2

网络安全技术基础

同现实生活一样，网络攻击者在开始入侵之前，往往要对对方的计算机进行一系列的“踩点”活动，将最大限度地获得对方的信息，然后从这些信息中找到对方的计算机漏洞，进行完准备工作再一举入侵，成功攻击对方计算机。

- 掌握常用的网络安全命令。

任务 1　网络基础介绍

【任务描述】

错综复杂的网络和数百上千的计算机怎么才能正常连接？主机之间相互不干涉能正常运作，数据又是如何正确地通过网络上传和下载的呢？计算机能通过网络共享资源，那么网络的安全就成为首要考虑的问题，也就是如何能保证系统连续可靠正常地运行，网络服务不中断。通过了解网络技术的一些基本知识能更好地理解网络是如何运行的。

【任务要求】

了解关于网络 IP 地址及端口的一些相关知识。

【知识链接】

1. IP 地址

Internet 网络上连接着数千百万的计算机主机，人们给每台主机都分配了一个联网专用的逻辑地址以区别这些主机，这个专门的地址称为 IP 地址。IP 地址具有唯一性，不重复，因此通过 IP 地址就可以访问世界上的任意一台计算机主机。

IP 地址由 4 部分十进制数字组成，各部分之间用小数点隔开，每部分十进制数字对应一个 8 位二进制数，共 32 位二进制数，例如，某台计算机主机的 IP 地址为 106.42.133.238。地址空间的不足必将妨碍互联网的进一步发展。为了扩大地址空间，拟通过 IPv6 重新定义地址空间，IPv6 采用 128 位地址长度。

IP 地址现由因特网名字与号码指派公司 ICANN（Internet Corporation for Assigned Names and Numbers）分配，Internet 的 IP 地址由 NIC（Internet Network Information Center，因特网信息中心）统一负责全球地址的规划、管理。同时由 Inter NIC 具体负责美国及其他地区的 IP 地址分配；APNIC（Asia Pacific Network Information Center）负责亚洲地区的 IP 地址分配；ENIC 负责欧洲及其他地区的 IP 地址分配。

- 固定 IP：固定 IP 地址是长期固定分配给一台计算机使用的 IP 地址，一般只有特殊的服务器才拥有固定 IP 地址。
- 动态 IP：由于 IP 地址资源非常短缺，电话拨号上网或者普通宽带上网用户一般不具备固定 IP 地址，而是由 ISP 动态分配暂时的一个 IP 地址。用户一般不需要去了解动态 IP 地址，这些是由计算机系统自动完成的。
- 公有地址（Public Address）：由 Inter NIC 负责。这些 IP 地址分配给注册并向 Inter NIC 提出申请的组织结构，通过它可以直接访问因特网。
- 私有地址（Private Address）：属于非注册地址，专门为组织结构内部使用，以下列出留用的内部私有地址：

  A 类：10.0.0.0～10.255.255.255

  B 类：172.16.0.0～172.31.255.255

  C 类：192.168.0.0～192.168.255.255

2. 计算机端口

（1）什么是端口。

端口（Port）可以认为是设备与外界通信交流的出口。端口的含义有以下两种：

物理端口：又称为接口，是可见端口，主要用于连接其他网络设备。如交换机、路由器、集线器等的 RJ-45 端口，计算机背板的 RJ-45 网口，MODEM的 Serial 端口，电话使用的 RJ-11 插口等。

逻辑端口：一般是指 TCP/IP 中的计算机或交换机、路由器内的端口，不可见。端口号的范围为 0～65535，如用于 FTP 服务的 21 端口；用于浏览网页服务的 80 端口等。

在 Internet 上，各主机间通过 TCP/IP 协议发送和接收数据包，各个数据包根据其目的主机的 IP 地址来进行互联网络中的路由选择，把数据包顺利地传送到目的主机。大多数操作系统都支持多程序（进程）同时运行，那么目的主机应该把接收到的数据包传送给众多同时运行

的进程中的哪一个呢？为了解决这个问题，引入了端口机制。

本地操作系统会给那些有需求的进程分配协议端口（protocol port），每个协议端口由一个正整数标识，如 80、139、445 等。当目的主机接收到数据包后，将根据报文首部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会领取数据并等待下一组数据的到来。

端口其实就是队，操作系统为各个进程分配了不同的队，数据包按照目的端口被推入相应的队中，等待进程取用，在极特殊的情况下，这个队也是有可能溢出的，不过操作系统允许各进程指定和调整自己队的大小。不光接收数据包的进程需要开启它自己的端口，发送数据包的进程也需要开启端口，这样，数据包中将会标识有源端口，以便接收方能顺利地回传数据包到这个端口。

（2）详解端口。

如果把 IP 地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口最多可以有 65536 个。端口是通过端口号来标记的，端口号只有整数，范围是 0～65535。不同的服务如 Web 服务、FTP 服务、SMTP 服务等通过不同的端口门进入到拥有 IP 地址的主机这个大房子中来实现。由上可以看出，一个 IP 地址可以对应多个网络服务，显然主机不能只靠 IP 地址来区分不同的网络服务，实际上通过“IP 地址+端口号”来区分不同的服务。换言之，如果没有端口，每一个服务进程要占用一个 IP 地址，这是一种极大的浪费。

一般一个端口对应一个应用程序，发送到这个端口的数据被这个应用程序接收，但是一个应用程序可以对应多个端口。

（3）端口类型。

- 公认端口（Well Known Ports）：范围是 0～1023，一般固定分配于一些服务。例如 80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。
- 注册端口（Registered Ports）：范围是 1024～49151，分配给用户进程或应用程序。这些进程主要是用户选择安装的一些应用程序，而不是已经分配好了公认端口的常用程序。这些端口在没有被服务器资源占用的时候，可以由用户端动态选用为源端口。例如，许多系统处理动态端口从 1024 左右开始。
- 动态端口（Dynamic Ports）：范围是 49152～65535。之所以称为动态端口，是因为它一般不固定分配某种服务，而是动态分配。

3. 端口扫描及端口扫描器

端口扫描是指某些别有用心的人发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型（这些网络服务均与端口号相关）。攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本，这样就能间接或直观地了解到远程主机所存在的安全问题。

【思考与练习】

理论题

1．IP 地址的含义是什么？
2．常用的端口有哪些？

任务 2　常用网络安全命令

【任务描述】

2014 年 9 月，一个严重的 Bash 安全漏洞影响了许多用户。Bash 是 Linux 用户广泛使用的一款用于控制的命令提示符工具，从而导致该漏洞影响范围甚广。安全专家表示，由于并非所有运行 Bash 的电脑都存在漏洞，所以受影响的系统数量有限。不过，Shellshock 本身的破坏力却更大，因为黑客可以借此完全控制被感染的机器，不仅能破坏数据，甚至会关闭网络，或对网站发起攻击。

网络攻击者经常还要配合使用一些命令，因此必须掌握和学习一些常见的网络安全命令，才能对追踪网络攻击者有所帮助，提高自身系统的防御能力。

【任务要求】

了解并掌握一些常用的网络安全命令。

【实现方法】

1．探测 IP 地址——ipconfig

每个用户如何探知自己电脑的 IP 地址呢？Windows 系统中，在“开始”菜单中选择“运行”命令，在打开的“运行”对话框中输入“cmd”命令，如图 2-1 所示。

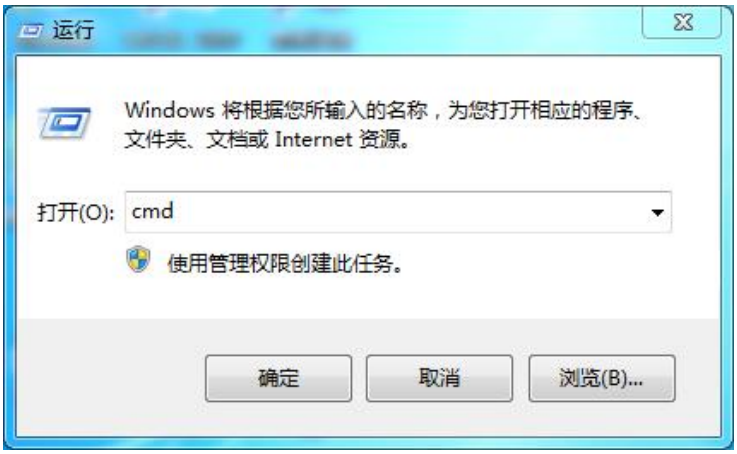

图 2-1　在“运行”对话框中输入“cmd”命令

在打开的命令提示符窗口中输入 ipconfig，并按 Enter 键，如图 2-2 所示。此时可显示本机的 IP 信息。其中外网 IP 地址为 169.254.248.80，子网掩码为 255.255.0.0，如图 2-3 所示。

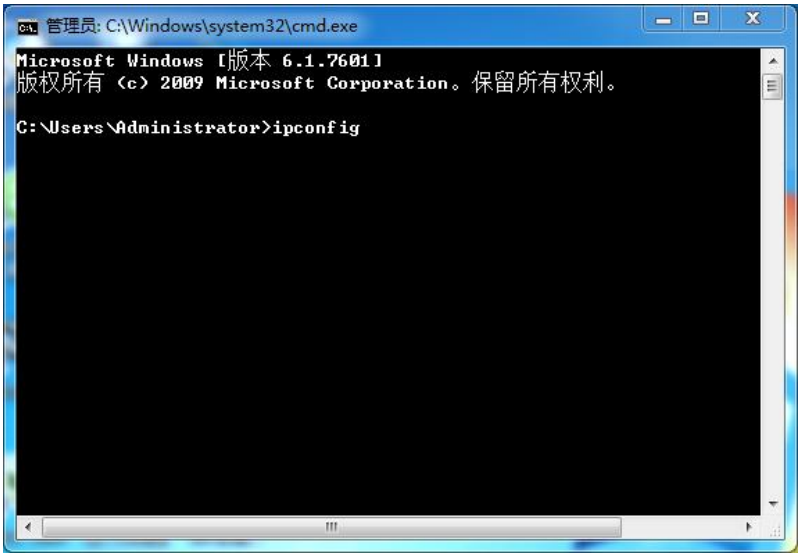

图 2-2　输入“ipconfig”命令

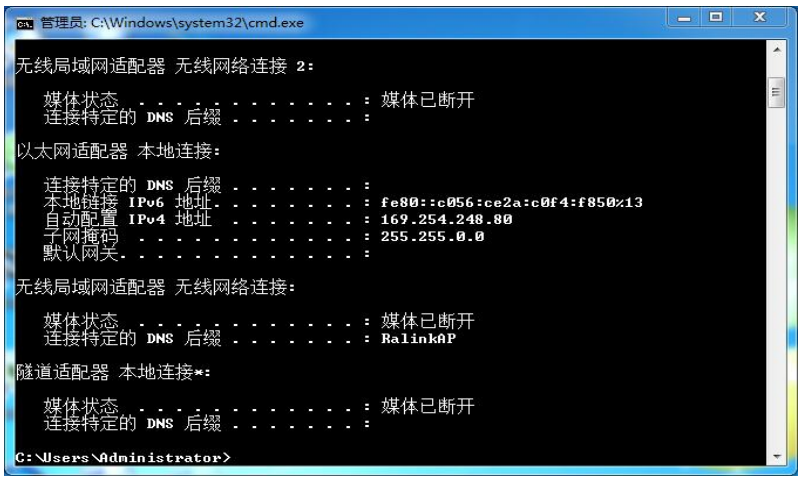

图 2-3　本机的外网 IP 地址

输入 ipconfig/all 命令，可见一个物理地址：E4-D5-3D-02-23-42，这是计算机的唯一网卡地址，如图 2-4 所示。

以太网的 IP 地址（局域网的 IP 地址）为 192.168.18.1，虚拟机的 IP 地址是 192.168.61.1，如图 2-5 所示。

【小知识】：网卡地址 MAC（Media Access Control，介质访问控制）是识别 LAN（局域网）节点的标识。网卡的物理地址通常是由网卡生产厂家烧入网卡的 EPROM（一种闪存芯片，通常可以通过程序擦写），它存储的是传输数据时真正赖以标识发出数据的电脑和接收数据的主机的地址。

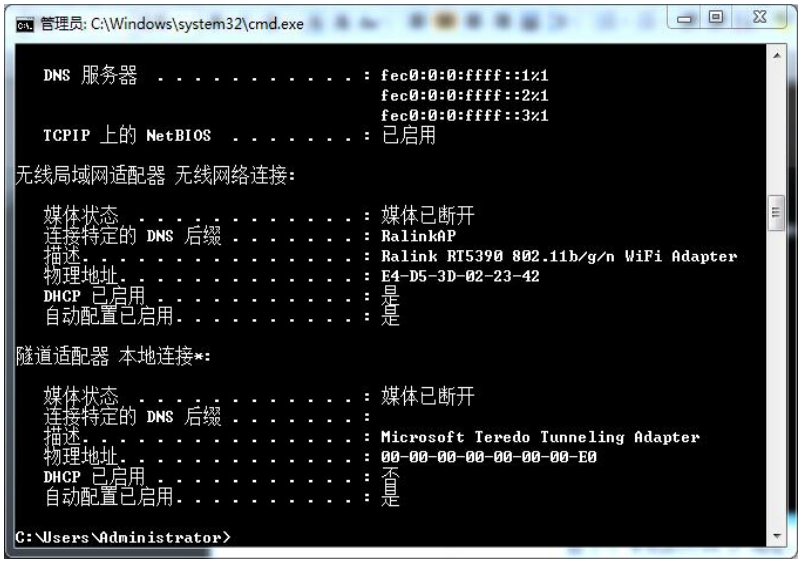

图 2-4　本机的网卡信息

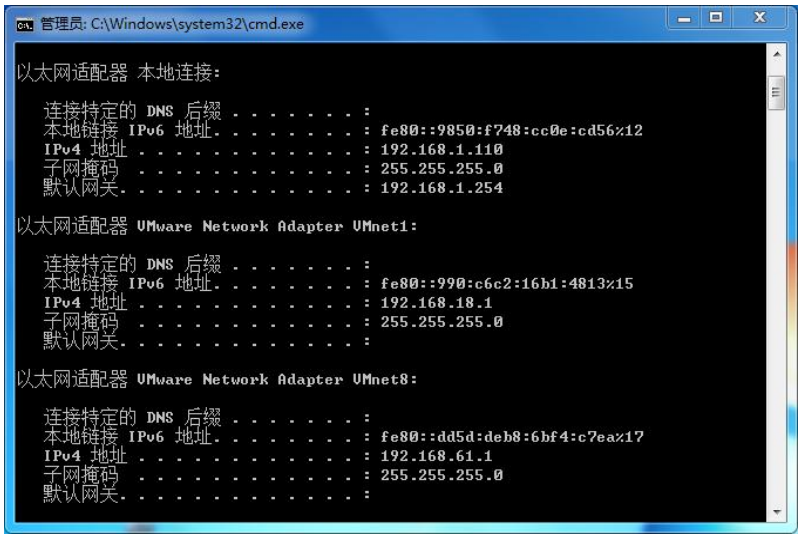

图 2-5　局域网 IP 地址

也就是说，在网络底层的物理传输过程中，是通过物理地址来识别主机的，它也是全球唯一的。比如著名的以太网卡，其物理地址是 48bit（比特位）的整数，以太网地址管理机构（IEEE）将以太网地址也就是 48 比特位的不同组合，分为若干独立的连续地址组，生产以太网网卡的厂家就购买其中一组，具体生产时，逐个将唯一地址赋予以太网卡。

形象地说，MAC 地址就如同身份证上的身份证号码，具有全球唯一性。

2. 连接测试——ping

ping 是测试网络连接状况以及信息包发送和接收状况非常有用的工具，是网络测试最常用的命令。ping 向目标主机（地址）发送一个回送请求数据包，要求目标主机收到请求后给予答复，若对方回应，可判断本机与目标主机网络连通；若提示 request time out，说明本机与

目标主机网络不通。同时，ping 命令可显示两台计算机的连接时间及速度。

在 Windows 操作系统中，通常与网络安全有关的命令是 ping\winipcfg\tracert\net\at\netstat。ping 是 TCP/IP 中有用的命令之一。

（1）在命令提示符窗口下输入 ping 命令，ping 命令格式为：

ping IP 地址或主机名 [-t] [-a] [-n count] [-l size][-f][-i TTL][-v TOS][-r count][-s count][[-j host-list] ¦ [-k host-list]][-w timeout][-R][-S srcaddr][-4][-6] target_name

如图 2-6 所示。

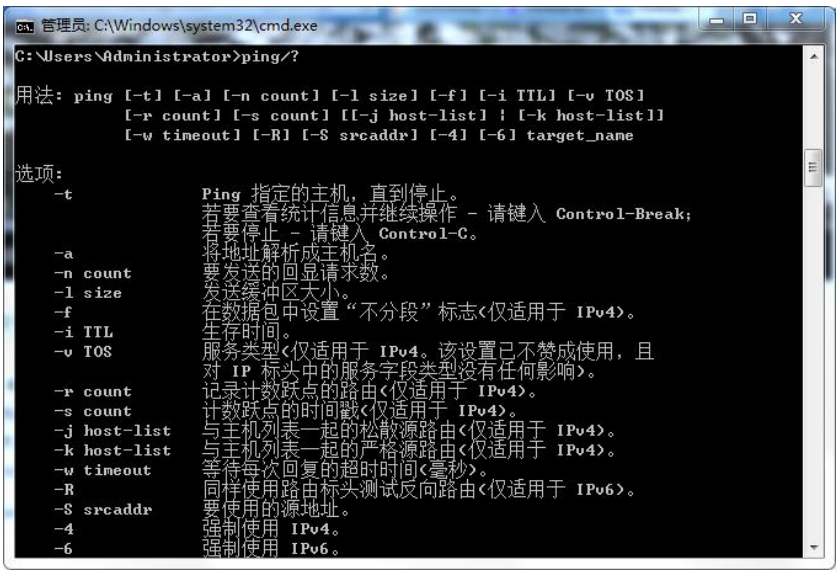

图 2-6　ping 命令格式图

参数含义：

-t：不停地向目标主机发送数据；

-a：以 IP 地址格式来显示目标主机的网络地址；

-n count：指定要 ping 多少次，具体次数由 count 来指定，默认值为 4；

-l size：指定发送到目标主机的数据包的大小；

-f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段；

-i TTL：表示 DNS 记录在 DNS 服务器上的缓存时间。

一般情况下 ping 命令正常的返回值如图 2-7 所示。其中的数据含义为：每次发送 32 字节的数据，返回时间为 0ms，TTL 值为 128；数据包发送了 4 个，收到 4 个，损耗 0。

根据 ping 命令后所跟参数不同，查看的功能不尽相同。例如，通过 ping 能判断目标主机的类型，通常来说：

- TTL=32 认为目标主机操作系统为 Windows 95/98；
- TTL=64～128 认为目标主机操作系统为 Windows 2000/XP；
- TTL=128～255 或者 32～64 认为目标主机操作系统为 UNIX/Linux。

以本机为例，命令为 ping 169.254.248.80，可以看到 TTL=64，说明是 Windows 操作系统，如图 2-8 所示。

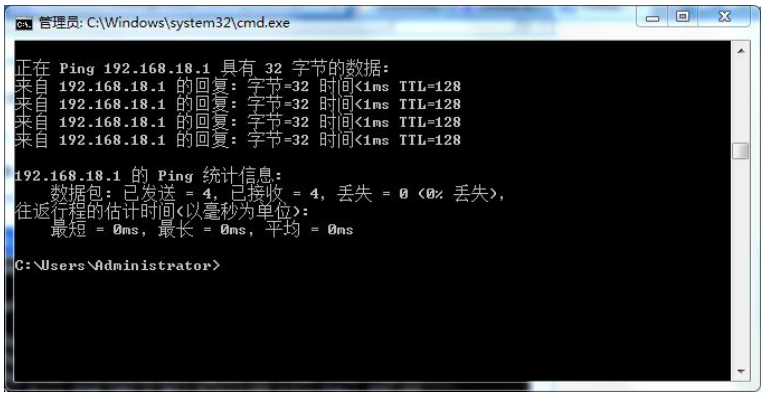

图 2-7　ping 命令返回值

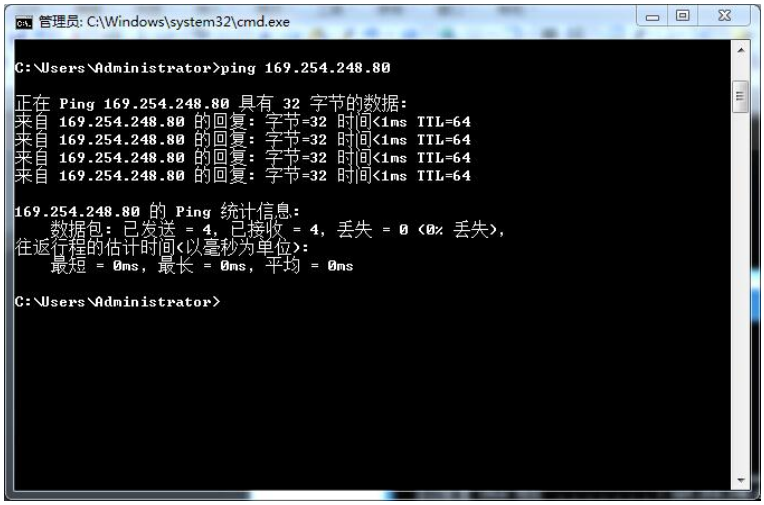

图 2-8　ping 本机的 TTL 返回值

以某网站为例，测试一下 ping 命令：ping www.sina.com.cn，如图 2-9 所示。

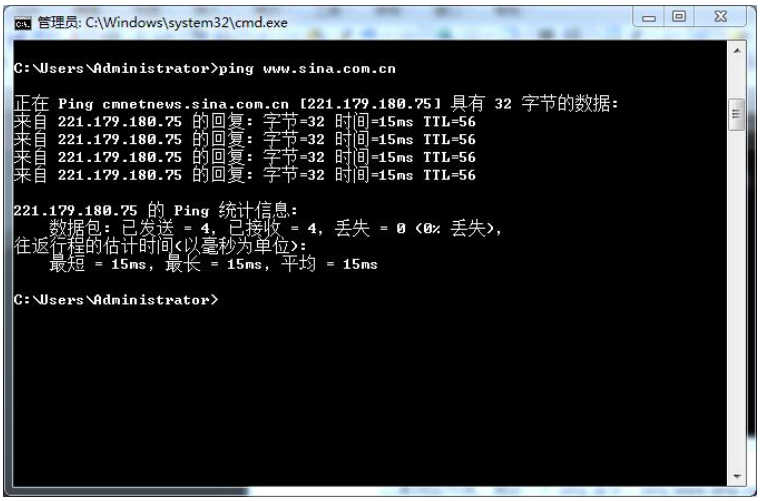

图 2-9　ping 网站主机的 TTL 返回值

TTL=56，说明www.sina.com.cn 使用的是 Linux主机。

（2）可以 ping 出一个网站的 IP 地址：ping www.baidu.com，得到当时这个网站绑定的 IP 地址为：111.13.100.92，如图 2-10 所示。

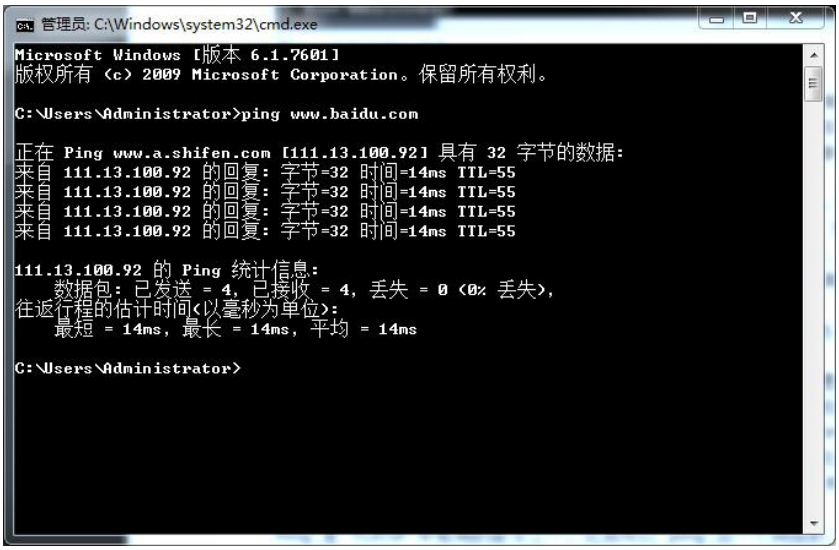

图 2-10　百度服务器的 IP 地址

（3）ping 本机命令“ping 127.0.0.1”，是为了检查本地的 TCP/IP 协议是否正常，但它仅是查看该协议是否正常，即使网卡禁用或者没有接入网络也都会返回正常，如图 2-11 所示。

图 2-11　检查本地 IP 图

3. 网络状态与资源共享——net

在命令提示符窗口下输入 net 命令，net 命令格式如图 2-12 所示。

参数之间用|分隔，下面分类进行介绍。

（1）net start。

命令行输入 net start，将显示启动的所有服务，如图 2-13 所示。

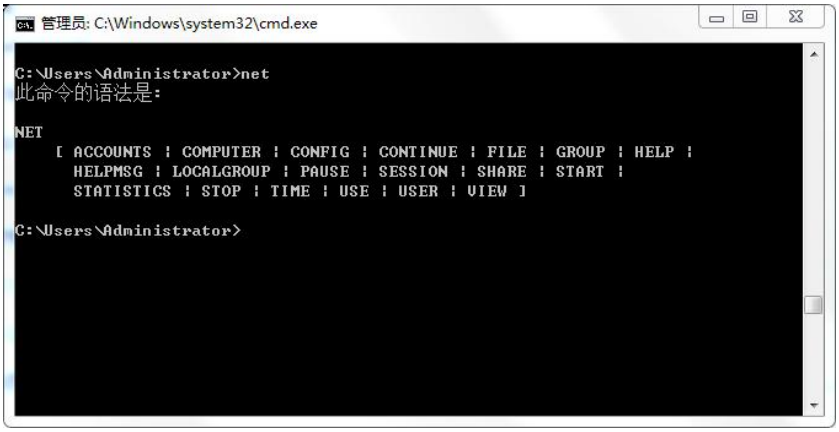

图 2-12　net 命令图

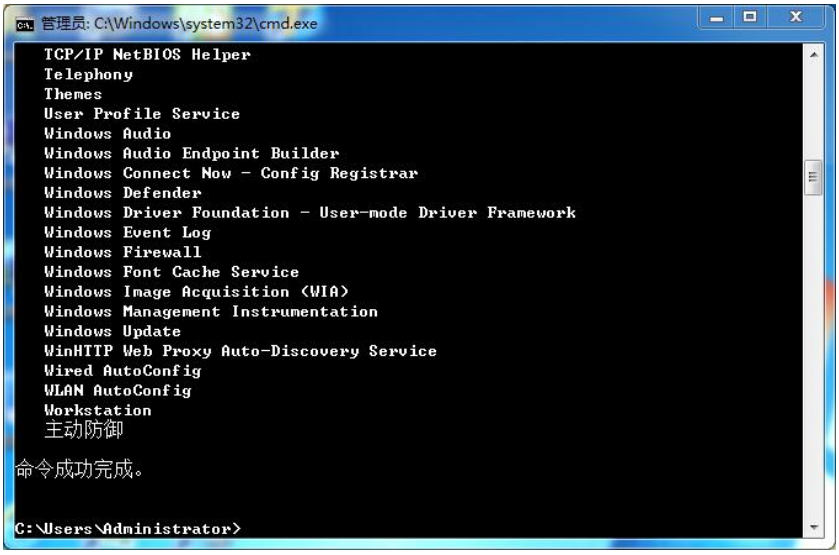

图 2-13　启动时的服务显示

（2）net view。

命令行输入 net view 用于显示计算机上所有共享资源的列表。当不带选项使用本命令时，它会显示当前域或网络上的计算机列表。

查看共享资源前，首先设置一个共享目录，在共享目录上右击，弹出的快捷菜单中选择“共享”命令中的“高级共享”命令，在“共享”对话框中选择“高级共享”命令，选择“共享此文件夹”复选框，设置文件的共享。这样将文件夹在局域网共享，局域网中的其他主机设备就可以访问共享文件夹，如图 2-14 所示。

在本机输入 net view 命令，可以显示相关信息。

4. 网络连接——netstat 命令

netstat 命令是在内核中访问网络及相关信息的命令，能够显示协议统计和当前 TCP/IP 的网络连接。也就是说，netstat 是一个观察网络连接状态的实用工具，可检验 IP 的当前连接状态。

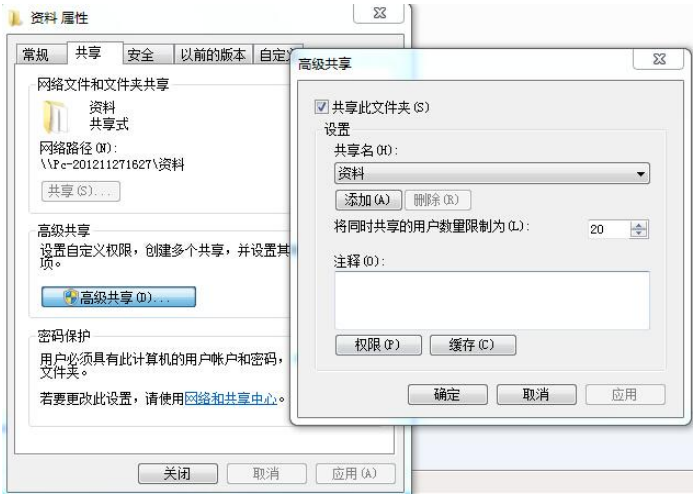

图 2-14　设置文件夹共享

命令格式为：netstat [-a][-b][-e][-n][-s][-r]

- 在命令提示符中输入“netstat -a”命令，可显示所有网络连接和侦听端口，如图 2-15 所示。

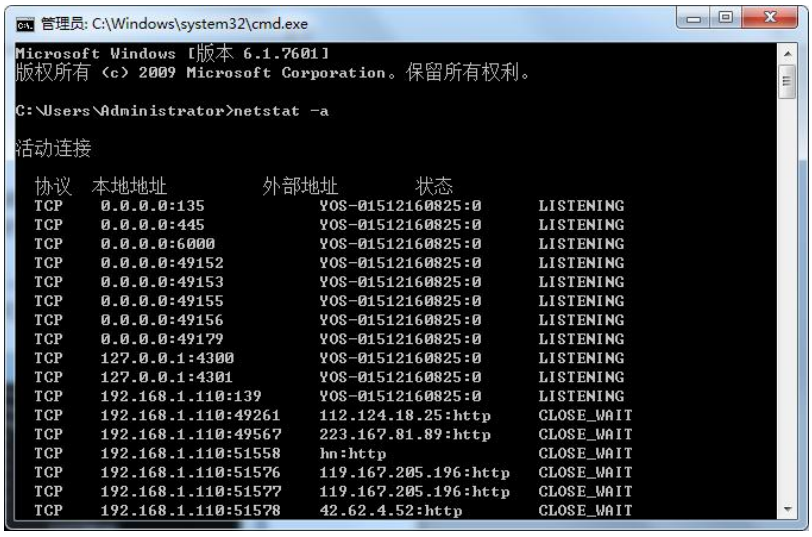

图 2-15　网络连接和侦听端口

第一列为协议，第二列为本地地址，第三列是外部地址，即与本机连接的主机或用户的 IP 地址，冒号后为端口号，第四列为状态。

- 在命令提示符窗口中输入“netstat -b”命令，可显示在创建网络连接和侦听端口时所涉及的可执行程序，如图 2-16 所示。
- 在命令提示符窗口中输入“netstat -n”命令，可显示已创建的有效连接，并以数字的形式显示本地地址和端口号。
- 在命令提示符窗口中输入“netstat -s”命令，可显示每个协议的各类统计数据，查看网络存在的连接，显示数据包的接收和发送情况。

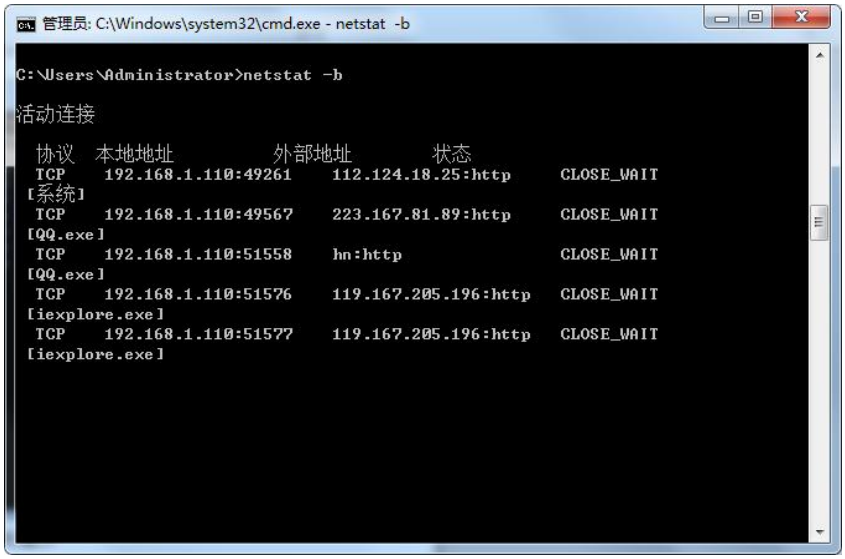

图 2-16　网络连接的程序

- 在命令提示符窗口中输入“netstat -e”命令，可显示关于以太网的统计数据，包括传送的字节数、数据包、错误等。
- 在命令提示符窗口中输入“netstat -r”命令，可显示关于路由表的信息，还显示当前的有效连接。

这里不再一一举例，学生自行实验。

5. 查看网络路由节点——tracert 命令

tracert 命令是可以显示信号到达目标经过的各个路由器。常见的使用方法是在 tracert 命令后加参数，例如输入 tracert www.baidu.com 就表示本机在访问 baidu.com时经过了哪些路由器，检测主机经历了哪些路由节点。当网络出现问题时，可以有针对性地检测，如图 2-17 所示。

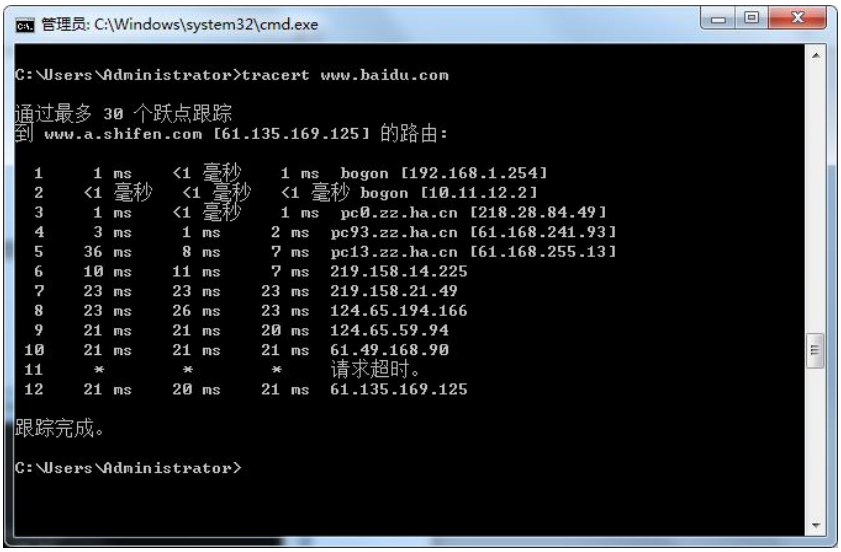

图 2-17　跟踪路由信息

【小知识】tracert 命令可以显示信号到达目标经过的各个路由器，从而判断问题所在节点；而 ping 命令是检测网络是否畅通的常用命令。两者经常配合使用，一个是反馈各动态或静态路由节点信息，一个是检测网络通道是否畅通，有无丢包及反应时间。

6. 远程登录主机——Telnet 命令

Telnet 只是一种远程登录的工具。一旦入侵者与远程主机建立了 Telnet 连接，入侵者便可以使用目标主机上的软、硬件资源，而入侵者的本地机只相当于一个只有键盘和显示器的终端而已。

在调试网络端口是否通畅的时候经常会使用到 Telnet 命令，但是在 Windows 7 系统下这个命令默认是不开启的，下面就告诉大家如何在 Windows 7 下开启 Telnet 命令。

在“开始”程序里，单击“控制面板”命令，在“控制面板”窗口里，单击“程序和功能”选项；在“程序”选项下，单击“打开或关闭 Windows 功能”；在打开的对话框中，找到“Telnet 客户端”，勾选前面对应的复选框，如图 2-18 所示。

图 2-18　Windows 7 开启 Telnet 服务

然后单击“确定”按钮，等待几分钟，系统将会开启 Telnet 客户端服务。为了验证 Telnet 服务命令是否开启成功，可以在“cmd”命令下测试一下，这个时候就不会再提示 Telnet 命令无法找到了。

如果开启了 Telnet 服务，就可以使用 Telnet 命令进行远程连接。

7. IP 地址的查找

前面介绍了 IP 地址和端口的含义，那么攻击者是如何找到互联网用户的 IP 地址进行攻击呢？下面就介绍几种查询 IP 地址的方法，知道了这些技术细节就可以做好防范，保护自己的 IP 地址不被泄露，防止攻击者的恶意攻击。

（1）ping 命令法。

若要查询一个网站服务器对应的 IP 地址，可以使用系统自带的 ping 命令，例如查询 www.pyvtc.cn 这个网站服务器的 IP地址时，可以先打开系统的“运行”对话框，然后输入 ping

www.pyvtc.cn命令，单击“确定”按钮即可，在弹出的窗口中就能知道要查询网站的 IP 地址，如图 2-19 所示。

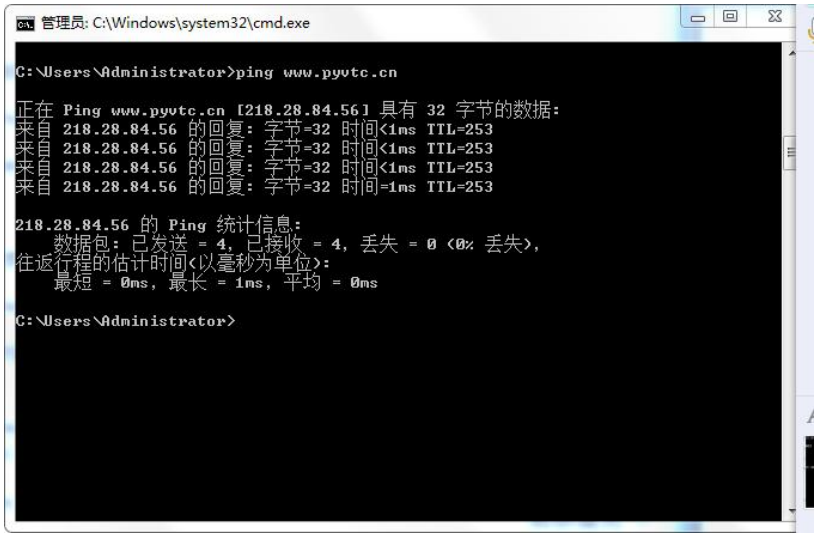

图 2-19　网站服务器的 IP 地址

如图 2-19 所示，www.pyvtc.cn 的服务器 IP 地址为 218.28.84.56。同种的方法可查询其他网站服务器的 IP 地址。

（2）netstat 命令查询法。

这种方法是通过 Windows 系统内置的网络命令 netstat 来查出对方的 IP 地址的，操作过程如下：

第 1 步：选择“开始”菜单下的“运行”命令，在弹出的“运行”对话框中输入“cmd”命令，单击“确定”按钮后，将屏幕切换到 MS-DOS 工作状态。

第 2 步：打开一个 QQ 好友窗口，然后给对方发送消息，如图 2-20 所示。

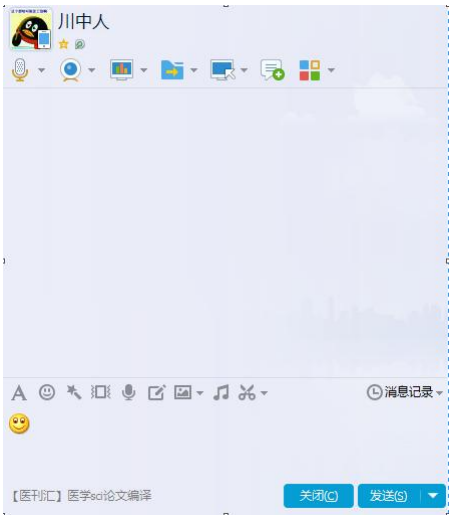

图 2-20　向好友发送消息

第 3 步：在 DOS 命令中执行 netstat -n 命令，在弹出的界面中就可以看到当前有哪些地址已经和本机建立了连接。如果对应某个连接的状态显示为 ESTABLISHED，表示本机和对方计算机之间的连接是成功的，如图 2-21 所示。

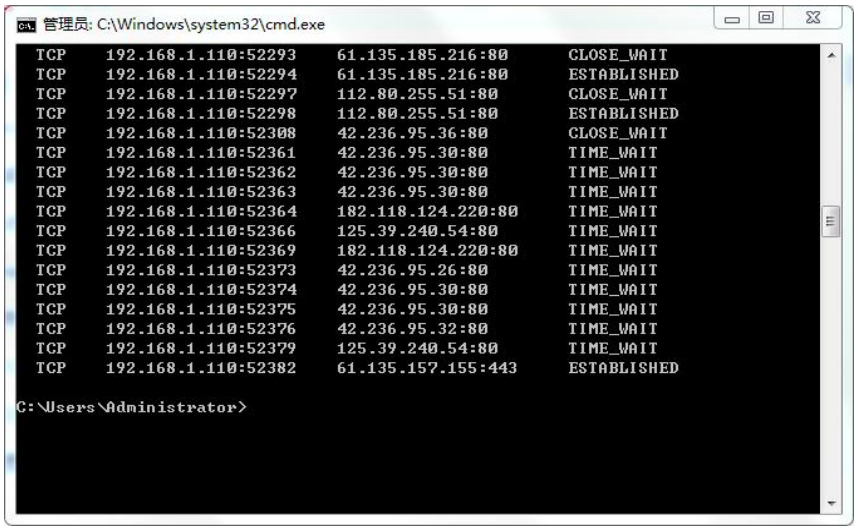

图 2-21　本机的连接状态

第 4 步：图 2-21 中可看到共有多个连接，其中开放 443 端口服务的主机是腾讯的服务器，剩下的就是对方的 IP 地址 61.135.157.155。

第 5 步：将 61.135.157.155 地址放到以下网址 www.123.cha.com 查询，就可以知道对方的地址，如图 2-22 所示。

图 2-22　查询 IP 所在地

第 6 步：打开对方的“查看用户信息”窗口，可以确认一下对方的地址信息和查询的地址信息是否一致。

【思考与练习】

实训题

1．查看本机网络连通情况以及本机的 IP 地址。
2．查看本机网络路由节点。

任务 3　搭建网络测试工作站

【任务描述】

许多网络攻防实验会造成本机操作系统的损毁及数据的破坏等后果，那么怎样才能既不损害本机又能进行攻防实验呢？虚拟机就可以解决这个问题。

虚拟机是通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。虚拟系统生成现有操作系统的全新虚拟镜像，它具有真实 Windows 系统完全一样的功能，进入虚拟系统后，所有操作都是在这个全新的独立的虚拟系统中进行，可以独立安装运行软件，保存数据，拥有自己的独立桌面，不会对真正的系统产生任何影响，而且具有能够在现有系统与虚拟镜像之间灵活切换的一类操作系统。

该怎样安装使用虚拟机呢？

【任务要求】

了解并掌握如何安装虚拟机。

了解并掌握如何使用虚拟机。

【知识链接】

当遇到一些暂时无法解决的问题时，需要进行频繁的测试，例如各种攻防的实践或者漏洞、工具的测试等操作，会对自己的计算机的操作系统产生一定的破坏，如何才能安全有效地进行各种实践和测试呢？VMware 软件可以搭建起一个庞大的网络实验室，它是一个“虚拟机”软件，可以实现不需要重新启动计算机就能在同一台计算机中使用多个操作系统。

【实现方法】

1．安装 VMware 软件

下面以 VMware 为例，介绍一下其安装过程，可参照步骤搭建测试环境。

第 1 步：双击安装文件，弹出 Welcome to the installation wizard for VMware Workstation 对话框，如图 2-23 所示。

第 2 步：单击 Next 按钮，弹出 License Agreement（VMware 安装协议）对话框，如图 2-24 所示。

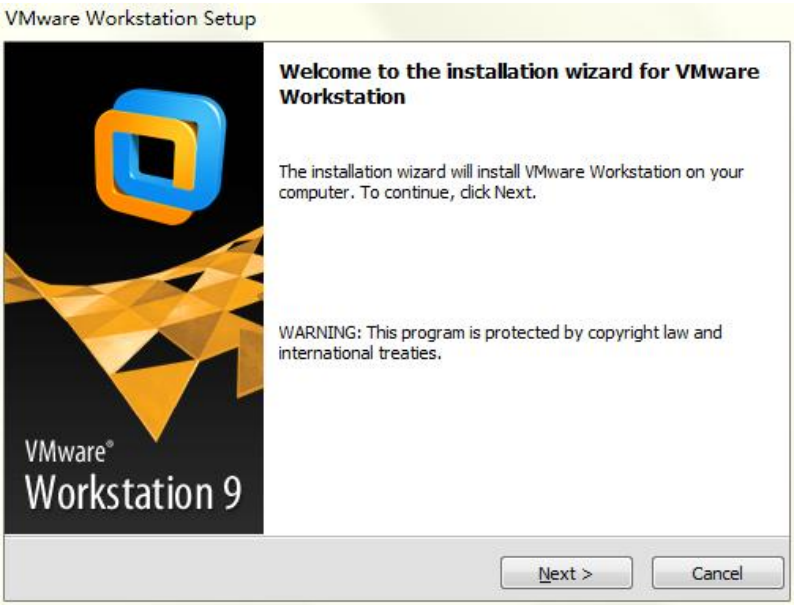

图 2-23　VMware 的欢迎界面

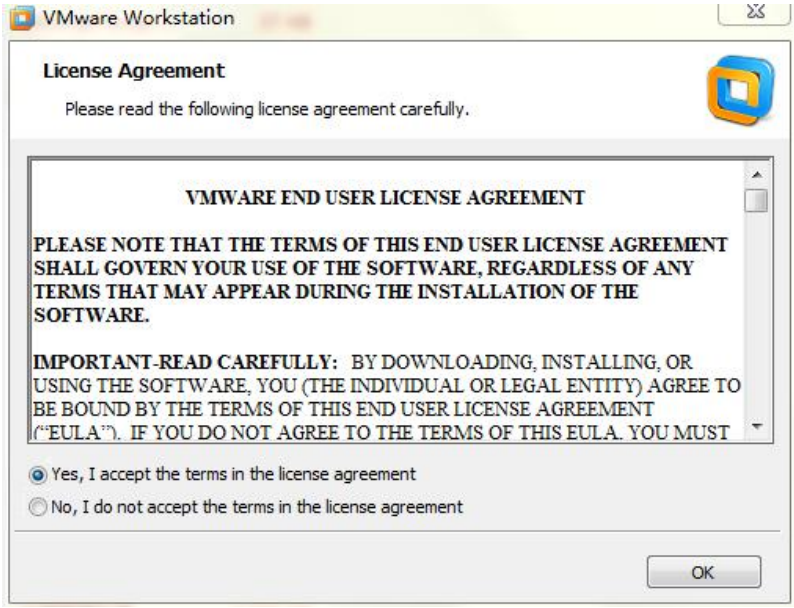

图 2-24　同意安装协议

第 3 步：选择 Yes,I accept the terms in the license agreement 单选按钮，单击 Next 按钮，弹出 Destination Folder（选择安装路径）对话框，如图 2-25 所示。

第 4 步：程序默认有一个安装路径，若想改变其安装路径，单击 Change 按钮，选择好安装路径后，单击 Next 按钮，弹出 Shortcuts（设置快捷方式）对话框，如图 2-26 所示。

第 5 步：保持默认值，勾选两个复选框，单击 Next 按钮，弹出 Ready to Perform the Requested Operations（准备安装）对话框，如图 2-27 所示。

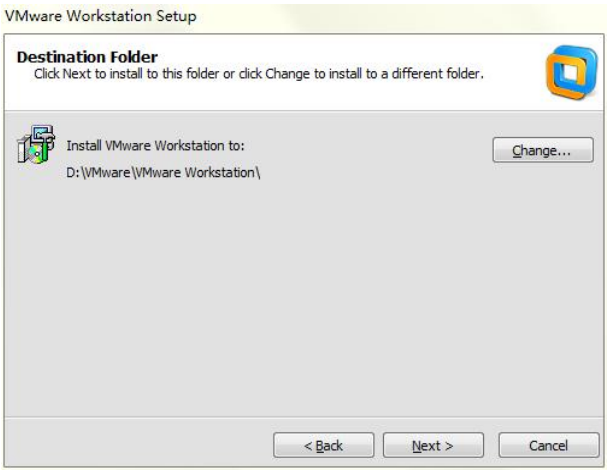

图 2-25　选择安装路径

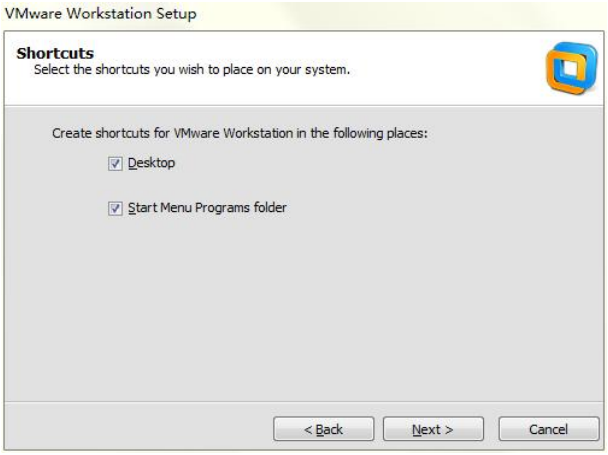

图 2-26　设置 VMware 快捷方式

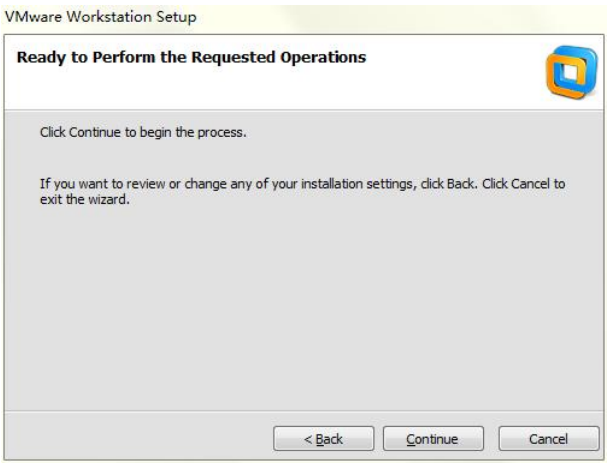

图 2-27　准备安装 VMware

第 6 步：单击 Continue 按钮，弹出对话框，如图 2-28 所示。

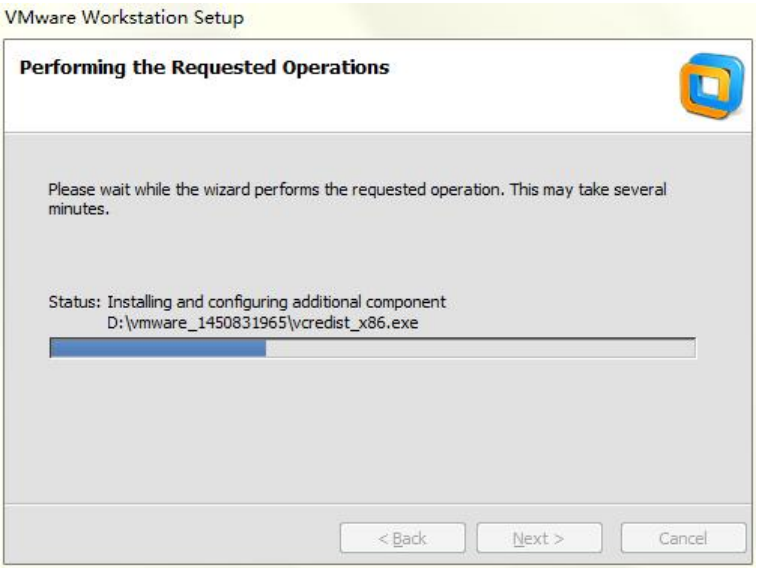

图 2-28　正在安装

第 7 步：单击 Finish 按钮，VMware 安装完成，如图 2-29 所示。

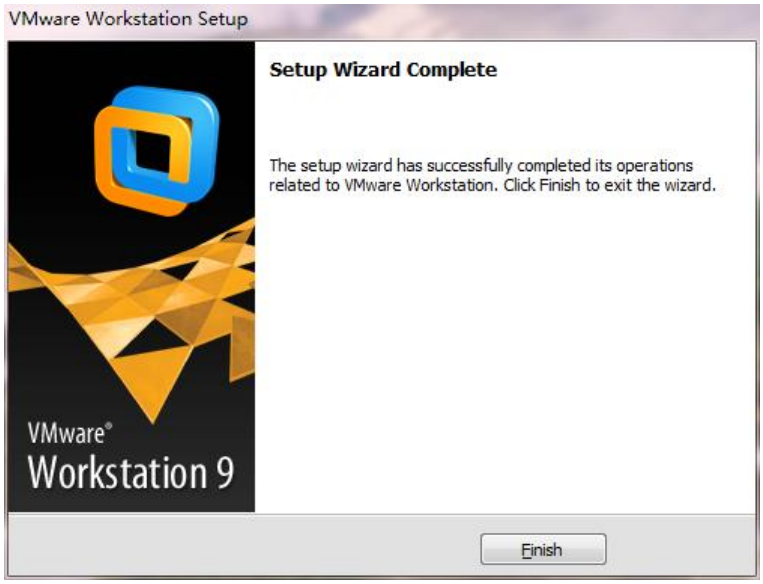

图 2-29　VMware 安装完成

2. 配置 VMware 并安装操作系统

VMware 安装完成后，桌面上将出现 VMware Workstation 字样的图标。双击这个快捷图标启动 VMware，主界面如图 2-30 所示。

这时，VMware 只相当于一台裸机，需要为其安装操作系统。操作步骤如下：

第 1 步：选择 File 菜单下的 New Virtual Machine 命令，如图 2-31 所示。

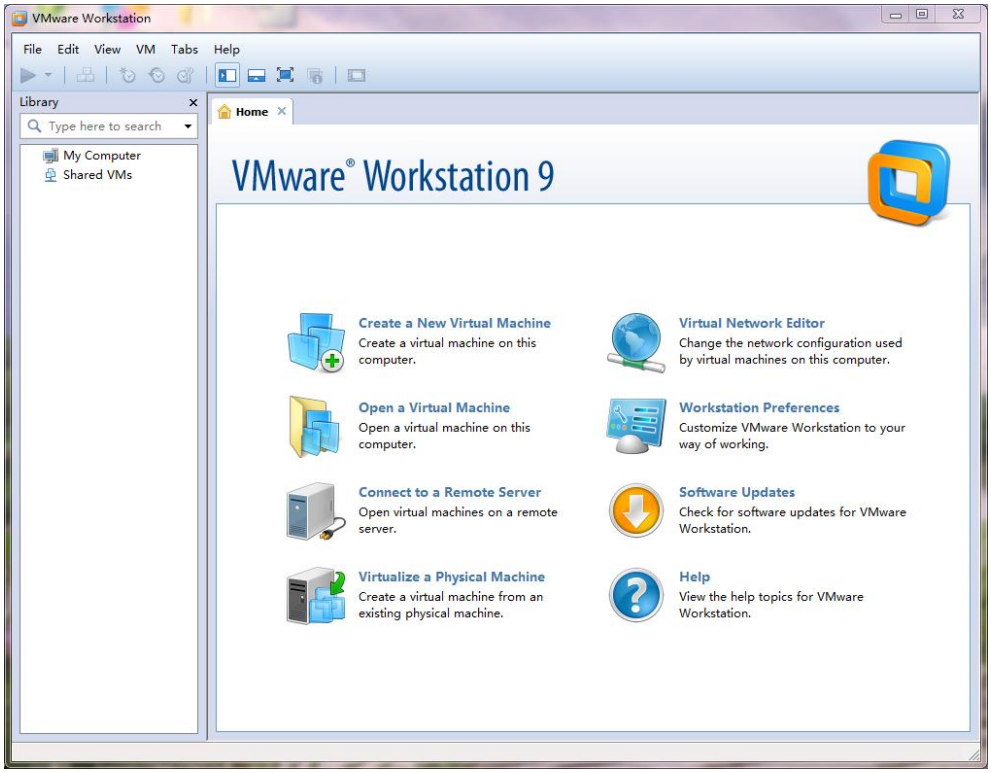

图 2-30　VMware 主界面

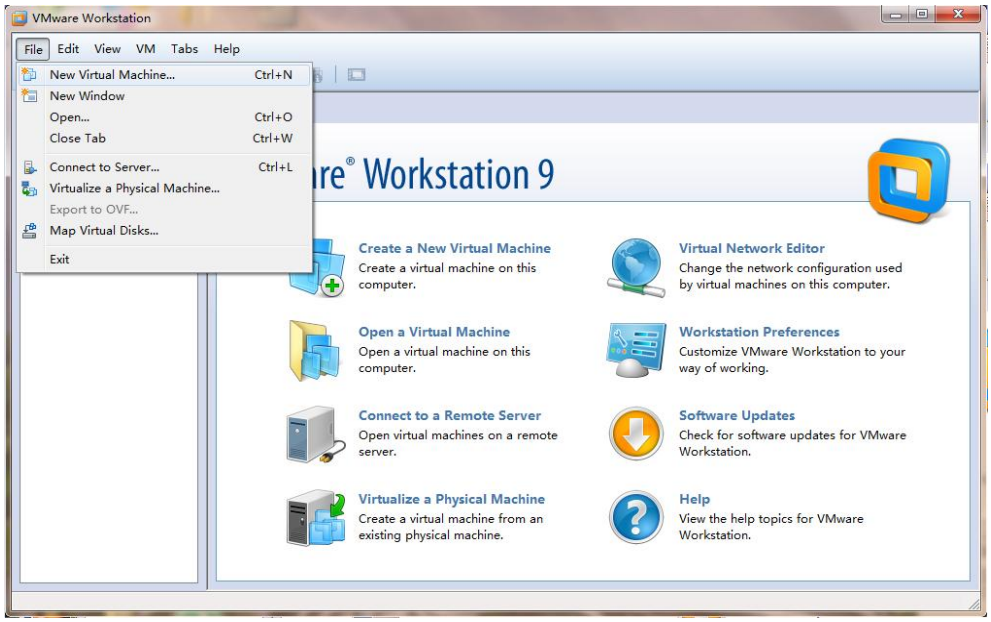

图 2-31　创建新的虚拟操作系统

弹出 Welcome to the New Virtual Machine Wizard（操作系统类型选择）界面，选择操作系统类型，单击 Next 按钮，如图 2-32 所示。

图 2-32　操作系统类型选择界面

在图中有两个配置选项，如果安装的是 Windows、Linux 或者其他 VMware 已经配置的操作系统，则选择 Typical 单选按钮。而 Custom 选项一般用于那些正在开发的系统进行测试的时候。在此选择 Typical 单选按钮。

第 2 步：单击该按钮后，弹出 Select a Guest Operating System（不同版本的操作系统选择）对话框，如图 2-33 所示。

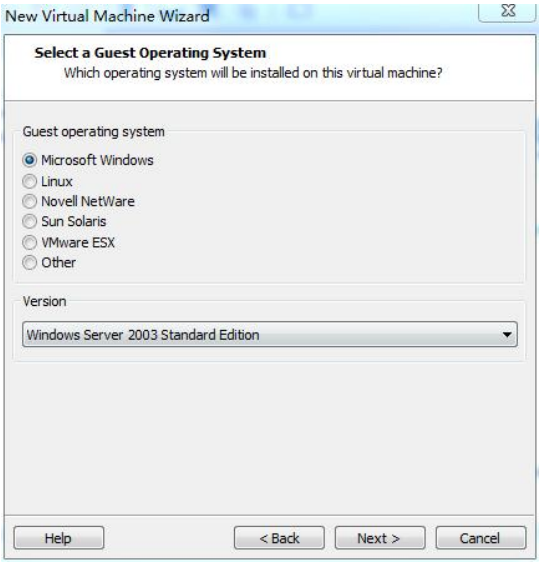

图 2-33　选择操作系统及系统版本

本书中使用的是 Windows Server 2003 Standard Edition，因此 Guest operating system 选项

选择 Microsoft Windows 单选按钮；在 Version 下拉列表框中选择 Windows Server 2003 Standard Edition 选项。

第 3 步：选择完成后，单击 Next 按钮，弹出 Name the Virtual Machine（虚拟机命名及路径）对话框，如图 2-34 所示。

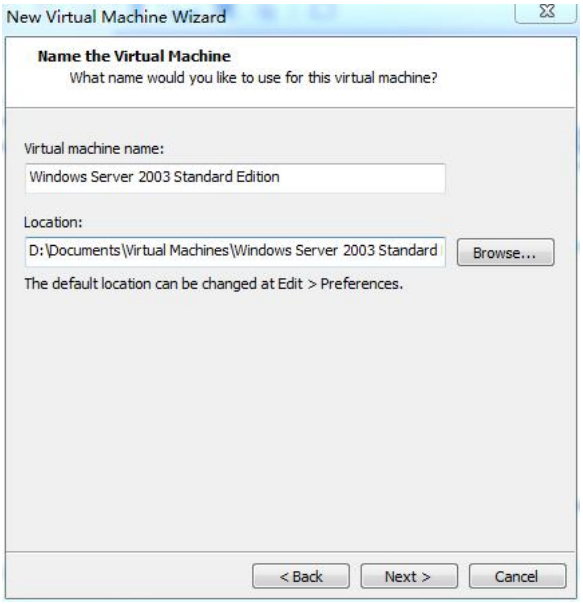

图 2-34　虚拟机命名及路径

第 4 步：单击 Next 按钮，弹出 Specify Disk Capacity（为虚拟机分配空间）对话框，如图 2-35 所示。

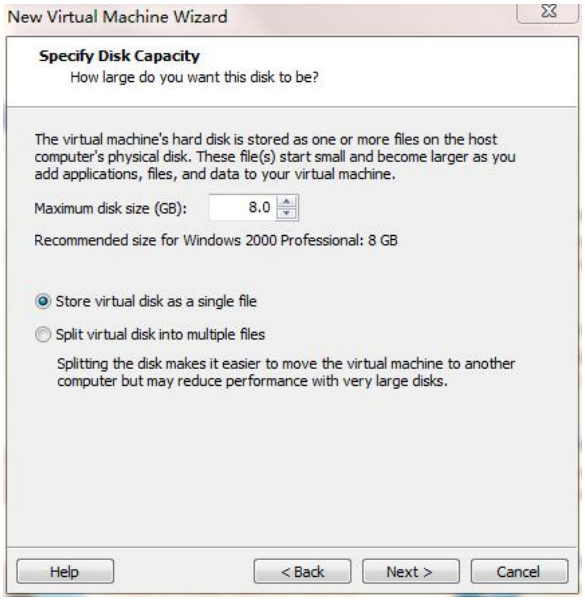

图 2-35　为虚拟机分配空间

第 5 步：分配空间后，单击 Next 按钮，单击“完成”按钮，虚拟机配置完成，如图 2-36 所示。

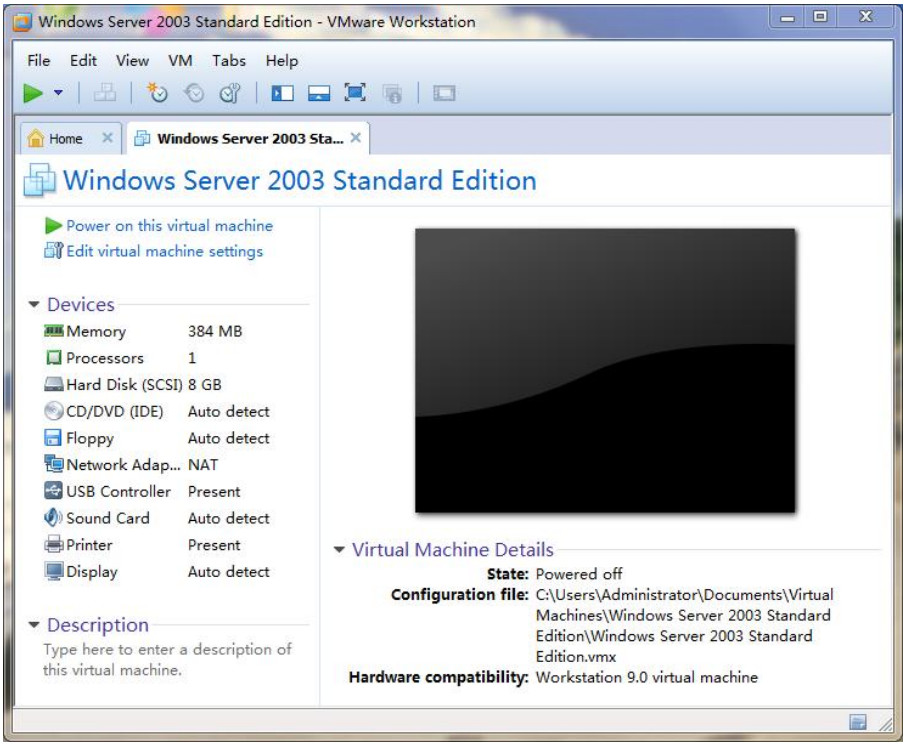

图 2-36　虚拟机配置完成

第 6 步：在虚拟机中安装操作系统，系统安装结束，进入操作系统。

【思考与练习】

实训题

安装 VMware 9 虚拟机软件，在虚拟机上安装加密软件。