防黑防毒防钓大作战

武新华　刘　岩　等编著

- **安防专家讲解，**揭秘多种黑客工具，确保网络安全
- **实战攻防互动，**剖析黑客入侵技术，提供防御措施
- **真正通俗易懂，**全面揭露防黑防毒防钓作战全过程
- **视频图解实例，**彻底打破电脑初学者的知识壁垒

随书附赠CD-ROM

清华大学出版社

防黑防毒防钓大作战

武新华　刘　岩　等编著

清华大学出版社
北 京

内 容 简 介

在如今这个信息时代，互联网在人们的工作学习中发挥了越来越大的作用，但目前大多数人的网络信息安全意识还很薄弱，给黑客和别有用心者留下可乘之机。本书的主要目的就是让读者在尽可能短的时间内，了解黑客的起源、常用工具以及攻击方式，并在熟悉网络信息安全基本知识的前提下，掌握基本的反黑知识、工具和修复技巧，并采取相应的方法来制订自救措施。

本书内容全面丰富，图文并茂，深入浅出，适用于广大互联网爱好者，同时还可供网络信息安全从业人员及网络管理员作为速查手册使用。

图书在版编目(CIP)数据

防黑防毒防钓大作战/武新华，刘岩等编著. —北京：清华大学出版社，2009.2

ISBN 978-7-302-19457-6

Ⅰ. 防…　Ⅱ. ①武…　②刘…　Ⅲ. 计算机网络—安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 010658 号

责任编辑：邹　杰
装帧设计：杨玉兰
责任校对：李玉萍
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：190×260　**印　张**：21.75　**字　数**：525 千字
版　　次：2009 年 2 月第 1 版　　**印　　次**：2009 年 2 月第1 次印刷
附光盘 1 张
印　　数：1～4000
定　　价：38.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：027528-01

前　言

随着社会各方面对网络技术的依赖性不断地增加，人们在体验互联网带来极大便利的同时，黑客入侵和网络安全也同样困扰着网络的发展，如僵尸网络(Botnet)、网络仿冒(Phishing)、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件和木马产业链的曝光等，使得网络安全问题成为大家关注的重点。

由于互联网本身的复杂性、开放性等特点，网络的安全性已成为阻碍信息化进程的重要因素，其影响已从互联网领域逐步扩大到政府、通信、广电、金融、电力、交通等应用和建设领域，网络安全问题已引起了全世界的密切关注，黑客的恶意行为已成为全球新的公害。

大家或许都曾碰到过这样的情况，正当自己为精彩的网页着迷时，突然硬盘狂响不止，最后发现所有的程序都不能运行了；正在给网友写 E-mail 时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的计算机！”；正在聊天室里与网友激情聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录 QQ 时却突然提示密码错误，试遍所有可能用过的密码却依然不能通过，这时才发现自己的 QQ 密码被盗了。

因此，就必须采取有力措施加强网络的自身安全防护性能，以有效地抵抗入侵和攻击破坏性。但随着攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生，攻击点也越来越趋于集中化和精确性，攻击破坏的影响面不断扩大并产生连环效应，这就势必需要构筑一种主动的安全防御措施，才有可能最大限度地有效应对攻击方式的变化。

本书的写作目的主要是通过介绍黑客的攻击手段以提供相应的主动防御保护措施，使读者能够循序渐进地了解防御黑客入侵的关键技术与方法，提高安全防护意识，在实际遇到黑客攻击时能够做到“胸有成竹”。希望读者能够运用本书介绍的知识去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书特别注重实例的使用，针对每一种攻防手段，都结合实例来进行介绍，并紧紧围绕黑客的“攻与防”这一主线，告诉读者如何建立个人计算机的安全防护措施，使自己远离黑客攻击的困扰，确保自己计算机数据的安全。

本书通俗易懂、图文并茂，即使是计算机新手也能无障碍阅读；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让用户“先下手为强”；先了解攻防互参的防御方法，全面确保用户的网络安全。

本书适合经常上网但缺乏网络安全和黑客知识的人员阅读，也可作为计算机网络爱好者的自学教材。

本书由众多经验丰富的高校教师编写，其中第 1 章由张克歌编写，第 2 章由李秋菊编写，第 3 章由陈艳艳编写，第 4 章由李防编写，第 5 章由杨平编写，第 6 章由段玲华编写，第 7 章由王英英编写，第 8、9、10 章由刘岩编写，第 11 章由武新华编写，第 12 章由孙世宁编写，最后由武新华统审全稿。由于作者水平有限，书中的疏漏之处在所难免，恳请广大读者批评指正。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后一定不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负。

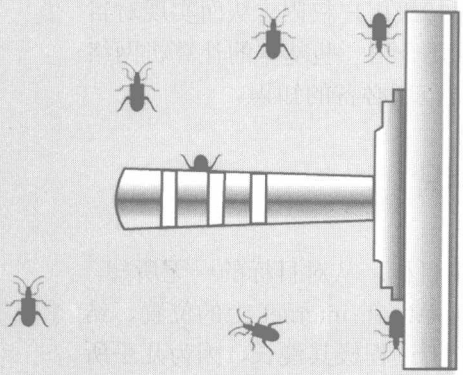
为便于读者阅读和理解，本书在写作时使用了如下图标约定。

提示：对文章中所涉及的一些内容进行特别描述，提醒读者注意操作到此处时，切忌不要犯的一些常识性错误。

说明：提示读者文中所述内容的一些相关信息，并对文中表述不清的内容进行进一步阐述。

技巧：对实际操作中的一些小技巧进行阐述，教给读者应该如何进行具体操作。

目　录



第 1 章

黑客必备的网络知识

重点提示

- 计算机网络基础知识
- 黑客的惯用伎俩——扫描端口
- 一般常用网络命令

本章精粹

了解黑客的相关知识不仅有助于防止黑客攻击，还可让自己在被攻击、侵犯时有一定的防范能力。本章将重点介绍与黑客有关的一些基础知识，让读者更好地掌握防止黑客攻击的基本理论。

黑客入侵一个系统要经过很多步骤，其最终目的是为了获得超级用户权限，从而实现对目标系统的绝对控制，获取自己所需资源或对其进行破坏。本章主要介绍一些基本的计算机网络知识、网络端口及一些常用的网络命令，这些都是黑客攻击与防范所必备的知识。

1.1 计算机网络基础知识

不管黑客进入目标系统要做些什么，第一步都是先确定攻击目标。从对目标的一无所知，到掌握与之相关的大量信息，需要黑客进行种种尝试。确定目标系统在 Internet 上的位置、结构，外围安全设备类型和结构之后确定入侵点。信息的搜集和分析过程极其漫长，因为几乎所有有关攻击目标的信息都有可能是入侵点。即使像操作系统类型、版本、用户名这些表面上无害的信息，也有可能会不经意地暴露系统的漏洞信息。

1.1.1 为什么要使用 IP

IP 地址(Internet Protocol Address)用来标识计算机网络中的通信实体，如一台主机或路由器的某一个端口。而基于 IP 协议在网络中传输的数据包，也都必须使用 IP 地址来标识，就如同我们写信要标明收信人的通信地址和发信人的地址，而邮政工作人员则通过该地址来进行邮件的投递。

同样的过程也发生在计算机网络中，每个传输的数据包都要包括的一个源 IP 地址和一个目的 IP 地址，当该数据包在网络中进行传输时，这两个地址要保持不变，以确保网络设备总是能根据确定的 IP 地址，将数据包从源通信实体送往指定的目的通信实体。

目前，IP 地址使用 32 位二进制地址格式，为方便记忆，通常使用以点号划分的十进制(即点分十进制表示法)来表示，例如 202.112.14.1。 一个 IP 地址主要由两部分组成：一部分用来标识该地址所属的网络号；另一部分用来指明该网络上某个特定主机的主机号。

为了给不同规模的网络提供必要的灵活性，IP 地址的设计者将 IP 地址空间划分为 5 个不同的地址类别，其中 A，B，C 三类最为常用。

- A 类 IP 地址：一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，地址范围从 0.0.0.1～126.0.0.0。可用的 A 类网络有 126 个，每个网络能容纳 1 亿多个主机。
- B 类 IP 地址：一个 B 类 IP 地址由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从 128.0.0.0～191.255.255.255。可用的 B 类网络有 16382 个，每个网络能容纳 6 万多个主机。
- C 类 IP 地址：一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是“110”，范围从 192.0.0.0～223.255.255.255。C 类网络可达 209 万个，每个网络能容纳 254 个主机。
- D 类地址：其 IP 地址第一个字节以“1110”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播(Multicast)中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

- E 类 IP 地址：以“11110”开始，预备将来使用。
- 全零(0. 0. 0. 0)地址：对应于当前主机。全“1”的 IP 地址(255. 255. 255. 255)是当前子网的广播地址。

所有的 IP 地址都由国际组织 NIC(Network Information Center，网络信息中心)统一分配。目前全世界共有三个这样的网络信息中心：InterNIC(负责美国及其他地区)、ENIC(负责欧洲地区)和 APNIC(负责亚太地区)。

我国申请 IP 地址要通过 APNIC，APNIC 的总部设在日本东京大学。申请时要考虑申请哪一类的 IP 地址，然后向国内的代理机构提出。网络号由因特网权力机构分配，目的是为了保证网络地址的全球唯一性。主机地址由各个网络的管理员统一分配，因此 IP 地址的全球唯一性确保了网络地址的唯一性与网络内主机地址的唯一性。

1.1.2　了解网络协议

网络协议是网络上所有设备(网络服务器、计算机及交换机、路由器、防火墙等)之间通信规则的集合，它定义了通信时信息必须采用的格式及其意义。大多数网络都采用分层的结构体系。一台设备上的第 n 层与另一台设备上的第 n 层进行通信的规则就是第 n 层协议。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。

常见的协议有：TCP/IP 协议、IPX/SPX 协议、NetBEUI 协议等。

- TCP/IP 协议

  TCP/IP 协议(Transmission Control Protocol/Internet Protocol，传输控制协议/Internet 协议)是一种网络通信协议，它规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式及传送方式。

  TCP/IP 协议是 Internet 中的基础协议，也是一种数据打包和寻址的标准方法。在数据传送中，可以形象地将 TCP 和 IP 理解为两个信封。要传递的信息被划分为若干段，每一段塞入一个 TCP 信封，并在该信封上记录分段号的信息，再将 TCP 信封塞入 IP 大信封，发送上网。在接收端，有一个 TCP 软件包收集信封，抽出数据，按发送前的顺序还原并加以校验，若发现差错，TCP 将会要求重发。

  因此，TCP/IP 在 Internet 中几乎可以无差错地传输数据。对普通用户来说，并不需要了解网络协议的整个结构，仅需了解 IP 的地址格式，即可与世界各地进行网络通信。

- IPX/SPX 协议

  该协议是由 Novell 公司开发的应用于局域网的高速协议，它和 TCP/IP 协议的区别在于不使用 IP 地址，而是使用网卡的物理地址，即(MAC)地址。在实际使用中基本不需要什么设置，装上即可使用。由于它在网络普及初期发挥了巨大的作用，所以得到了很多厂商的支持，包括 Microsoft 等，到现在很多软件和硬件也都支持这种协议。

- NetBEUI 协议

  NetBEUI 协议(NetBIOS Enhanced User Interface，NetBIOS 增强用户接口)是 NetBIOS 协议的增强版本，曾被许多操作系统采用，例如 Windows for Workgroup、Windows 9x 系列、Windows NT 等。NetBEUI 协议可用于多种情况，是 Windows 98 之前的操作

系统的默认协议。

总之，NetBEUI 协议是一种短小精悍、通信效率很高的广播型协议，安装后不需要进行设置，特别适合在“网络邻居”中传送数据。所以建议除 TCP/IP 协议之外，局域网内的计算机最好也安装 NetBEUI 协议。另外，如果一台只安装了 TCP/IP 协议的 Windows 9x 系统，要想加入到 WINNT 域，也必须安装 NetBEUI 协议。

在局域网中应用较多的是 IPX/SPX 协议。用户如果访问 Internet，则必须在网络协议中添加 TCP/IP 协议。

1.2 黑客的惯用伎俩——扫描端口

黑客在攻击某一台计算机之前，必须先扫描目标计算机的 IP 地址和端口，从中找到系统的漏洞之后再着手进行攻击入侵。

1.2.1 什么是端口

端口一直以来都是学习黑客知识的必由之路。

1. 端口的概念与作用

在网络技术中，端口(Port)大致有两种含义，物理意义上的端口(如 ADSL Modem、集线器、交换机、路由器等)用来连接其他网络设备的接口，如 RJ-45 端口、SC 端口等。逻辑意义上的端口一般指网络技术中 TCP/IP 协议涉及的端口，端口号的范围从 0 ～65535，例如用于浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

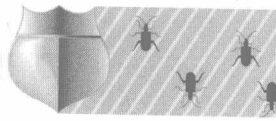
软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O(输入/输出)缓冲区。本地操作系统会给那些有需求的进程分配协议端口(Protocol Port，即常说的端口)，每个协议端口用一个正整数来标识，例如 80、139、445 等。当目的主机接收到数据包后，将根据包文头部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会接收数据并等待下一组数据的到来。

不仅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，以便接受方能顺利指数据包到这个端口。

一台拥有 IP 地址的主机可以提供许多服务，例如 Web 服务、FTP 服务、SMTP 服务等。这些服务完全可以通过 IP 地址来实现。主机是如何区分不同的网络服务呢？显然不能只靠 IP 地址，因为 IP 地址与网络服务是一对多的关系，所以实际上是通过“IP 地址+端口号”来区分不同的服务。

但端口并不是一一对应的，例如某台计算机作为客户机访问一台 WWW 服务器时，WWW 服务器使用“80”端口与该机通信，但该机则可能使用“3457”这样的端口。

入侵者通常会用扫描器对目标主机的端口进行扫描，以确定哪些端口是开放的。从开放的端口，入侵者可以知道目标主机大致提供了哪些服务，进而猜测可能存在的漏洞。因此，对端口的扫描可以帮助用户更好地了解目标主机，而对于管理员来说，扫描本机的开放端口也是做好安全防范的第一步。



2. 端口的分类

(1) 根据端口号可将端口划分为以下 3 类。

- 公认端口(WellKnownPorts)
  公认端口紧密绑定于一些服务，其范围是 0～1023。通常这些端口的通信明确表明了某种服务的协议，例如 80 端口实际上总是 HTTP 通信。
- 注册端口(RegisteredPorts)
  注册端口松散地绑定于一些服务，其范围是 1024～49151。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的，例如许多系统处理动态端口从 1024 左右开始。
- 动态和/或私有端口(Dynamicand/orPrivatePorts)
  其范围是从 49152～65535。理论上，不能为服务分配这些端口。实际上，计算机通常从 1024 起分配动态端口，但也有例外，SUN 的 RPC 端口从 32768 开始。

(2) 根据所提供的服务方式(协议类型)，端口又可分为“TCP 端口”和“UDP 端口”两种。一般直接与接收方连接大多采用 TCP 协议。如果只是把信息放在网上发布出去而不关心信息是否到达，也即“无连接方式”，这种方式则大多采用 UDP 协议。

使用 TCP 协议的常见端口主要有如下几种。

- FTP
  文件传输协议，使用 21 端口。某计算机开通了 FTP 服务便启动了文件传输服务，下载和上传文件都要用到 FTP 服务。
- Telnet
  一种用于远程登录的端口，用户能以自己的身份远程登录到计算机上，通过这种端口可提供一种基于 DOS 模式的通信服务。例如支持纯字符界面 B/S 的服务器会将 23 端口打开，以对外提供服务。
- SMTP
  现在很多邮件服务器使用 SMTP(简单邮件传输协议)来发送邮件。常见的免费邮件服务都使用此邮件服务端口，所以在电子邮件设置中经常会看到有 SMTP 端口设置栏，服务器开放的是 25 端口。
- POP3
  POP3 协议用于接收邮件，通常使用 110 端口。只要有使用 POP3 协议的程序(如 Outlook 等)，就可以直接使用邮件程序接收邮件(如使用 126 邮箱的用户就不必打开 Internet Explorer 来接收邮件了)。

使用 UDP 协议的常见端口主要有如下几种。

- HTTP 协议使用的 80 端口
  HTTP 是用户使用最多的协议，即“超文本传输协议”。在上网浏览网页时，就要在提供网页资源的计算机上打开 80 端口来提供服务。通常的“WWW 服务器”、“Web 服务器”等使用的就是 80 端口。
- DNS 协议使用的 53 端口
  DNS 用于域名解析服务，这种服务在 Windows NT 系统中用得最多。Internet 上的每一台计算机都有一个网络地址与之对应，这个地址就是 IP 地址，它以纯数字的形式

表示。但由于这种表示方法不便于记忆，于是就出现了域名。访问计算机只需要知道域名即可，域名和 IP 地址之间的变换由 DNS 服务器来完成(DNS 用的是 53 端口)。

- SNMP 协议使用的 161 端口
  SNMP 即简单网络管理协议，用来管理网络设备，使用 161 端口。
- QQ 使用的 8000 端口和 4000 端口
  QQ 程序既提供服务又接收服务，使用的是无连接协议，即 UDP 协议。QQ 服务器使用端口 8000 侦听是否有信息到来，客户端使用端口 4000 向外发送信息。

【提示】
在计算机的 6 万多个端口中，通常把端口号在 1024 以内的端口称为常用端口，这些常用端口所对应的服务通常情况下是固定的。

1.2.2 查看端口的方法

为了查找目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

Netstat 命令显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6 以及通过 IPv6 的 UDP 协议)等，在使用时如果不带参数，则 Netstat 显示活动的 TCP 连接。

命令格式：

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval] [/?]
```

各参数说明如下。

- -a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。
- -e：显示以太网的统计信息，例如发送和接收的字节数、数据包数等。该参数可以与 -s 结合使用。
- -n：显示活动的 TCP 连接，只以数字形式表现地址和端口号，却不尝试确定名称。
- -o：显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。可在 Windows 任务管理器的【进程】选项卡中找到基于 PID 的应用程序。该参数可与-a、-n 和-p 结合使用。
- -p：显示 Protocol 所指定的协议连接，可以是 TCP、UDP、TCPv6 或 UDPv6 等。如果该参数与-s 一起使用，按协议显示的统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6 等。
- -r：显示 IP 路由表的内容，该参数与 route print 命令等价。
- -s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 Windows XP 的 IPv6 协议，则显示有关 IPv6 上的 TCP、UDP、ICMP 等协议统计信息(可以使用-p 参数指定协议集)。
- Interval：每隔 Interval 秒重新显示一次选定的信息。按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，则 Netstat 将只打印一次选定的信息。
- /? ：在命令提示符下显示帮助信息。

与 Netstat 命令一起使用的参数，必须以连字符(-)而不是以短斜线(/)作为前缀。

Netstat 提供下列统计信息。

- Proto：协议的名称(TCP 或 UDP)。
- Local Address：本地计算机的 IP 地址和正在使用的端口号。如果不指定-n 参数，则显示与 IP 地址和端口名称对应的本地计算机名称。如端口尚未建立，端口以星号“*”显示。
- Foreign Address：连接到该插槽的远程计算机的 IP 地址和端口号码。如果不指定-n 参数，则显示与 IP 地址和端口相对应的名称。如端口尚未建立，则端口以星号“*”显示。
- State：表明 TCP 连接的状态。

Netstat 命令只有当网络协议(TCP/IP)协议在网络连接中，安装为网络适配器属性的组件时才可使用，具体表现如下。

- 显示以太网统计信息和所有协议的统计信息，输入命令“netstat -e -s”。
- 要仅显示 TCP 和 UDP 协议的统计信息，输入命令“netstat -s -p tcp udp”。

用户可以在命令提示符窗口中使用 Netstat 命令，具体使用实例如下。

步骤 1：在命令提示符窗口中输入“netstat -a”并按 Enter 键，即可显示用户计算机当前开放的所有端口，其中参数-a 的含义表示显示所有连接和侦听端口，如图 1-1 所示。

步骤 2：运行“netstat -s -e”命令，即可显示用户详细的网络信息，包括 IP、ICMP、TCP 和 UDP 的统计等，如图 1-2 所示。

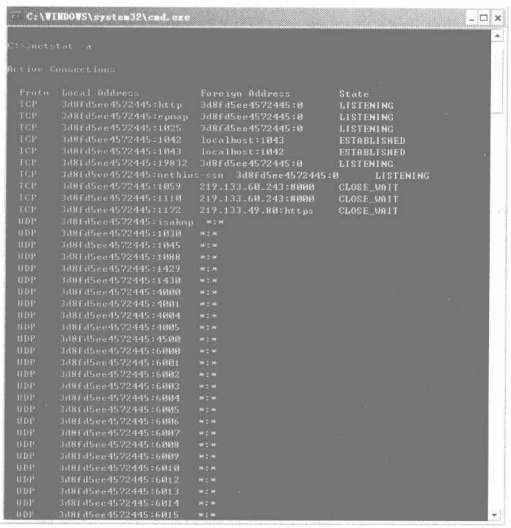


图 1-1　显示当前开放的所有端口

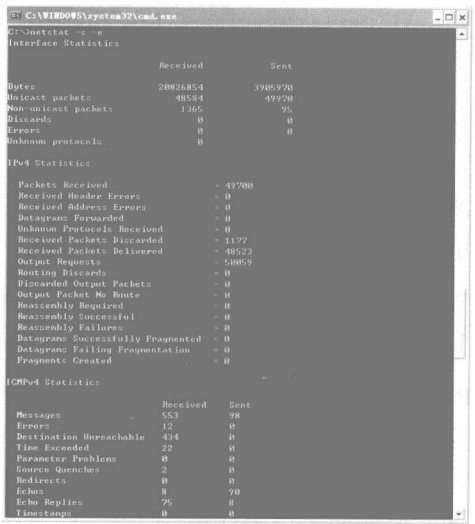


图 1-2　显示端口详细信息

步骤 3：如果运行“netstat -r”命令，则可显示内核路由表，如图 1-3 所示。

步骤 4：运行“netstat -a -n”命令，即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 1-4 所示。

【注意】

如果在管理员不知情的情况下打开了太多端口，则可能出现两种情况：一种情况是提供的服务管理员没有注意到，例如安装 IIS 服务时，软件就会自动地增加很多服务；

另一种情况是服务器被攻击者植入了木马程序，通过特殊的端口进行通信。这两种情况都比较危险，管理员不了解服务器提供的服务，就会减小系统的安全系数。

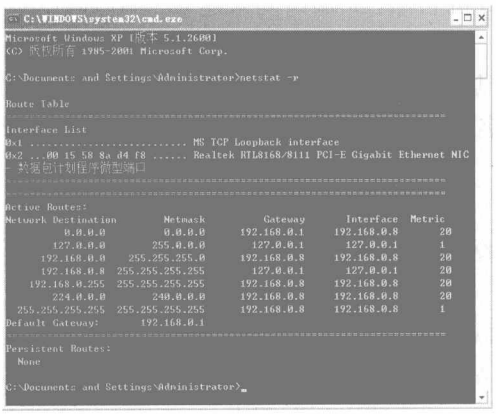


图 1-3　显示路由表

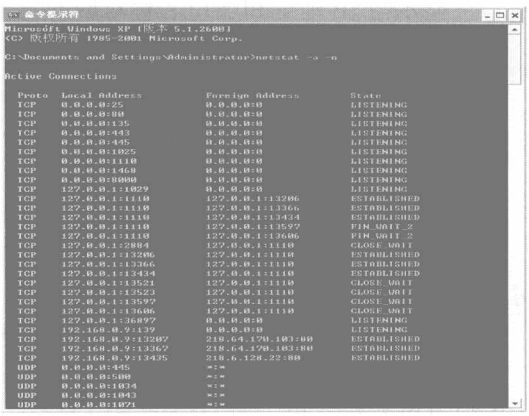


图 1-4　查看商品号状态

1.3　一些常用网络命令

在学习计算机网络基础知识的过程中，掌握一些常用的 Windows 自带的网络命令是非常必要的。

1.3.1　测试物理网络

测试物理网络的命令是 Ping，它是用来测试网络连接量的程序。它向目的地发送一个 ICMP 回声请求消息，并报告是否收到所希望的 ICMP 回声应答，校验与远程计算机或本地计算机的连接。

1. 认识 Ping 命令

Ping 命令只有在安装了 TCP/IP 网络协议的计算机中才能使用，主要用于验证连接到网络的计算机是否连通。TCP/IP 协议可在【本地连接 属性】对话框中进行设置，如图 1-5 所示。在设置好 TCP/IP 协议之后，就可以使用 Ping 命令了。

Ping 命令的工作原理是：利用用户的计算机向待验证连通与否的计算机发送一些包含特定数据的数据包，并等待这些计算机返回特定的数据包。

2. Ping 命令的使用

在【运行】对话框的【打开】文本框中输入“cmd”命令，单击【确定】按钮，即可打开 DOS 命令提示符窗口，其中的 Administrator 即为本计算机的名字，如图 1-6 所示。

在输入“cd\”返回到 C 盘根目录之后，再输入格式为“ping+空格+IP 地址”的命令，例如输入“ping 192.168.0.4”，如图 1-7 所示。其中 192.168.0.4 是目标地址，发送包大小是 32 字节。在命令结束之后，可以看到发送和接收包的数量，还可以查看丢包率。

如果想长时间进行测试，则可以在命令后加一个参数-t，命令格式为“ping+空格+IP 地址+