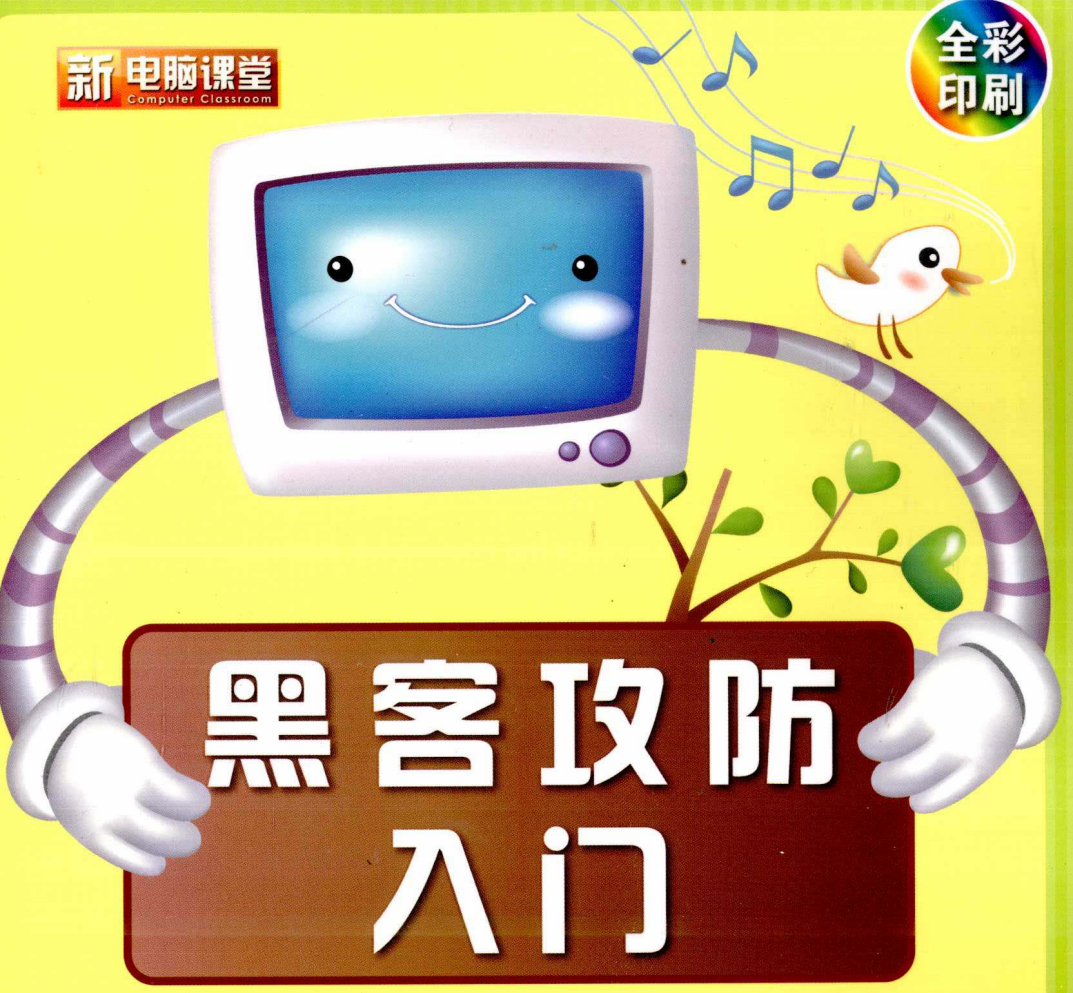
新电脑课堂
Computer Classroom

全彩印刷



黑客攻防入门

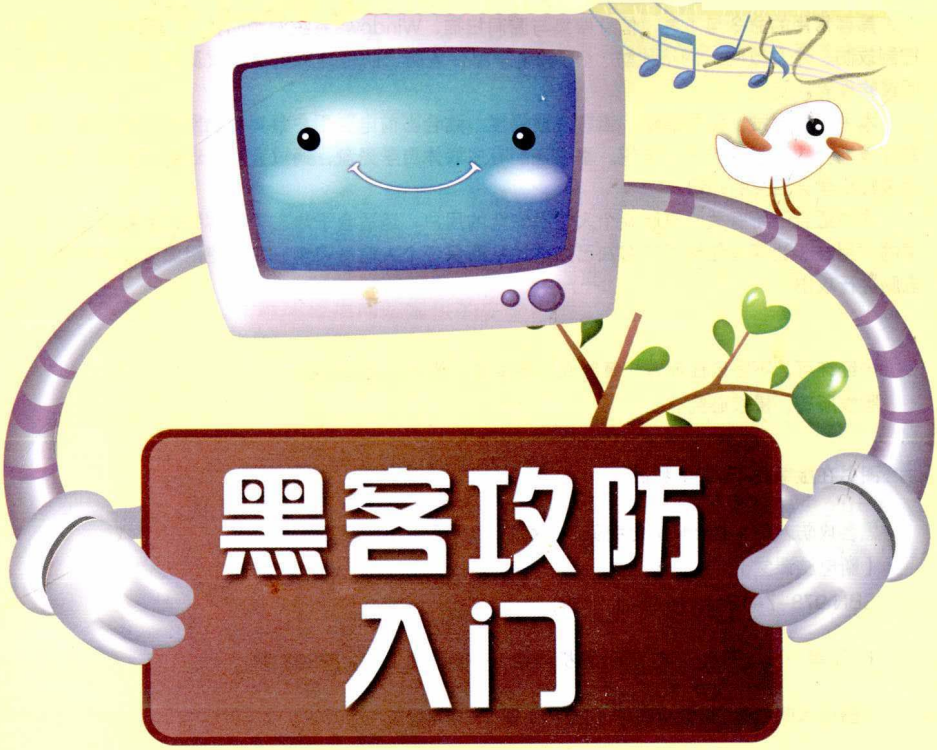
七心轩文化　编著

超值DVD

★包含数小时精彩、生动的多媒体视频教程
★赠送电脑故障排除、电脑应用技巧等电子书，内容超全，使用方便
★赠送其他图书配套多媒体视频教程

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

新电脑课堂
Computer Classroom



黑客攻防入门

七心轩文化 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内容简介

本书主要介绍了黑客常见的入侵手段和一些基本的防范措施，主要内容包括：黑客基础知识、黑客常用的命令与工具、信息搜集与漏洞扫描、Windows系统漏洞防范、密码攻防、远程控制攻防、木马攻防、网络攻防、QQ和电子邮件攻防、防范计算机病毒以及防范流氓软件与间谍软件等。

本书内容丰富、结构清晰、语言浅显易懂，结合当前电脑用户最关心的网络安全问题，图文并茂地介绍了黑客攻防的措施。本书还配有多媒体自学光盘，通过直观生动的视频演示帮助读者轻松学会相关的知识。

本书适合于所有关心电脑及个人信息安全的用户，还适合于热衷于黑客知识的初学者。本书的作用在于让读者能够对黑客知己知彼，从而保证个人信息安全，切勿使用黑客技术对他人电脑进行攻击。

图书在版编目（CIP）数据

黑客攻防入门 / 七心轩文化编著. —北京：电子工业出版社, 2010.9
（新电脑课堂）
ISBN 978-7-121-11472-4

Ⅰ. ①黑… Ⅱ. ①七… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2010）第146008号

责任编辑：牛　勇
文字编辑：张丹阳
印　　刷：中国电影出版社印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：900×1280　1/32　　印张：7.625　　字数：342千字
印　　次：2010年9月第1次印刷
定　　价：28.00元（含DVD光盘1张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

这，是一个星光闪耀的**传奇**：

- 诞生于2002年1月，是计算机图书市场上最“长寿”丛书之一，目前共有十多个子系列、近200个图书品种，正版图书累计销量超过250万册。
- 多次刷新国内计算机图书各种销售与排行榜纪录。
- 覆盖电脑学习的各个方面，适用于各类电脑使用者。
- 曾获“全国优秀畅销书”等顶级荣誉。
- 被无数电脑爱好者与初学者交口称赞与追捧。
- 国内率先推出“网上和电话答疑”等贴心服务，首创多种课程结构和学习方法，图解式教学方法的先驱……太多的“第一”不及细数。

……

这，就是著名电脑普及类丛书品牌——《新电脑课堂》！值此诞辰八周年之际，新版《新电脑课堂》图书重装上阵，奉献给广大电脑爱好者最优的内容品质、最佳的学习方法和最贴心的服务。

《新电脑课堂》适合您吗?

如果下面的描述有两条或更多符合您的情况，那么，《新电脑课堂》是您的最佳选择。

- 对电脑一无所知，或者在某方面略懂、想学习其他方面的知识。
- 想快速掌握电脑的某方面应用技能，例如打字、上网、办公、组装……
- 在电脑使用的过程中，遇到了难题不知如何解决。
- 想找本书作为参考手册，在以后工作、学习过程中方便地查阅知识或技巧。
- 觉得看书学习太枯燥、不直观，想通过视频课程进行学习。
- 担心看书自学效率不高，希望有老师指点迷津。

是否选择《新电脑课堂》?

想看书学电脑，图书怎么选?

- 一看图书难易程度和包含的知识是否适合个人需求。
- 二看图书的学习结构是否符合个人的情况或特点。
- 三看书中的案例是否实用、精彩，最好能直接借鉴、使用。
- 四看配套光盘是否配有多媒体视频教程，以及教程演示是否直观、生动、易于领会。
- 五看图书的售后服务是否全面。学习过程中难免会遇到问题，有名师指点事半功倍。

《新电脑课堂》丛书的特点：

- **专为电脑初学者量身打造：**知识点的选取完全依据电脑初学者的主流需求和接受能力。
- **学习结构科学合理：**以丰富的教学和出版经验为底蕴，学习结构切合初学者的特点和习惯。部分图书提供了众多灵活的学习计划和学习指引，引导读者根据不同的需求进行学习。一本书支持多种学习方法，总有适合您的。
- **精选实用案例，理论联系实际：**以实用为宗旨，知识点融入应用案例中讲解，轻轻松松理解重点和难点。
- **附带精彩、超值的大容量多媒体自学光盘：**配套DVD光盘包含数小时的精彩多媒体视频教程，提供图书配套素材文件，还附赠其他图书的配套多媒体视频教程。
- **贴心服务帮您排忧解难：**通过热线电话或电子邮件，可以轻松与我们进行交流，解决您在学习过程中遇到的难题。

了解了《新电脑课堂》丛书的特点，相信正在为如何选书而发愁的您，心里已经有了明确的选择。

答疑服务

如果读者在学习本书的过程中遇到了疑难问题，或者有其他建议与意见，可以通过以下方式与我们联系。我们会尽力为您排忧解难。

- 热线电话：400-650-6806（无长途话费，工作日9:00~11:30，13:00~17:00）。
- 电子邮件：jsj@phei.com.cn。

丛书作者

本套丛书的作者和编委会成员均是多年从事电脑应用教学和科研的专家或学者，有着丰富的教学经验和实践经验，这些作品都是他们多年科研成果和教学经验的结晶。参与本书编写工作的有谢斌、张月萍、刘霞、朱爱平、陈颖、黄波、唐锐、颜霜霜、罗亮、文湘屏、袁洪川、肖敏、唐波、丁小冬、汤天萍等。由于作者水平有限，书中疏漏和不足之处在所难免，恳请广大读者及专家不吝赐教。

结束语

欢迎进入《新电脑课堂》，您将体验到不一般的学习感受！这个课堂将指引您轻松走入广阔、精彩的电脑世界！

目　录

第10章 防范计算机病毒

第11章 防范流氓软件与间谍软件

Chapter 01

第1章 黑客基础知识

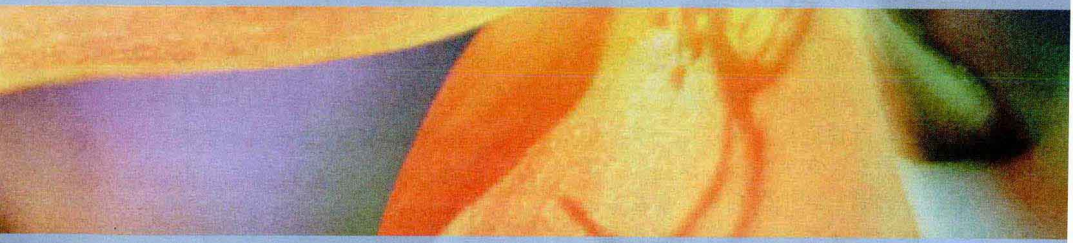
网络就像一把双刃剑，它在给我们带来便利的同时，也让我们的个人财产受到了病毒、木马以及恶意软件等的威胁。随着各种网络攻击的频繁出现，“黑客”这个名字已被广大电脑用户所熟知，然而很多人并不知道黑客的具体含义，以及其攻击的手段等，本节将为读者介绍黑客基础知识，带领大家走进黑客的世界。

本章要点：

★ 认识黑客

★ IP地址与端口

★ 了解系统进程



1.1 认识黑客

知识导读

对于很多电脑用户来说，“黑客”是非常神秘的，总由心底对他们产生一种畏惧。但是如果对黑客有一定的了解，我们就会发现“黑客”其实并没那么可怕，下面就带领大家初步认识黑客。

1.1.1 什么是黑客

“黑客”一词源于英文“Hacker”，原指热衷于电脑技术、水平高超的电脑专家，尤其是程序设计人员。这些人专注研究系统漏洞和程序缺陷，他们不以入侵网络为乐趣，而更多地致力于发现新的漏洞，并提出修补漏洞的方法，这类人被称为“白帽黑客”。

但到了今天，黑客一词已被用于泛指那些为了显示自己的本领和成就，以恶意入侵别人电脑进行破坏和信息窃取为标志的群体，这些人其实应该称为“Cracker”，即“骇客”。

这类人以利用自己掌握的技术入侵网络中的电脑为乐趣，网络上被骇客入侵的电脑被他们称为“肉鸡”。一旦他们入侵了某台电脑，就取得了这台电脑的绝对控制权，可以随意对系统进行破坏并窃取数据等。

1.1.2 黑客常用的攻击手段

黑客攻击手段可分为非破坏性攻击和破坏性攻击两大类。非破坏性攻击一般只是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以入侵他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的的。下面介绍黑客常用的几种攻击手段。

1. 网络嗅探与监听

网络嗅探其实最开始是应用于网络管理的，就像远程控制软件一样。但是，随着黑客技术的进步，这些强大的功能就开始被黑客们所利用。最普遍的安全威胁来自内部，同时这些威胁通常是致命的，破坏性也非常大。很多黑客使用嗅探器进行网络入侵渗透。

提 示

网络嗅探器对信息安全的威胁来自其被动性和被干扰性，使得网络嗅探具有很强的隐蔽性，这也让网络信息的泄密变得不容易被发现。

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用于获取用户口令。

2. 后门程序

由于程序员设计一些功能复杂的

程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用“穷举搜索法”发现并利用这些后门，然后进入系统并发动攻击。

3. IP地址欺骗

IP地址欺骗攻击是黑客们假冒受信主机目标进行的攻击。在这种攻击中，受信主机指的是拥有管理控制权限的主机或明确做出“信任”决定允许其访问自己网络的主机。通常，这种IP地址欺骗攻击局限于把数据或命令注入到客户机/服务器应用之间，或对等网络连接传送中已存在的数据流。为了达到双向通信，攻击者必须改变指向被欺骗IP地址的所有路由表。

4. 信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。比如向没有安装补丁的Windows系统发送特定组合的UDP数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机；向某人的电子邮件发送大量的垃圾邮件将此邮箱“撑爆”等。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。

5. 拒绝服务

“拒绝服务”又叫分布式DOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统的可用系统、带宽资源，最后导致网络服务瘫痪的一种攻击手段。攻击者通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制进程，攻击者把攻击对象的IP地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。比如1999年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

6. 应用基层攻击

应用基层攻击能够使用多种不同的方法来实现，最平常的方法是使用服务器上可找到的应用软件（例如SQL Server、Sendmail和FTP等）的缺陷，通过使用这些缺陷，攻击者能够获得电脑的访问权，以及在该电脑上运行相应程序所需的账户许可权等。

1.2 IP地址与端口

知识导读

IP地址和端口是电脑中不可或缺的两个部分。IP地址是一台连接到互联网中的电脑的标识，通过它可以轻松地找到目标主机；端口是为电脑提供服务的大门，黑客通常会通过开启某些端口来提高权限。本节将为读者介绍IP地址和端口的基础知识。

1.2.1 IP和IP地址

IP是英文Internet Protocol（网络之间互连的协议）的缩写，中文简称为“网协”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。

IP地址是按照网协给每个连接在Internet上的主机分配的一个32bit的标识符。（IPv4是32bit，IPv6是128bit。本书在后面提到的IP地址除非特别声明，否则均指IPv4。）按照TCP/IP协议规定，IP地址用二进制来表示，每个IP地址长32bit，比特换算成字节，就是4个字节。例如一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址，人们处理起来也太费劲了。为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节。于是，上面的IP地址可以表示为“10.0.0.1”。IP地址的这种表示法叫做“点分十进制表示法”，这显然比1和0容易记忆得多。

提 示

TCP/IP（Transmission Control Protocol/Internet Protocol的简写），中文译名为传输控制协议/因特网互联协议，又叫网络通信协议，这个协议是Internet最基本的协议，是Internet国际互联网络的基础，简单地说，就是由网络层的IP协议和传输层的TCP协议组成的。

1.2.2 端口的分类

计算机“端口”是英文port的义译，可以认为是计算机与外界通讯交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。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（基本输入/输出）缓冲区，这类端口也是黑客们入侵电脑的途径之一。

注 意

硬件领域的端口不会被黑客利用，进而攻击电脑，所以本书后面提到的“端口”均指软件领域的端口。

在一台电脑中最多有65535个端口，我们可以按照端口号将它们划分为以下三类。

- 公认端口（Well Known Ports）：从0到1023，它们紧密绑定（binding）于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如，80端口实际上总是HTTP通讯。
- 注册端口（Registered Ports）：从1024到49151。它们松散地绑定于一些服务。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（Dynamic and/or Private Ports）**：从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外，SUN的RPC端口从32768开始。

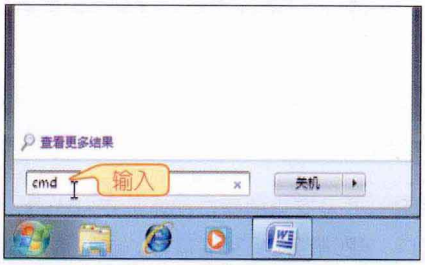
1.2.3 查看端口

很多电脑用户对电脑中开启的端口并不了解，这也使得这部分用户在需要关闭危险端口时显得非常迷茫，这时就需要想办法查看电脑中的端口。通常情况下可以使用Netsat命令和端口查看器来查看电脑中的端口。

1. 使用Netsat命令

在Windows操作系统中，我们可以使用Netstat命令来查看电脑中端口的状态，具体操作方法如下。

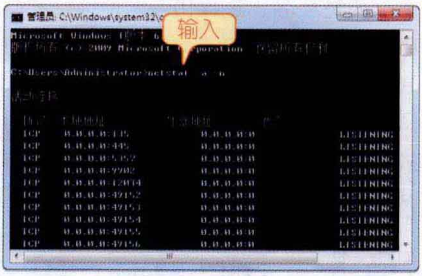
01 单击系统桌面左下角的“开始”按钮，在弹出的“开始”菜单的搜索栏中输入“cmd”命令，然后按下“Enter”键。



提示

在Windows XP系统中可在“开始”菜单中单击“运行”命令，然后在弹出的“运行”对话框中进行上述操作。

02 在弹出的命令提示符窗口中输入“netstat -a -n”命令，按下“Enter”键，然后在接着出现的界面中即可查看当前电脑中端口的状态。



提示

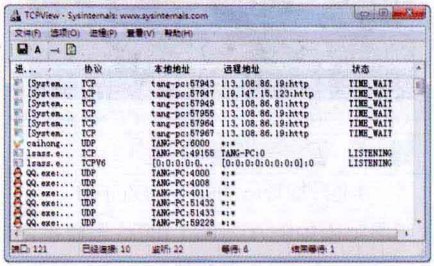
本地IP地址后的就是开放的端口号，如果电脑中的7626端口的状态显示为LISTENING（正在监听等待连接）状态，那么电脑极有可能是感染了冰河病毒，应马上断开网络，进行杀毒。

技巧

“Netstat”命令的用法：其后加“-a”表示显示所有活动的TCP连接，以及计算机监听的TCP和UDP端口；加“-e”表示以以太网发送和接收的字节数、数字包数等；加“-n”表示只以数字形式显示所有活动的TCP连接的地址和端口号；加“-o”标识显示活动的TCP连接并包括每个连接的进程ID；加“-s”表示按协议显示各种连接的统计信息，包括端口号。

2. 使用端口查看器

除了使用Netstat命令可以查看端口以外，还可以使用TCPView软件来进行查看，用户可在网上搜索下载该软件，然后启动软件程序。在打开的主界面的网络连接显示框中，会显示所有进程的网络连接，包括病毒建立的由内到外的TCP连接，并且这些连接信息会实时进行动态变化，显示出详细的TCP连接参数信息。如进程名、进程ID、本地地址和端口号、远程地址和端口号等信息。通过TCPView程序，我们可以很轻松地分析出每个TCP连接的情况。



在使用TCPView软件查看端口信息时，如果发现程序窗口中有熟悉的进程名，并且这个进程名的TCP连接数量非常多，变化频率也很快，这就说明这些TCP连接很可能是病毒建立的恶意的由内到外的TCP连接。为了防止病毒的蔓延和传播，应记录下病毒进程使用的本地端口号，然后右键单击不明进程，在弹出的菜单中单击“结束进程”命令，结束病毒由内到外的TCP连接，然后关闭前面记录下的端口（具体关闭方法将在后面的讲解中具体介绍）即可。

1.2.4 关闭端口和限制端口

默认情况下，电脑系统中很多不安全的和一些没有用的端口都处于开启状态，例如Telnet服务的23端口、FTP服务的21端口、RPC服务的135端口等。这些端口很容易被黑客利用，进而入侵个人电脑系统。因此为保证电脑安全，应将系统中危险的、没有用的端口关闭或加以限制。

1. 关闭端口

电脑中的各项服务通常都对应相应的端口，例如我们熟悉的WWW的服务对应的是80号端口，SMTP服务对应的是25端口等，因此关闭相应的服务也就关闭了与其对应的端口。下面以关闭360杀毒全盘扫描辅助服务对应的57575端口为例，介绍关闭端口的方法，具体操作步骤如下。

01 在系统桌面左下角单击“开始”按钮，在弹出的“开始”菜单中单击“控制面板”命令。