实验 1 网络信息安全基础实验

中国科学技术大学 曾凡平

2025 年 9 月

1.1 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。

1.2 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。

1.3 实验步骤

1.3.1 安装 VirtualBox 虚拟机

本学期的课程，老师使用的虚拟机系统为 Windows 环境下的 VirtualBox 7.1.12。

从链接：https://pan.ustc.edu.cn/share/index/f4a29c8c096049a9a331（或从 https://www.virtualbox.org/）下载 virtualbox 及对应的 VirtualBox Extension Pack，双击安装文件（先安装 python-3.13.1-amd64 和 VC_redist.x64），按照提示进行安装。（注：截至 2025 年 9 月 21 日星期日，最新版本为 VirtualBox 7.2.2，**VirtualBox 7.2.x 可能存在一些兼容问题，不建议使用**）

按默认方式安装，安装完成后打开 virtualbox 软件（virtualbox 管理器），如图 1 所示：

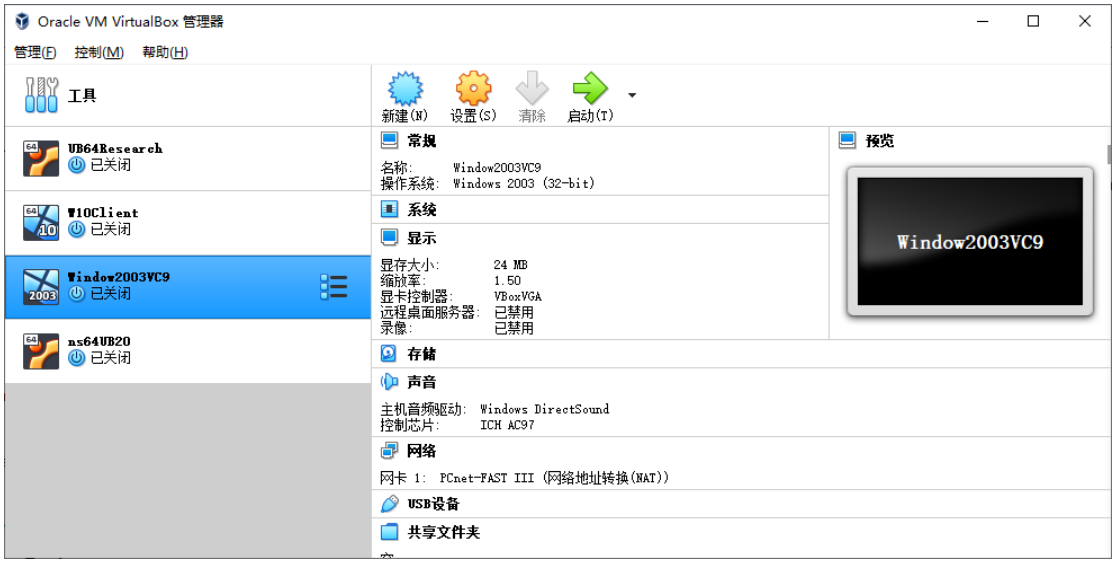


图 1 Virtualbox 管理器

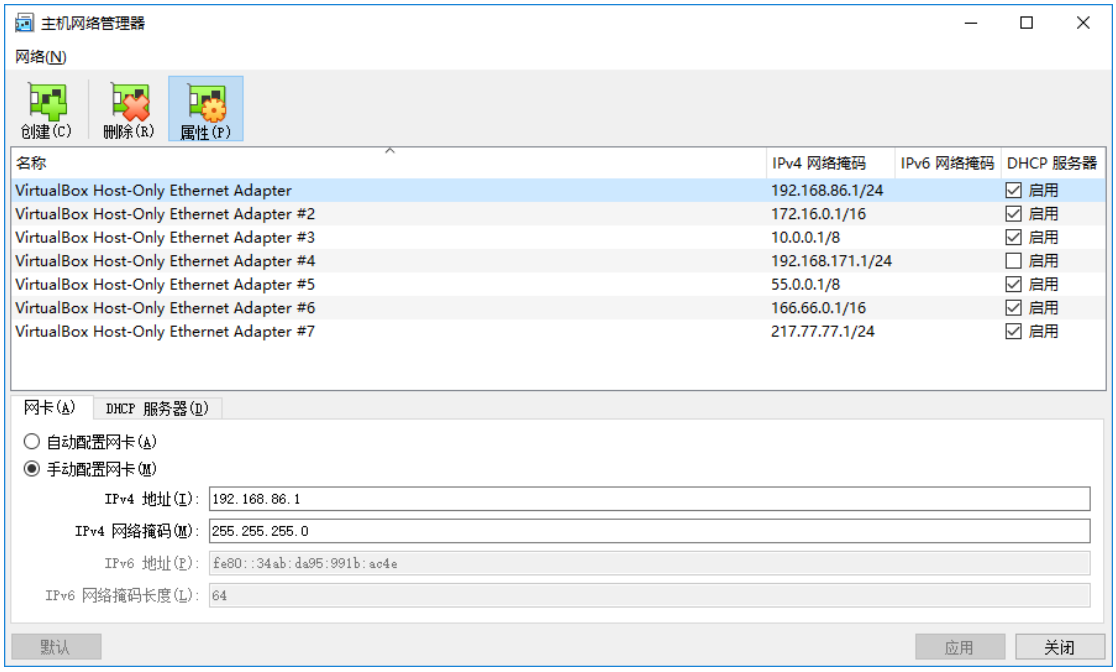
如果能正确运行 virtualbox 管理器，则说明 virtualbox 安装完毕。

接下来双击 VirtualBox Extension Pack，安装“扩展包”使虚拟机能充分利用 virtualbox 提供的“增强功能”。

注意：为了更好地管理主机的磁盘空间，一般将默认虚拟电脑位置（“管理”—“全局设定”—“常规”—默认虚拟电脑位置）设置为 D:\中的某个目录下(例如：D:\VirtualBoxVms)。

1.3.2 配置多个虚拟网卡，模拟多个网络

从 virtualbox 管理器中选“管理”— “工具”— “主机网络管理器”，如图 2 所示：



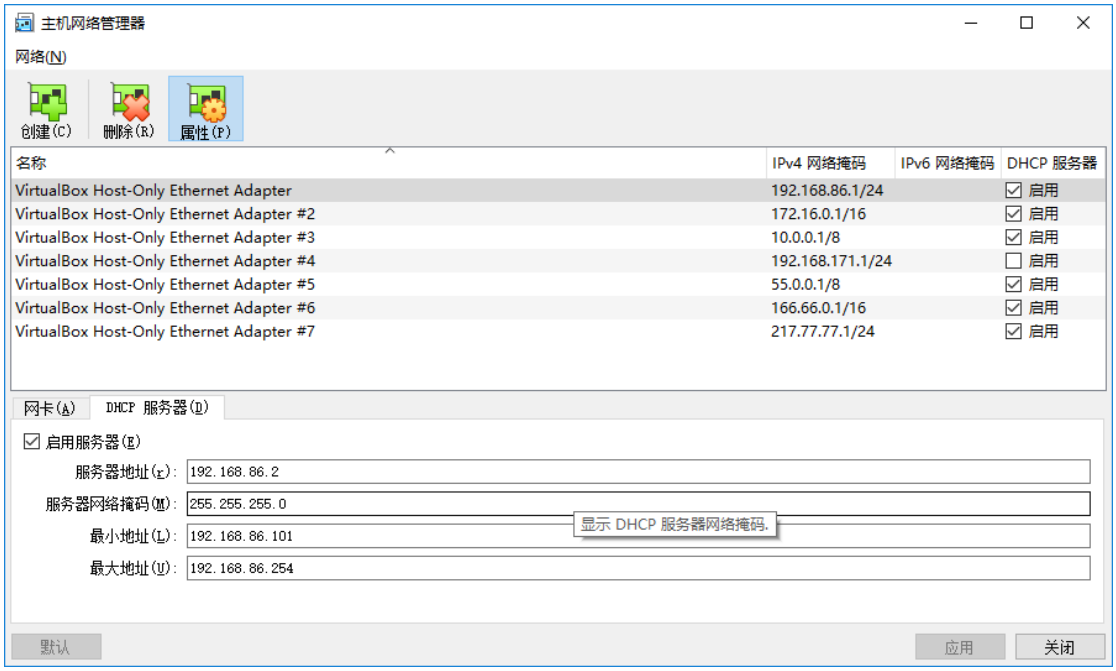


图 2　Virtualbox 主机网络管理器

建议按图 2 所示设置 7 个“仅主机(Host-Only)网络”虚拟网络，按下表配置网络：

网络	参数	作用
Host-Only Ethernet Adapter	192.168.86.1 255.255.255.0	模拟 C 类内部网
Host-Only Ethernet Adapter#2	172.16.0.1 255.255.0.0	模拟 B 类内部网
Host-Only Ethernet Adapter#3	10.0.0.1 255.0.0.0	模拟 A 类内部网
Host-Only Ethernet Adapter#4		备用
Host-Only Ethernet Adapter#5	55.0.0.1 255.0.0.0	模拟 A 类外网
Host-Only Ethernet Adapter#6	166.66.0.1 255.255.0.0	模拟 B 类外网
Host-Only Ethernet Adapter#7	217.77.77.1 255.255.255.0	模拟 C 类外网

1.3.3 安装和配置新的虚拟机系统

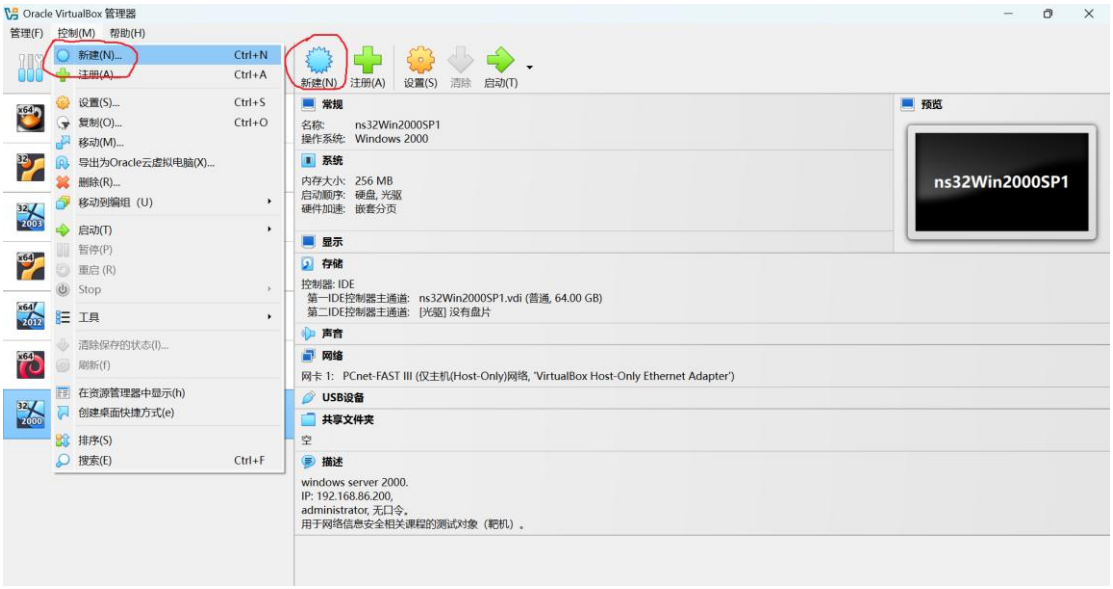
本节以 ubuntu 为例说明虚拟机操作系统的安装与配置。首先下载合适版本的 desktop LTS 版本的安装盘映像文件(ISO 文件，从 http://mirrors.ustc.edu.cn/下载安装映像)，然后点击“VirtualBox 管理器”的“新建(N)”快捷图标，按提示的步骤，新建一个 32 位或 64 位的 ubuntu 虚拟机。

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。

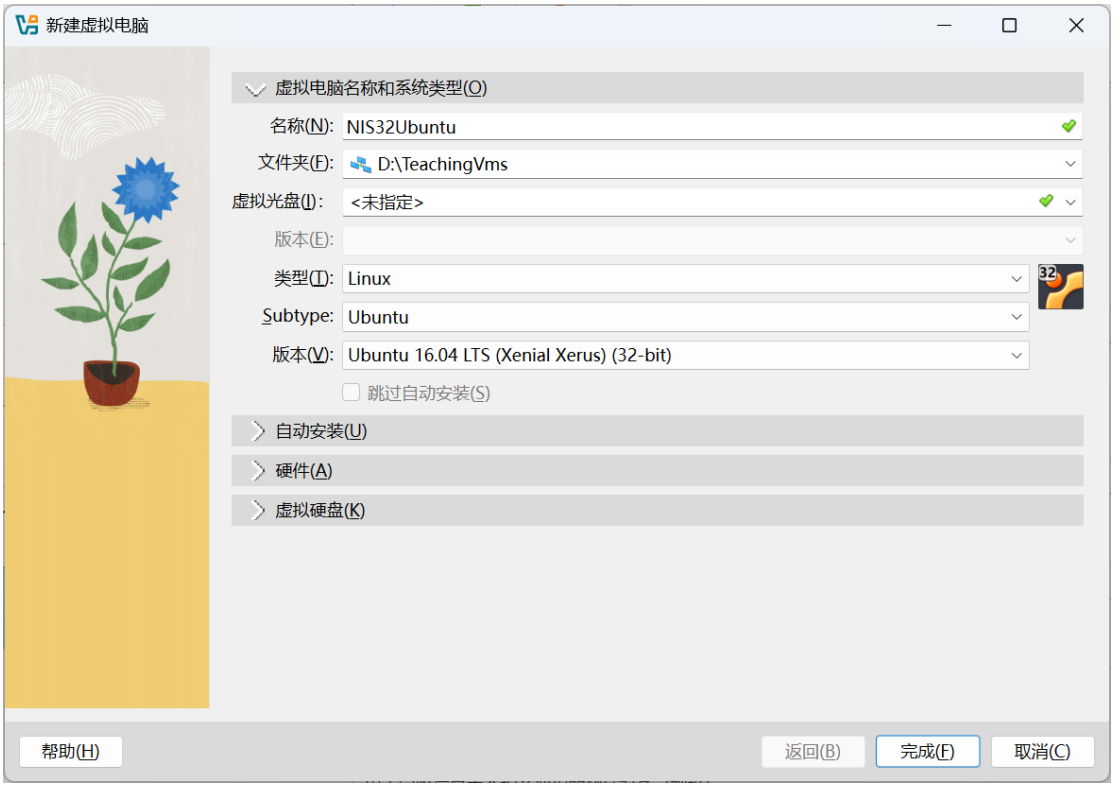
1.3.4 从安装好的虚拟介质（虚拟硬盘）建立虚拟机

从 https://pan.ustc.edu.cn/share/index/c85f22384aca4c9abb91 下载 NIS32SEED16x04.vdi 文件，将该文件拷贝到合适的文件夹(本例为 D:\TeachingVms\vdisk)。

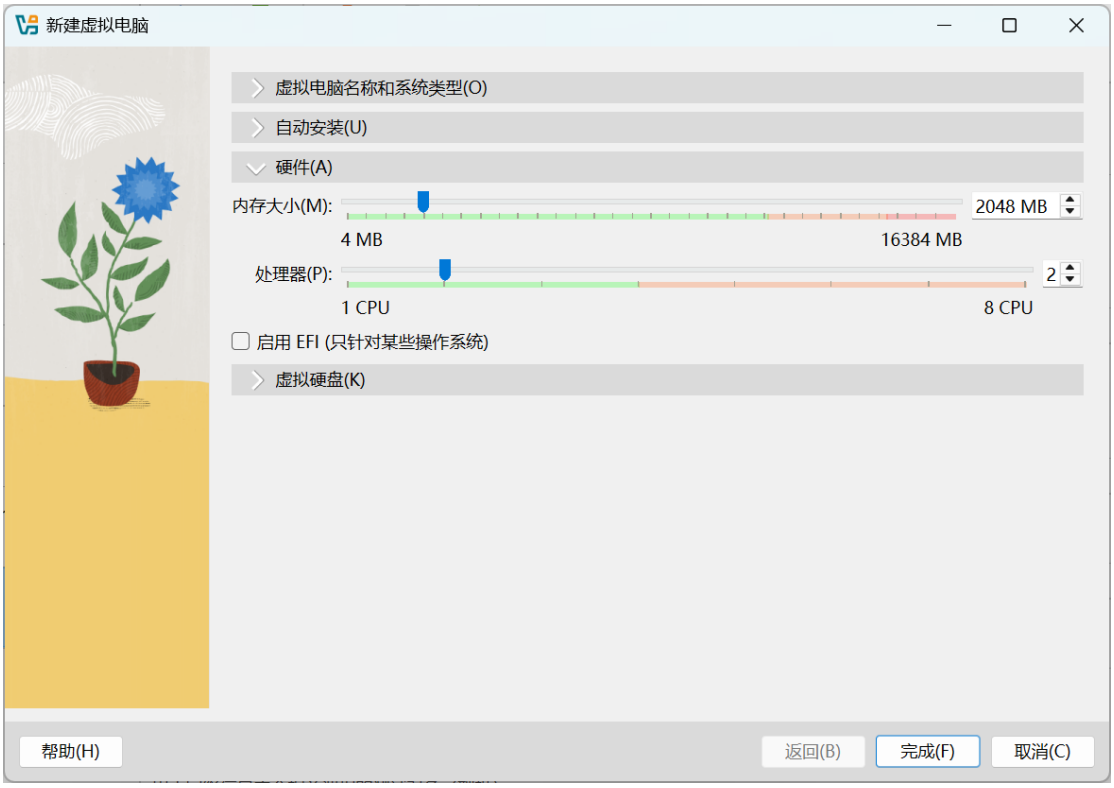
新建一个 32 位 ubuntu Linux 系统：



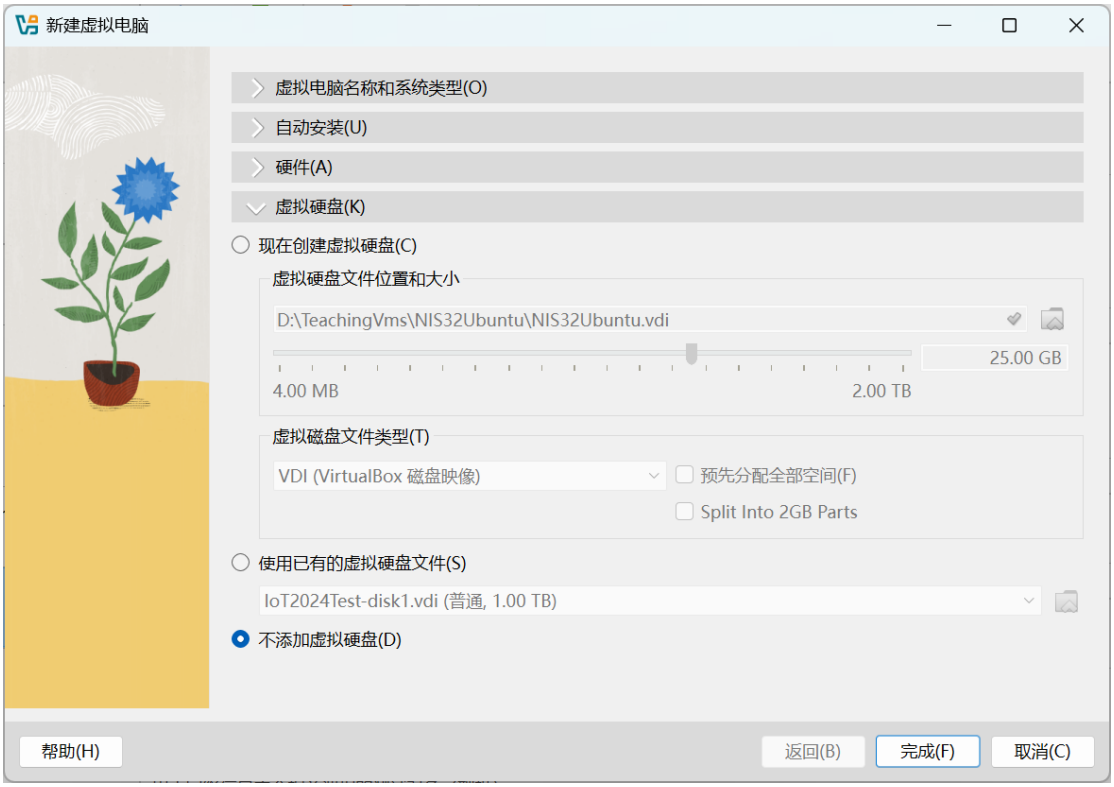
按如下方式设置名称和系统类型：



然后设置硬件（2048MB 内存和 2 个 CPU）：

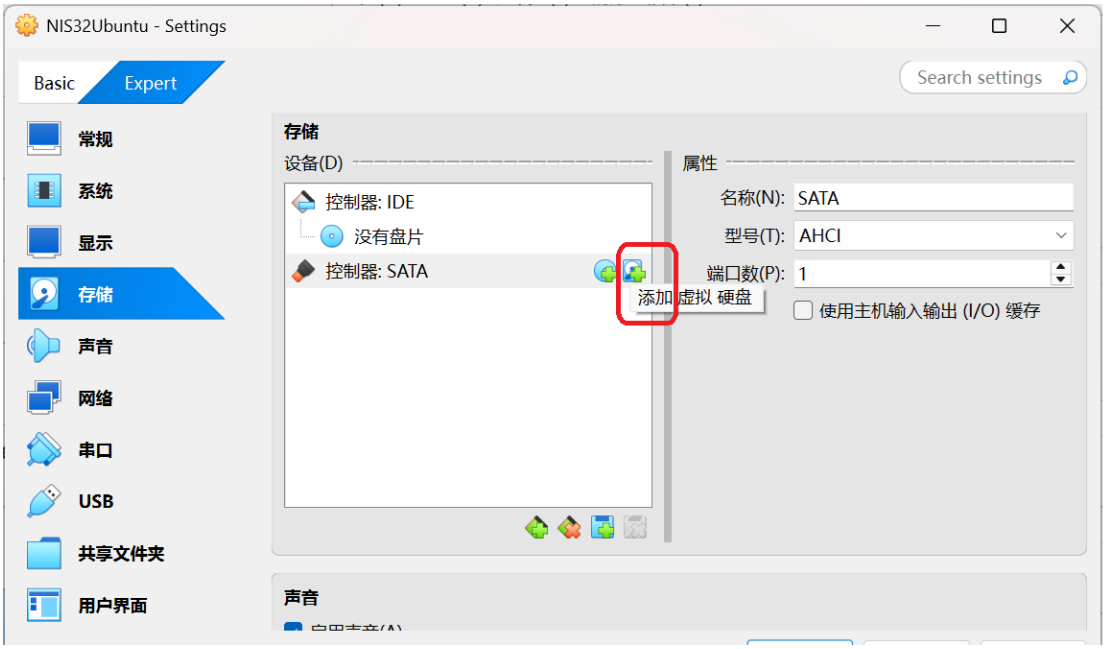


接下来设置虚拟硬盘，选择不添加虚拟硬盘：

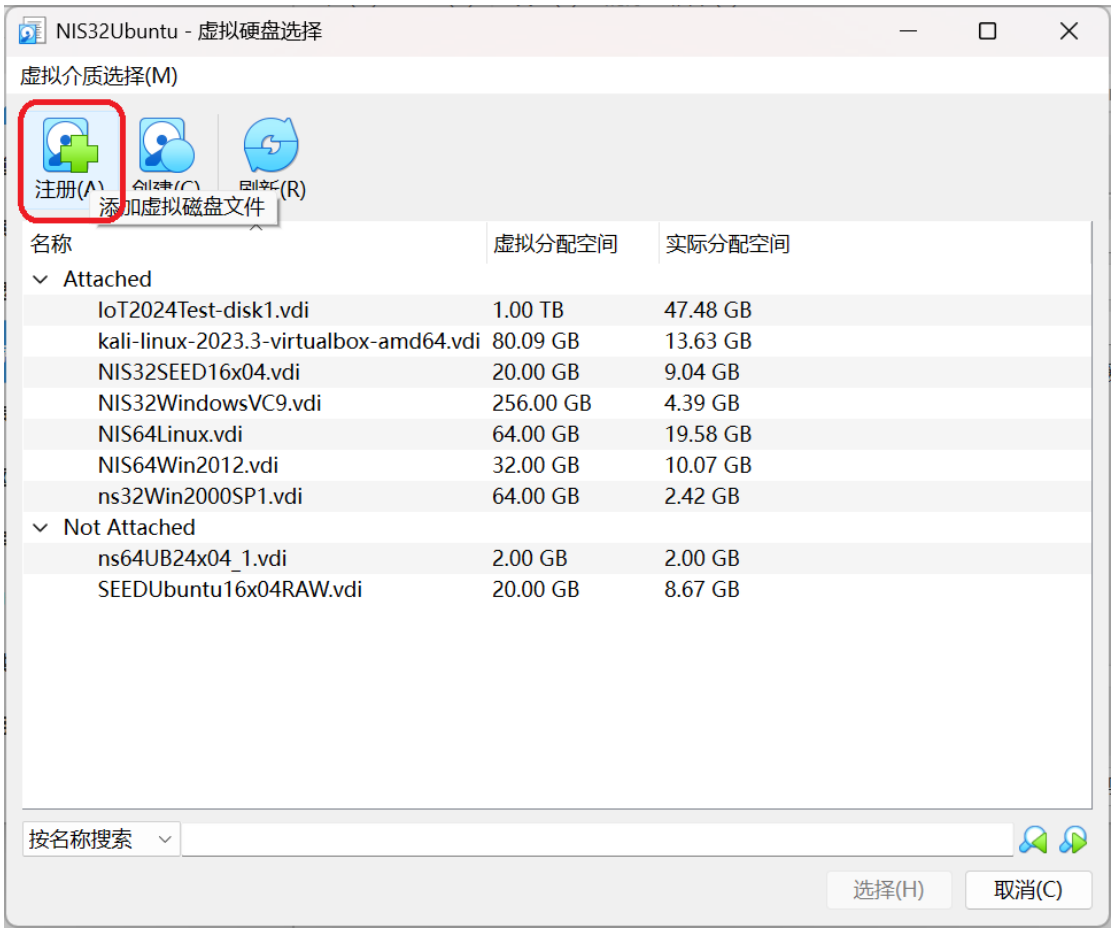


点击完成，将生成一个新的 ubuntu Linux 虚拟机：

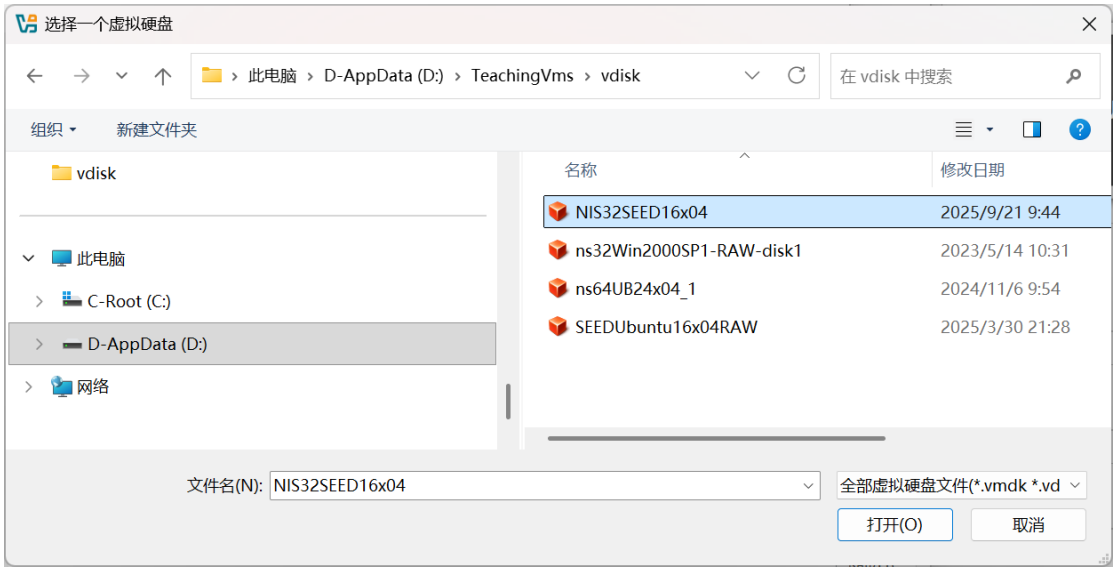
点击上图中的“存储”图标，为虚拟机添加虚拟磁盘。



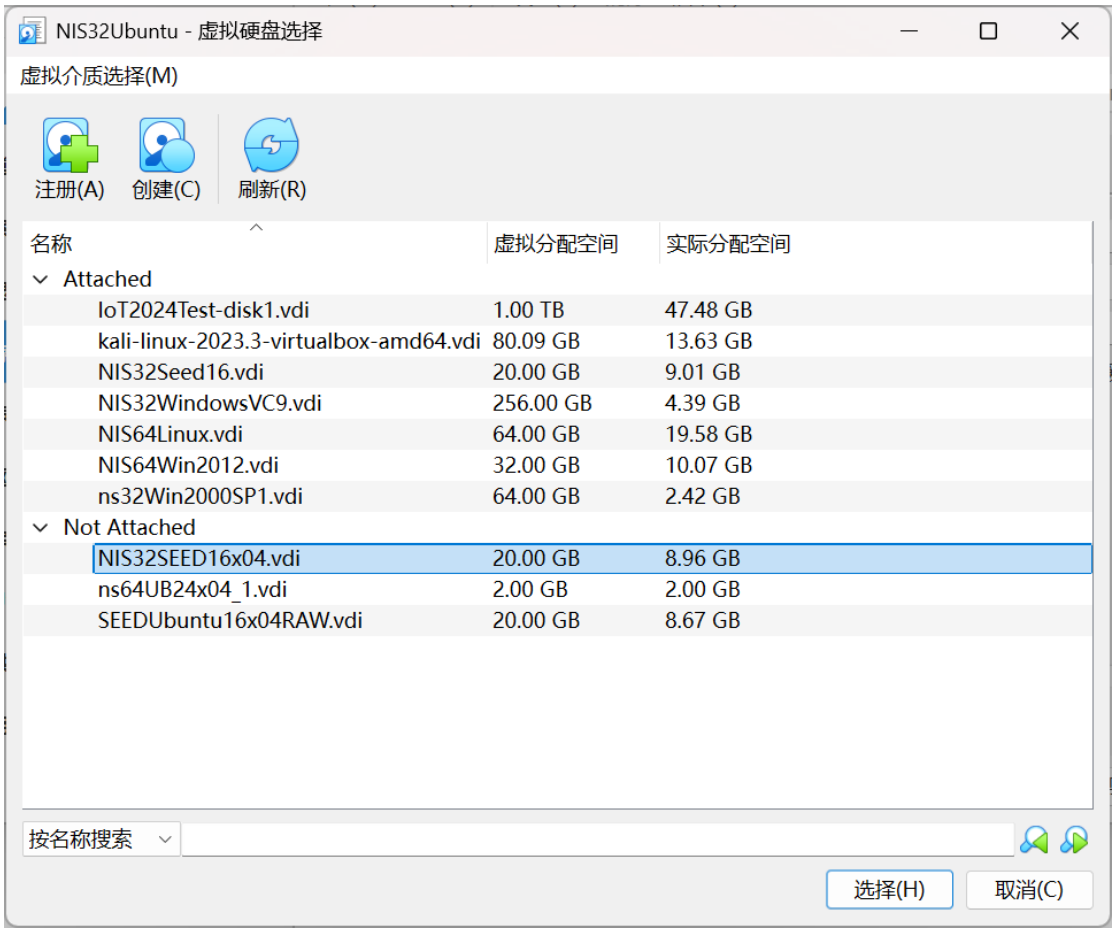
点击“添加虚拟硬盘”图标：



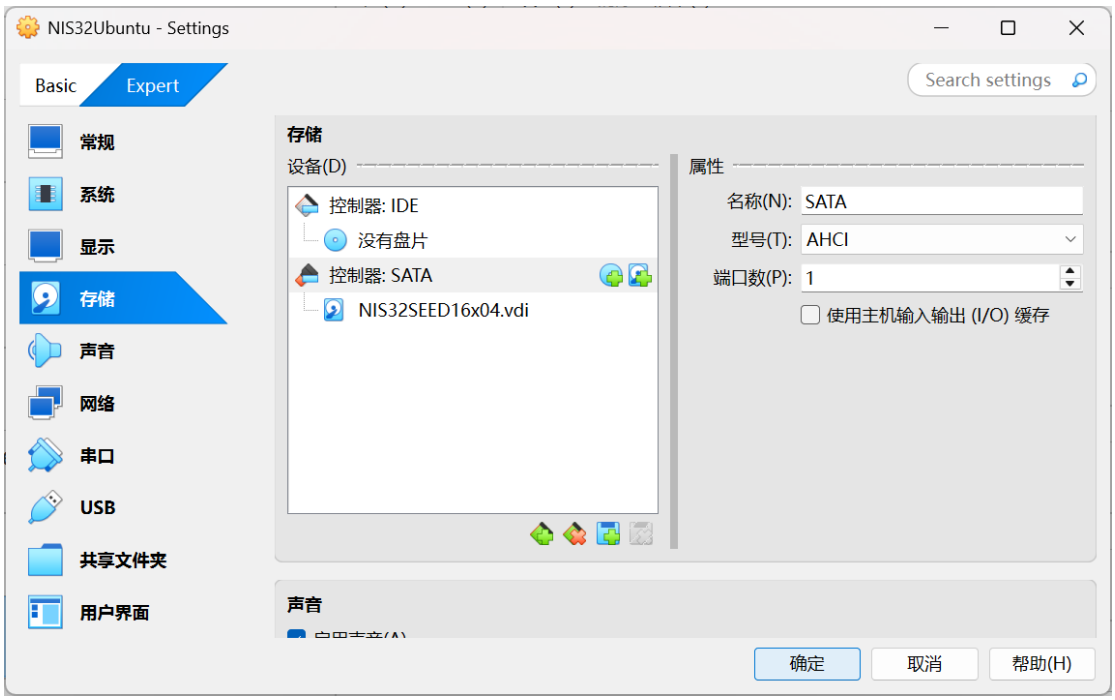
点击注册图标，选择磁盘文件 NIS32SEED16x04：



单击“打开”：

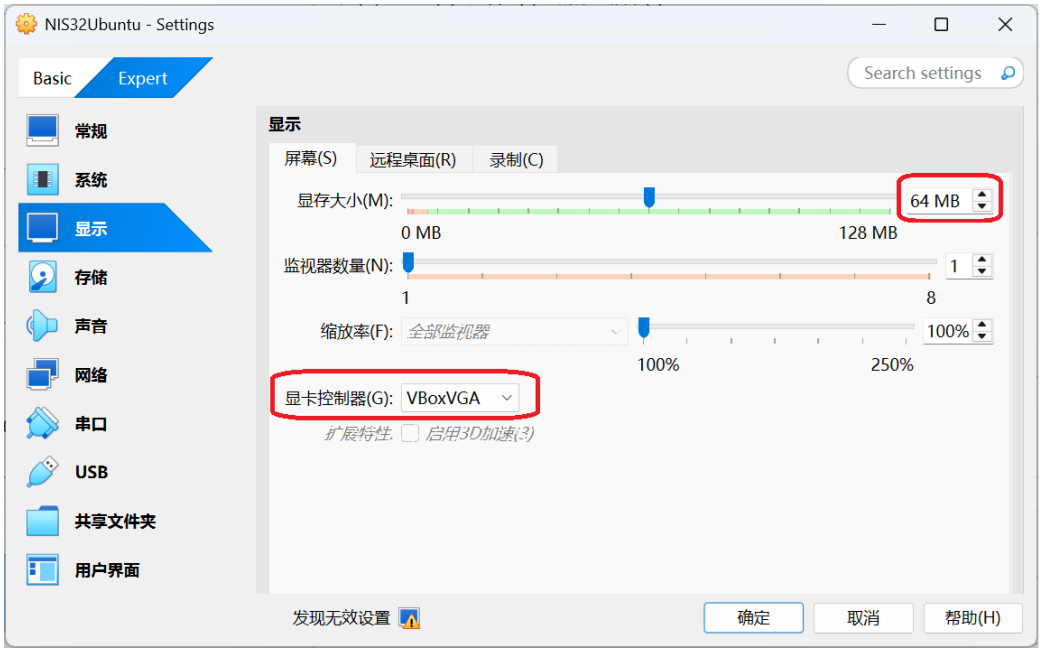


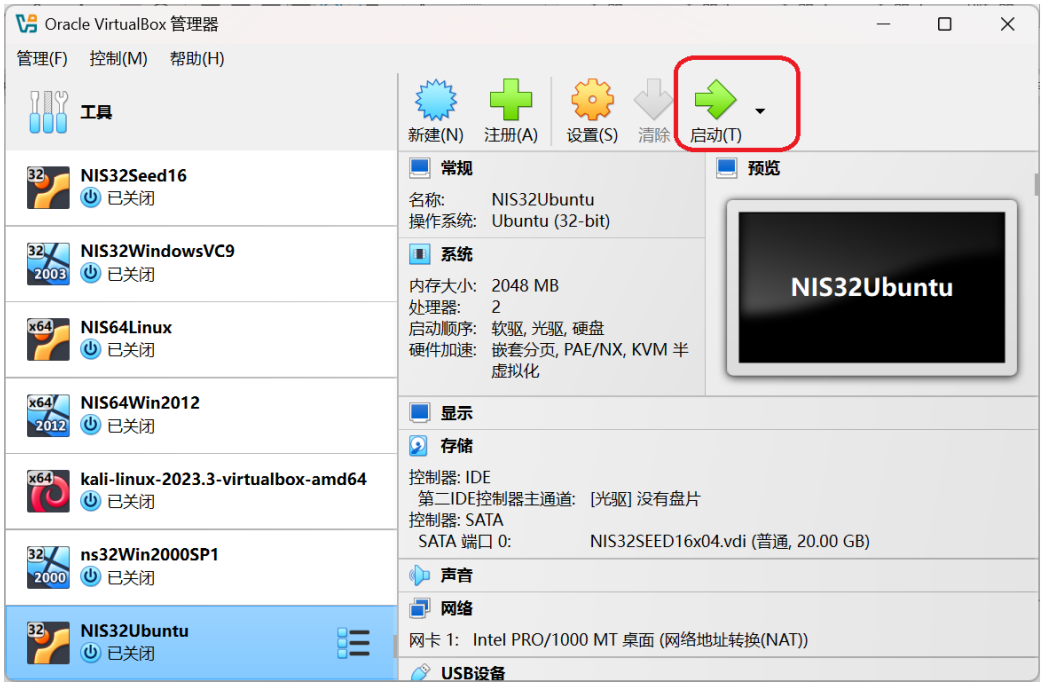
点击“选择”：



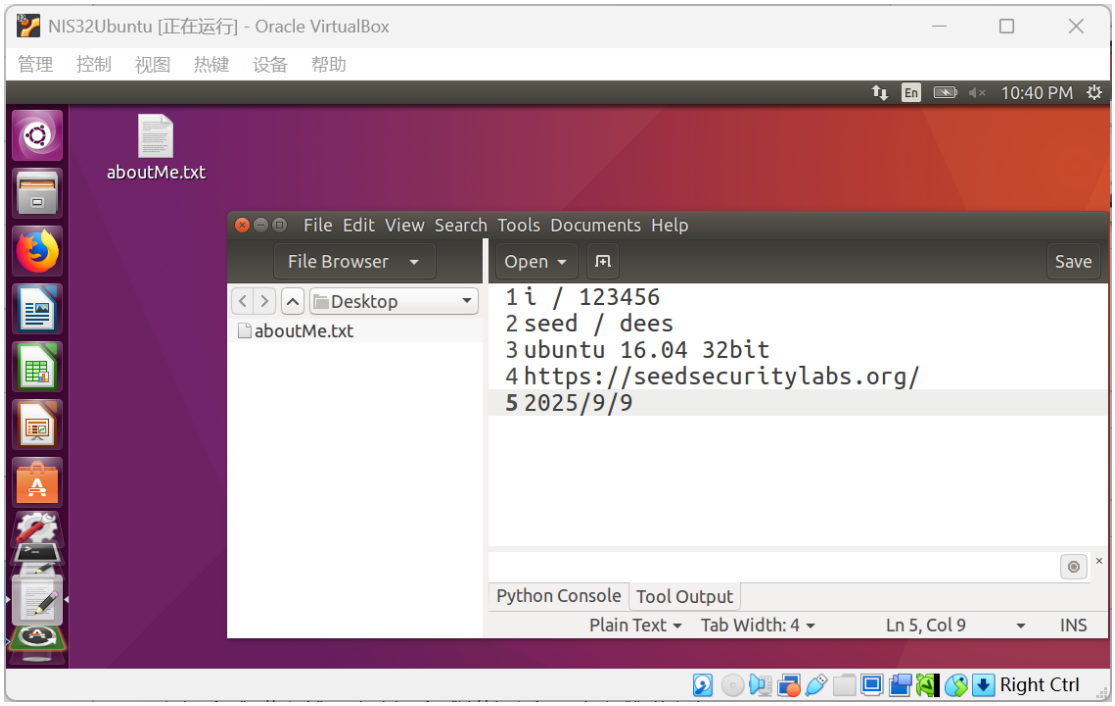
点击“确定”，完成了这个虚拟机的初始创建。

创建完成之后，需要**更改虚拟机的显卡控制器为 VBoxVGA，由于未知的原因，32 位的 ubuntu Linux 16.04LTS 虚拟机在其他显卡模式不能正常工作**。





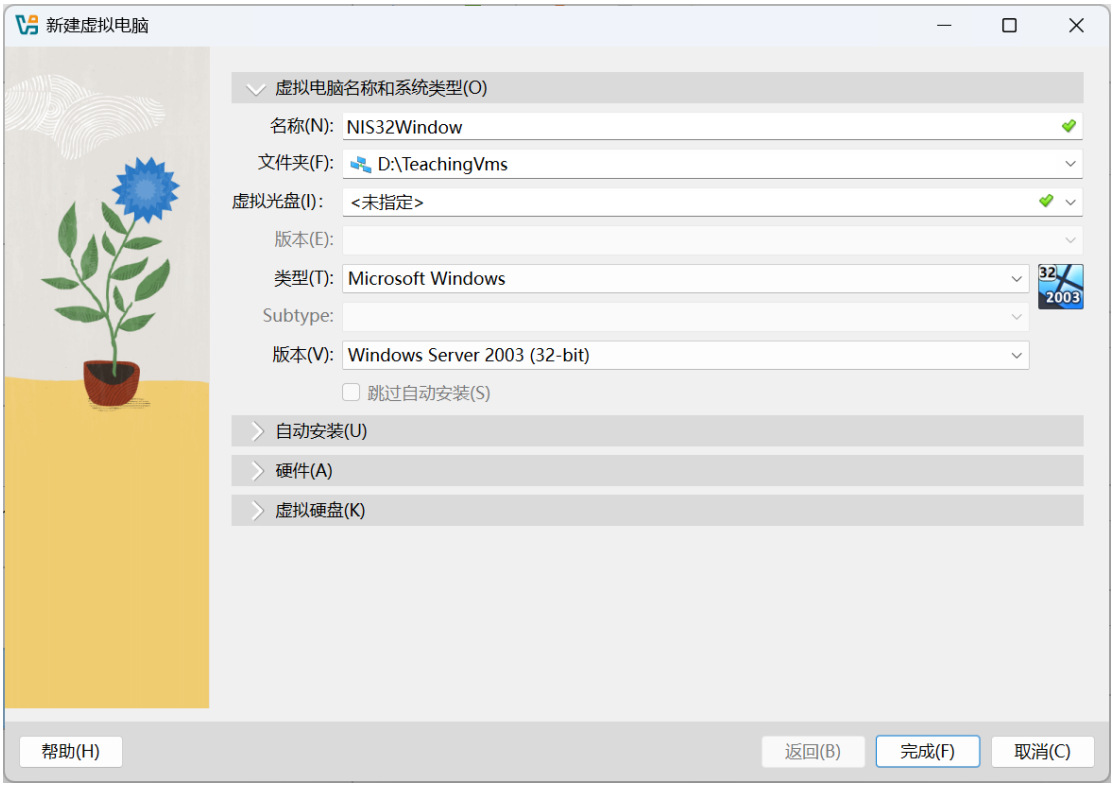
点击“启动”，启动后的虚拟机如下：



桌面上的 aboutMe.txt 包含了该系统的已有用户和口令信息。

另一个常用的 Linux 系统为 64 位 ubuntu Linux 24.04.02 LTS，它的虚拟硬盘文件 NIS64Linux.vdi 下载链接为：https://pan.ustc.edu.cn/share/index/96300c150a344a6db598，可以下载、配置使用。

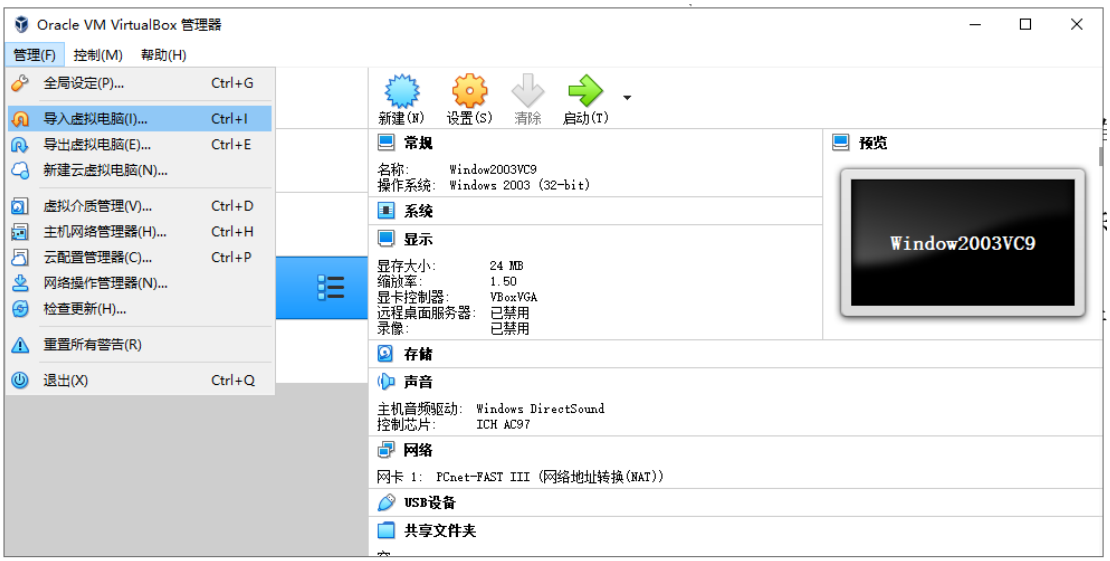
Windows2003 虚拟硬盘链接：https://pan.ustc.edu.cn/share/index/b907a6f06c714ba79349 ，下载该虚拟硬盘文件后，新建一个 Windows ：



完成后可以进行后续实验。

1.3.5 导入和导出安装好的虚拟机

为了分发已经安装好的虚拟机，virtualBox 管理器提供了“导出”和“导入”功能。



导入和导出虚拟电脑

导出的虚拟机映像以压缩格式存放在一个文件中。

选择好需要导入的虚拟机映像，就可以导入虚拟机。为了不与原有的虚拟机的网卡冲突，要选用“重新初始化所有网卡的 MAC 地址”。

导入虚拟机后，可能需要重新设置 IP 地址及主机名等信息，以免和系统中已有的虚拟机冲突。

1.3.4 所述的 32 位 ubuntu Linux 虚拟机 ova 文件链接为：https://pan.ustc.edu.cn/share/index/76a9bdb3c0454442b32c ，下载后导入系统即可运行。

1.3.6 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。

1.4 上机实践(自己练习，不考核)

(1) 熟悉 Windows 2003 下的 net 命令的使用，用 net 命令将目录 C:\hello 共享为 helloc，在主机上将该虚拟机（假定其 IP 地址为 192.168.86.102）的\\192.68.86.102\helloc 映射为本机的 Y:\（注：要实现正确的共享，目录 c:\hello 需要授权为某个用户(比如 guest)可读）。

(2) 在 Windows2003 虚拟机中用 CSocket 编写 C 语言程序实现两台计算机之间的 C/S 模式的网络通信。

(3) netcat 是经典的网络安全工具，在 ubuntu 虚拟机中熟悉该工具的使用。

1.5 做实验并写实验报告(自己练习，不考核)

(1) 用 ubuntu 虚拟机中的网络侦察工具 nmap（如果没有，安装一个）查看并记录已下载的 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。

(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。

(3) 用 nmap 扫描 114.214.236.76，查看并记录该 IP 地址开放了哪些网络端口，记录下你进行实验的时间。注意：在不同的时间段，114.214.236.76 地址开放了不同的网络端口。