

信息安全导论第一次实验

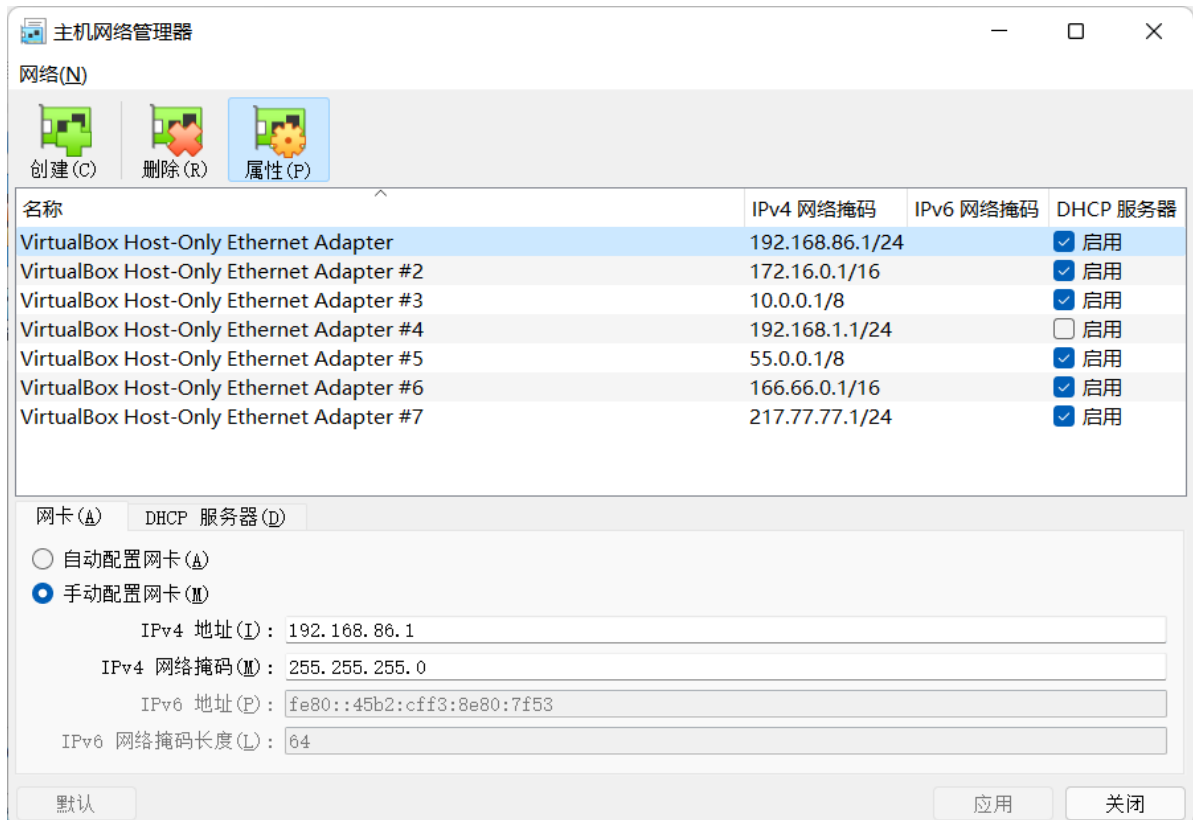
PB19051183 吴承泽

1.3

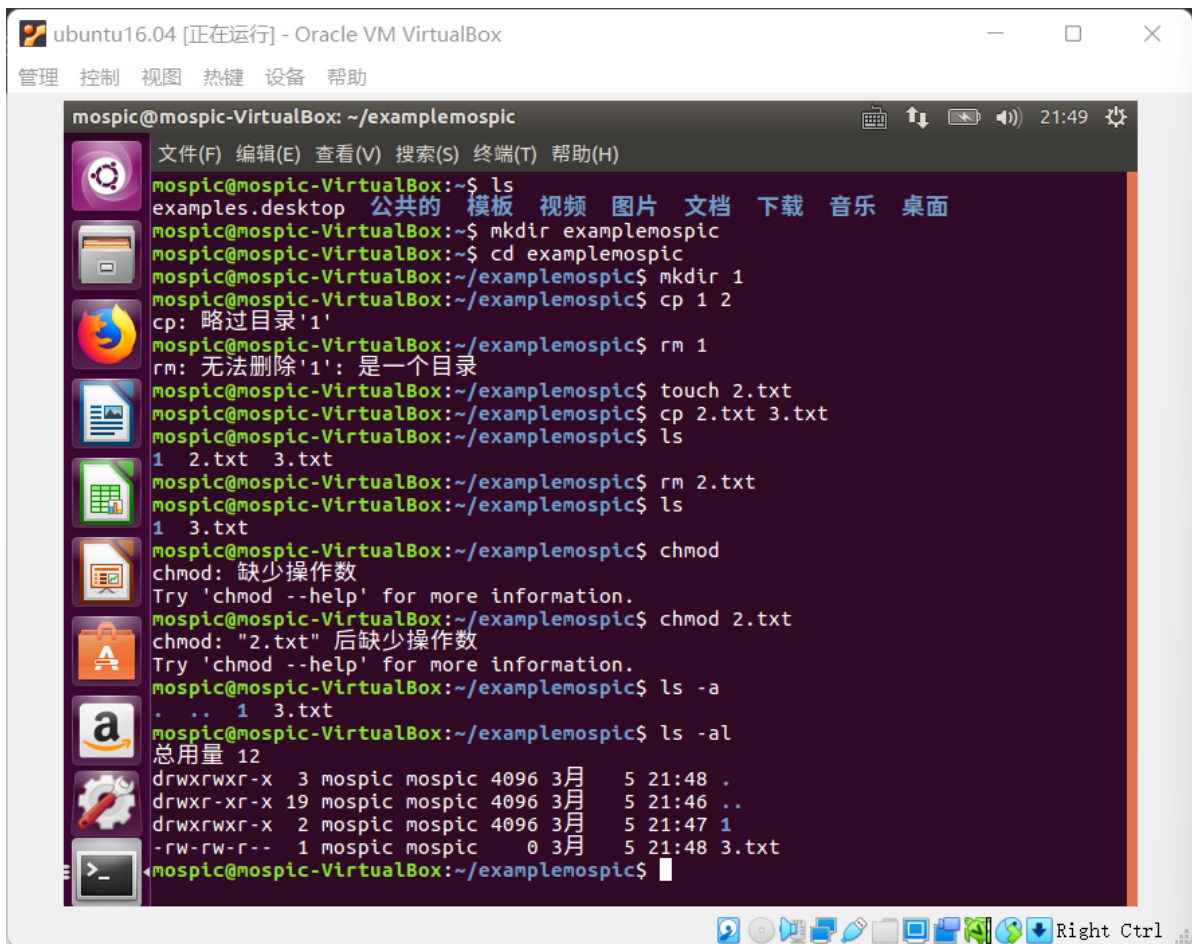
安装好Virtualbox并且导入新建好两个虚拟机后的界面如下：



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：

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : ustc.edu.cn
    IP Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.2

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

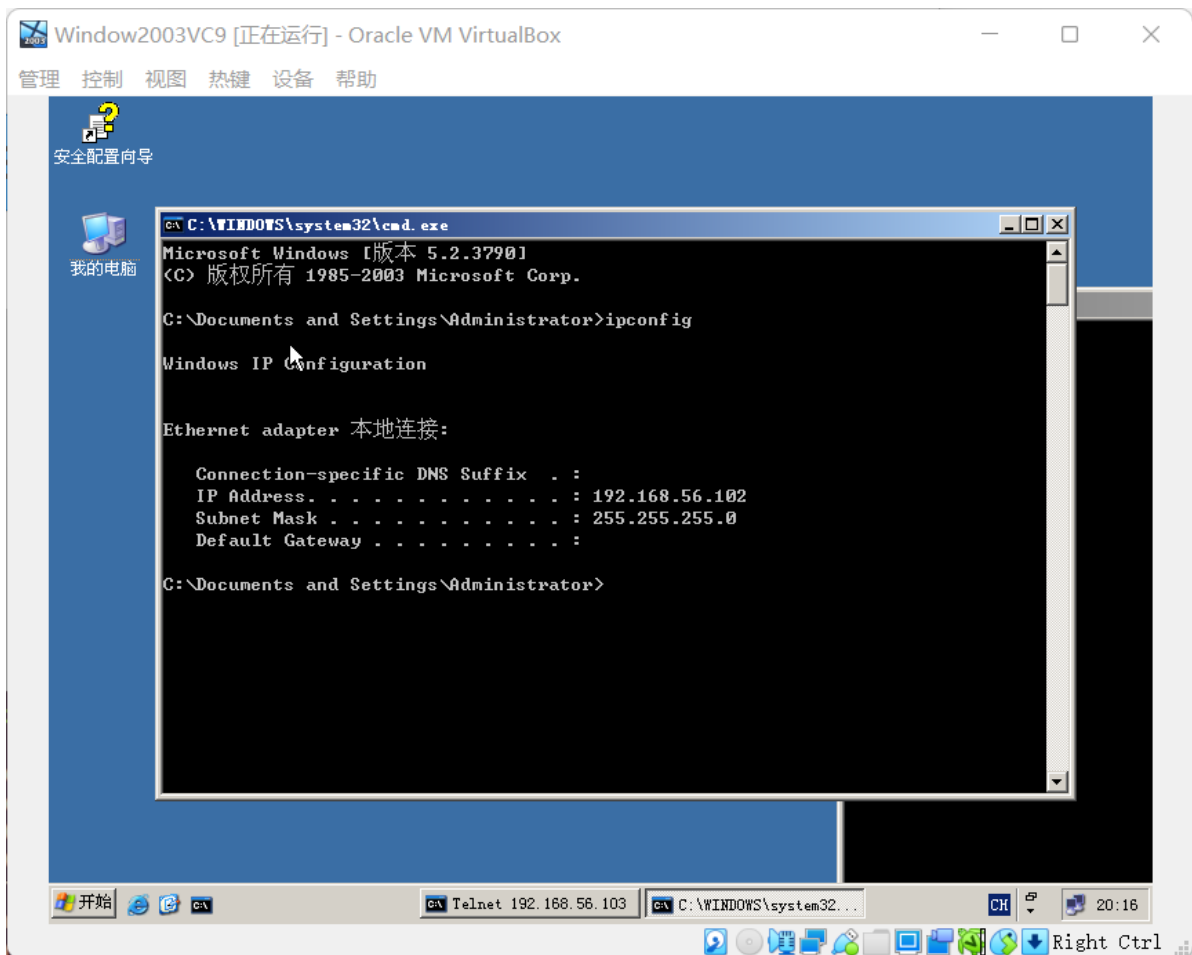
```
C:\Documents and Settings\Administrator 的目录

2015-11-11  21:34    <DIR>          .
2015-11-11  21:34    <DIR>          ..
2015-11-11  21:34    <DIR>          Favorites
2015-11-12  08:45    <DIR>          My Documents
2015-11-11  21:26                0 Sti_Trace.log
2015-11-11  21:25    <DIR>          「开始」菜单
2015-11-11  21:25    <DIR>          桌面
                1 个文件                0 字节
                6 个目录 130,125,209,600 可用字节
```

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。

```
mospic@mospic-VirtualBox: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds
mospic@mospic-VirtualBox:~$ nmap -O 192.168.56.102
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
mospic@mospic-VirtualBox:~$ sudo nmap -O 192.168.56.102

Starting Nmap 7.01 ( https://nmap.org ) at 2022-03-05 16:48 CST
Nmap scan report for 192.168.56.102
Host is up (0.0033s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
MAC Address: 08:00:27:A9:11:8D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.18 seconds
mospic@mospic-VirtualBox:~$
```

(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：

```
ubuntu16.04 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助

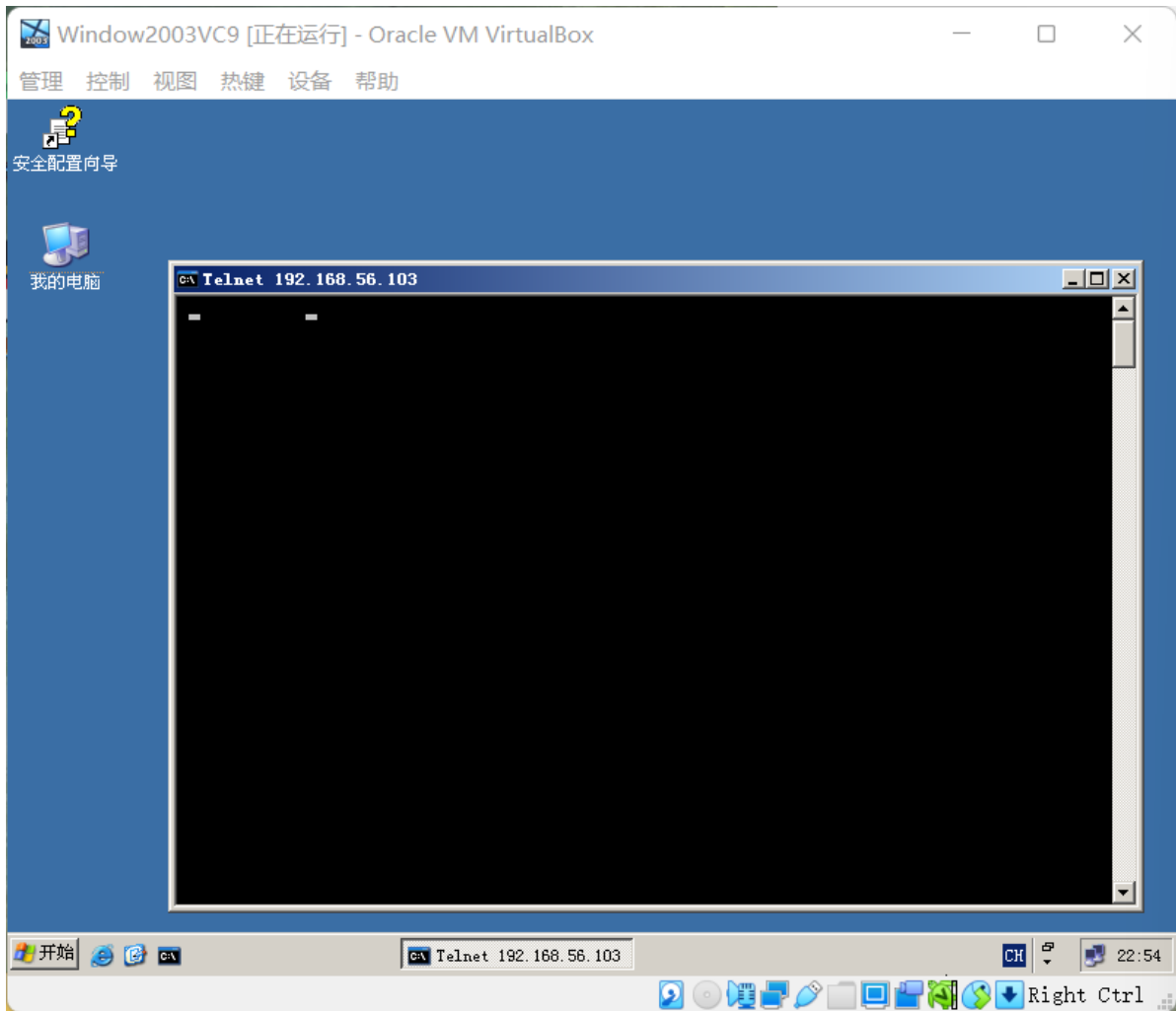
mospic@mospic-VirtualBox: ~/examplemospic
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Try 'chmod --help' for more information.
mospic@mospic-VirtualBox:~/examplemospic$ ls -a
. . . 1 3.txt
mospic@mospic-VirtualBox:~/examplemospic$ ls -al
总用量 12
drwxrwxr-x 3 mospic mospic 4096 3月 5 21:48 .
drwxr-xr-x 19 mospic mospic 4096 3月 5 21:46 ..
drwxrwxr-x 2 mospic mospic 4096 3月 5 21:47 1
-rw-rw-r-- 1 mospic mospic 0 3月 5 21:48 3.txt
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)

mospic@mospic-VirtualBox:~/examplemospic$ nc -l 192.168.56.102 8080
nc: Cannot assign requested address
mospic@mospic-VirtualBox:~/examplemospic$ nc -l -p 8080
aaaaaasssss
```

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。