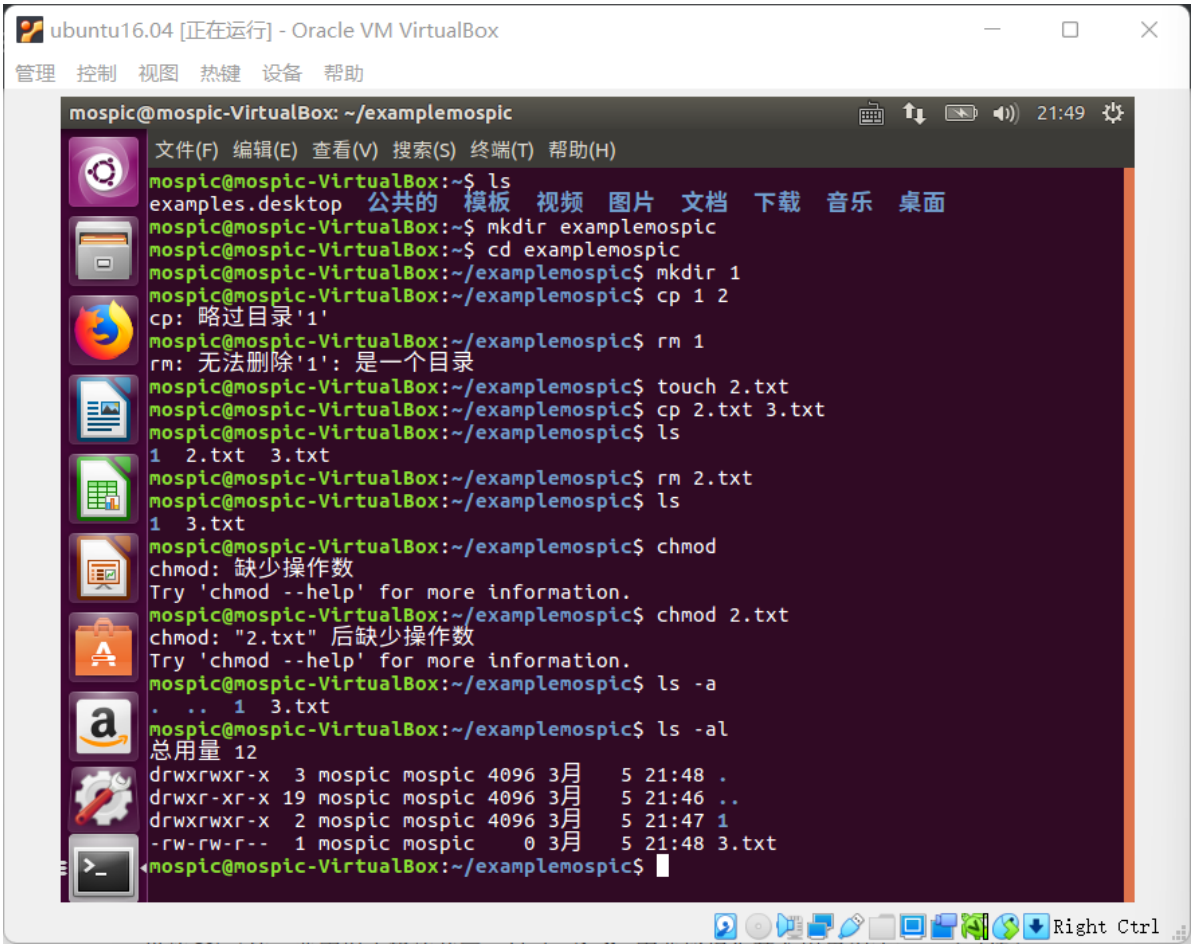
1.3

安装好Virtualbox并且导入新建好两个虚拟机后的界面如下：

修改主机网络管理器，配置虚拟网卡，新建7个以太网，并修改其IP地址与子网掩码后如下显示：



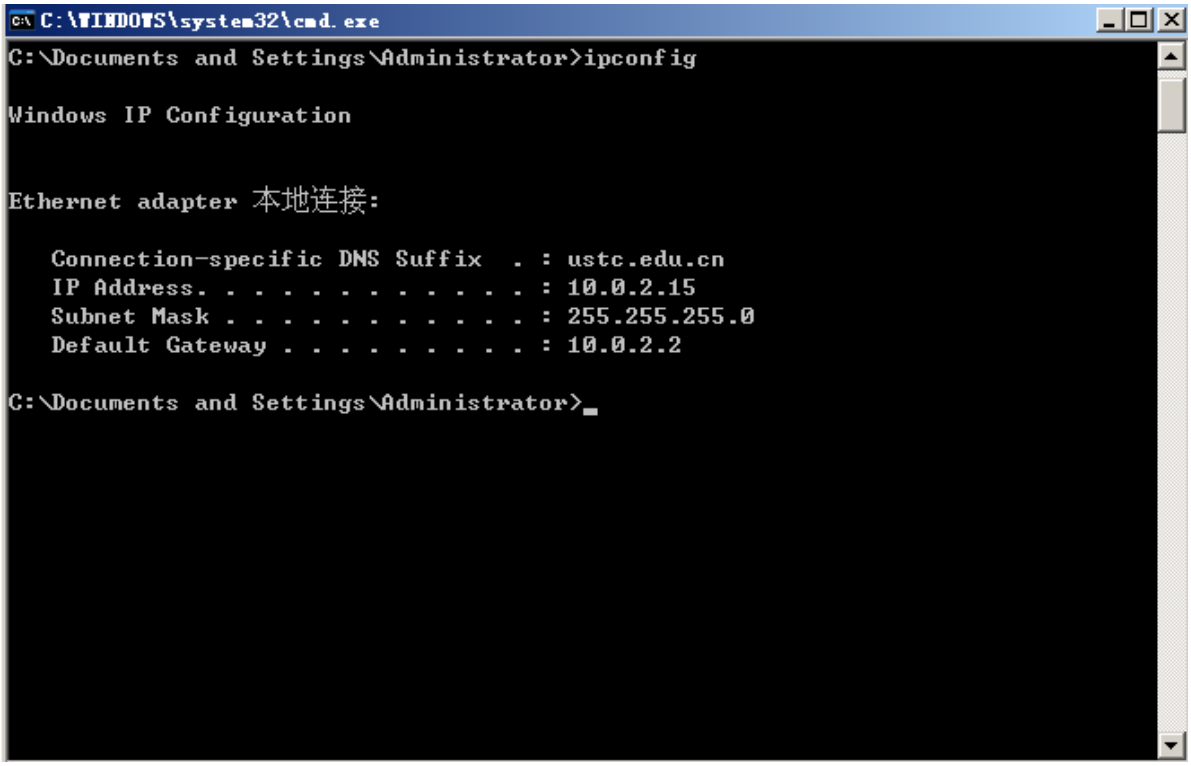
进入Ubuntu虚拟机后，运行常用命令如下：




```
mospic@mospic-VirtualBox:~/examplemospic$ ifconfig
enp0s3    Link encap:以太网  硬件地址 08:00:27:be:6a:c1
          inet 地址:192.168.56.103  广播:192.168.56.255  掩码:255.255.255.0
          inet6 地址: fe80::8f6:a535:277b:e0b4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
          接收数据包:1826 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:3761 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:1000
          接收字节:170841 (170.8 KB)  发送字节:264138 (264.1 KB)

lo        Link encap:本地环回
          inet 地址:127.0.0.1  掩码:255.0.0.0
          inet6 地址: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  跃点数:1
          接收数据包:30295 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:30295 错误:0 丢弃:0 过载:0 载波:0
          碰撞:0 发送队列长度:1000
          接收字节:2065314 (2.0 MB)  发送字节:2065314 (2.0 MB)
```

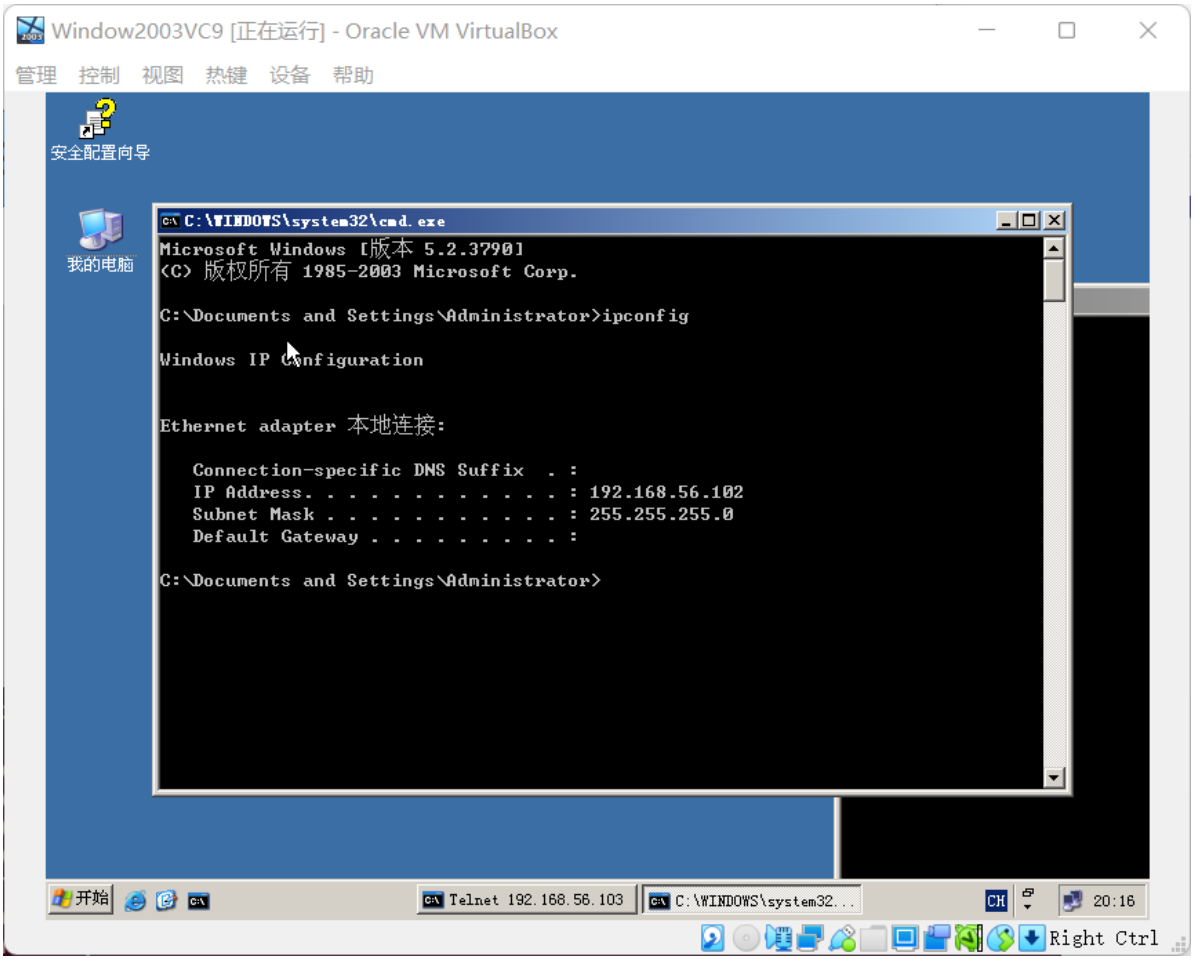
在Windows虚拟机中，试着使用常见的命令得到一些结果：



1.5

(1) 用 ubuntu 虚拟机中的网络侦察工具 nmap（如果没有，安装一个）查看已下载的 Windows 2003 虚拟机中开放了哪些网络端口，用 nmap 探测 Windows 2003 虚拟机的操作系统类型。

在Windows2003虚拟机中调出命令控制符，输入ipconfig得到分配的IP address为**192.168.56.102**。

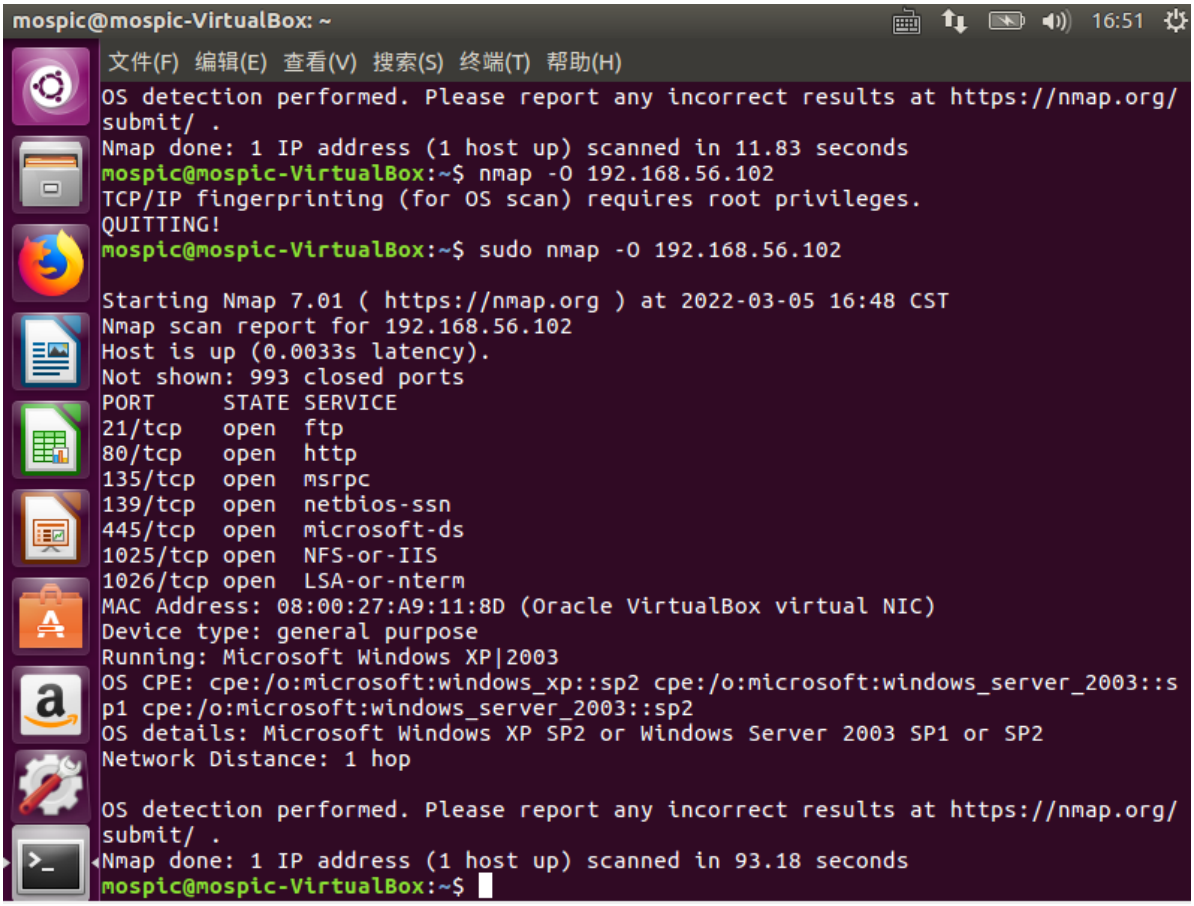


在Ubuntu虚拟机，通过指令`sudo nmap -O 192.168.56.102`，查看得到Windows虚拟机中的一些开放端口，如下图显示：

端口有：

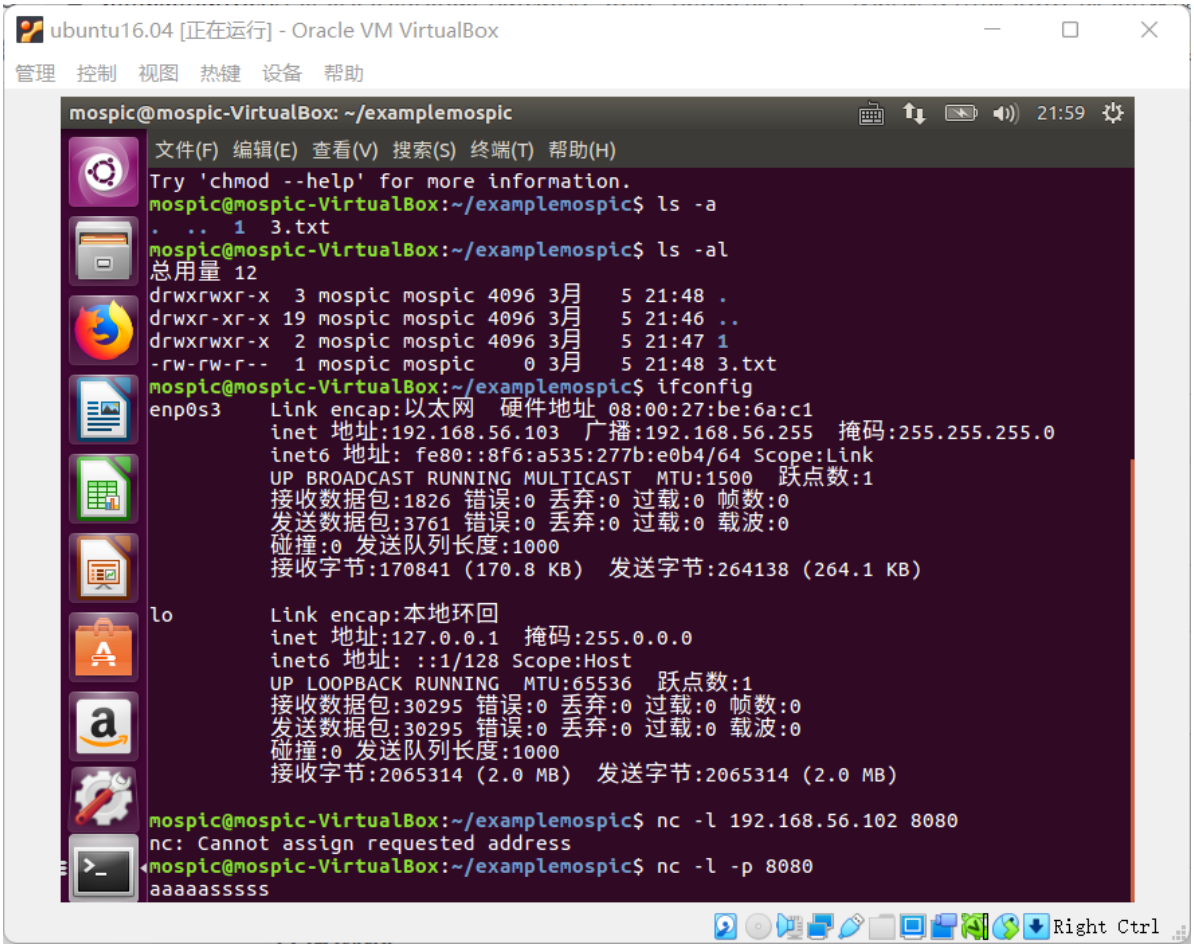
- 21
- 80
- 135
- 139
- 445
- 1025
- 1026

在该MAC地址上运行的操作系统为**Microsoft Windows XP|2003**，符合实际情况。



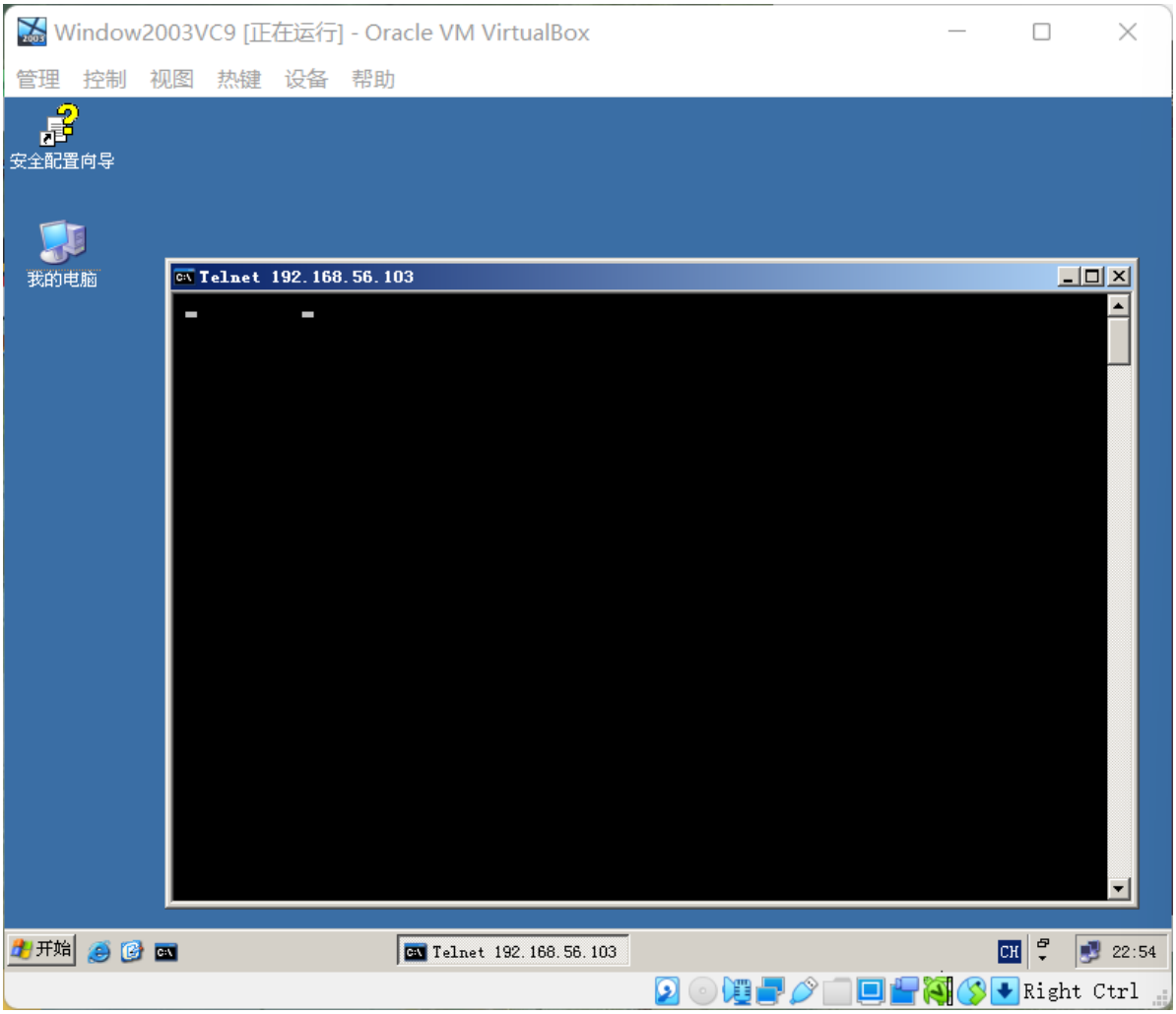
(2) 在 ubuntu 虚拟机中用经典的网络安全工具 netcat 在本机开启一个监听端口，实现远程木马的功能。

通过指令`nc -l -p 8080`监听本机的8080端口如下：



在Windows虚拟机中，通过指令`telnet 192.168.56.103 8080`，测试该端口，在打开的Telnet命令控制符窗口内，输入一些字符，会一次在Ubuntu中的监听窗口中打出来，如上图所示：

在Windows虚拟机中，窗口中的如下，在里面输入aaaaasssss，最后在Ubuntu虚拟机中出现一样的字符串，如上面所示：



可见在Ubuntu虚拟机中实现了监听主机通信的功能。