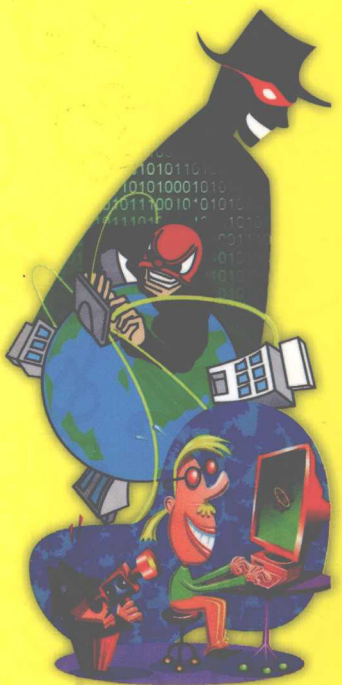
视频教学 一看就会 无师自通 得心应手

第二版

黑客攻防入门

华诚科技 编著



新手易学

版式新颖 内容丰富
全程图解 一学就会
知识技巧 一应俱全
书盘结合 互动教学
视频讲解 生动有趣

超值赠送

超值赠送本书全程视频讲解

机械工业出版社
China Machine Press

视频教学 一看就会 无师自通 得心应手

易对象 第三版

黑客攻防入门

华诚科技 编著

新手易学

机械工业出版社
China Machine Press

本书是指导初学者学习黑客攻防的入门书籍，书中详细地介绍了黑客通常会使用的入侵手段和工具，将黑客入侵的整个过程展现在读者面前，同时也讲解了防御这些攻击时必须掌握的基础知识、使用方法和操作步骤，以免读者在起步的过程中走弯路。

全书共分为13章，首先介绍了黑客攻防的基本知识，包括黑客、网络攻击基础、IP和端口等概念；然后介绍了嗅探工具和扫描工具的使用，常见木马的植入、清除和防范，远程控制技术，QQ远程协助、网络执法官、远程控制任我行等远程监视工具，ARP欺骗、入侵隐藏技术、黑客常用的追踪工具等知识；接着介绍了常见的漏洞入侵实例和注入工具，网页恶意代码，网页攻击的实现与防范，邮件炸弹实战，破解电子邮箱密码的手段，常用的QQ盗号工具、QQ信息攻击工具以及QQ的安全防范，局域网监听、局域网挂马、局域网攻击与防范等知识；最后介绍了系统流氓软件和间谍软件的清理，更改组策略和注册表编辑器，以及防火墙技术、文件加密技术、数据恢复技术等知识。

本书内容详尽、讲解清晰，力求使读者通过本书的学习，快速掌握黑客攻防的相关知识。本书适合对黑客感兴趣的新手，也可作为了解黑客攻防的参考书，是一本实用性较强的黑客攻防类书籍。

图书在版编目（CIP）数据

新手易学：黑客攻防入门 / 华诚科技编著. —北京：机械工业出版社，2011.1

ISBN 978-7-111-32464-5

Ⅰ. 新…　Ⅱ. 华…　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（2010）第220134号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：李　荣
北京京师印务有限公司印刷
2011年1月第1版第1次印刷
185mm×260mm • 15印张
标准书号：ISBN 978-7-111-32464-5
　　ISBN 978-7-89451-763-0（光盘）
定价：35.00元（附光盘）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：(010)88378991；88361066
购书热线：(010)68326294；88379649；68995259
投稿热线：(010)88379604
读者信箱：hzjsj@hzbook.com

前　言

互联网发展的同时也造就了一批网络高技术的不法分子，即大家通常所说的黑客，他们经常利用自己高超的电脑技术一次又一次地入侵他人电脑，窃取隐私信息和重要数据。因此，广大电脑爱好者必须了解黑客常用的入侵方式及对应的防范措施。

本书从“攻”、“防”两个不同的角度，在介绍黑客攻击手段的同时，也讲解了相应的防范措施；通过介绍黑客常用的入侵工具和浅显易懂的操作步骤向用户展现了黑客入侵网络与防御的全过程。

全书共分为13章，第1章介绍了黑客攻防的基础知识，包括黑客、网络攻击基础、IP地址和端口等概念，同时也介绍了黑客攻防的相关术语和常用的命令；第2章介绍了搭建虚拟环境、使用嗅探工具监听网络、扫描网络中主机的开放端口等知识；第3章介绍了常见木马的植入、清除和防范；第4章介绍了远程控制技术，例如常用的QQ远程协助，还有网络执法官、远程控制任我行等远程监视工具等知识；第5章介绍了网络攻击与欺骗技术，包括ARP欺骗、DNS欺骗和DDoS欺骗等知识；第6章介绍了黑客的隐匿与追踪技术，包括入侵隐藏技术、黑客常用的追踪工具等知识；第7章介绍了漏洞攻防实战，包括漏洞攻击基础、常见的漏洞入侵实例、常用的注入工具等知识；第8章介绍了网页攻防实战，包括网页恶意代码、网页攻击的实现与防范等知识；第9章介绍了邮件攻防实战，包括邮件炸弹实战、破解电子邮箱密码的手段等知识；第10章介绍了QQ攻防实战，包括常用的QQ盗号工具、QQ信息攻击工具以及QQ的安全防范等知识；第11章介绍了局域网攻防实战，包括局域网监听、局域网挂马、局域网攻击与防范等知识；第12章介绍了系统清理与安全性能提升，包括流氓软件、间谍软件的清理，更改组策略和注册表编辑器等知识；第13章介绍了系统安全防御技术，包括防火墙技术、文件加密技术、数据恢复技术等知识。

本书以场景式教学、案例驱动与任务进阶为写作特色，在书中可以看到一个个生动的场景案例。通过一个个任务的实践操作，读者不仅可以轻松掌握有关网络安全的知识，还可在不知不觉中快速提升网络安全防范的实战技能。

本书涉及面较广，可作为一本黑客攻防技术的速查手册，也适合网络管理人员、喜欢研究黑客技术者、大中专院校相关专业的学生使用。

随书附赠的光盘为用户提供了多种攻防实战的教学视频，通过增加读者对主流操作手法感性的认识，使读者提高防范技能，确保自己电脑的系统安全。

由于笔者水平有限，在本书的编辑过程中难免会存在一些疏漏之处，希望广大读者发现后批评指正，并提出宝贵的意见。

最后需要提醒读者的是：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，后果自负。

编 者

2010年10月

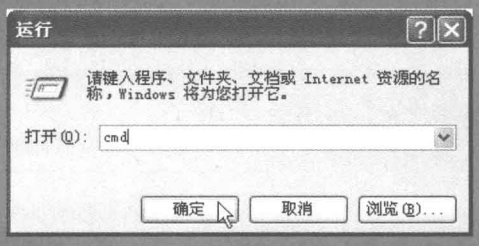
目　录

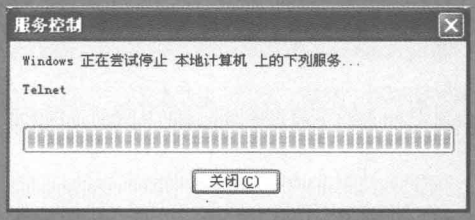
第 1 章

黑客攻防基础知识

要点导航

- 认识黑客
- 认识常见的网络协议
- IP地址与端口
- 认识系统进程
- 黑客常用的DOS命令





黑客往往会被认为是神秘的、不可捉摸的、难以接近的一类人，他们利用自己熟练的技术使得互联网的安全频频告急，有时候还会使得人们随时在担心自己的系统是否被黑客成功入侵了。其实黑客也有高手和菜鸟之分，只要用户了解了黑客的基本手段，一般的黑客是无法入侵您的电脑的。而对于黑客高手来说，可能您的电脑没有让他入侵的价值，所以不用太担心。

本章将主要介绍什么是黑客，常见的网络协议有哪些，认识IP地址、端口和系统进程以及黑客常用的DOS命令等知识，最后还向用户介绍一些黑客常用的专业术语。

1.1 认识黑客

关键字
黑客、骇客、入侵

视频学习 无

难度水平
◆◇◇◇◇

“黑客”是英文hacker直接音译过来的，简单地说，可将黑客理解为破坏者，黑客一般都是利用系统或者软件的漏洞来入侵用户电脑，当用户使用了一些较为危险的操作时就会给黑客创造机会。说直接一点，黑客最拿手的就是乘人之危。

黑客一词，原意是指计算机技术水平高超的电脑专家，尤其是指程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的家伙，而对这些人正确的英文叫法是cracker，音译为“骇客”。黑客与骇客的主要区别是黑客们修补相关漏洞，而骇客们却抓住这些漏洞对其他电脑进行入侵。

在网络发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以为所欲为。目前各国法律的发展速度仍落后于互联网的发展速度，在黑客活动转入地下以后，其攻击的隐蔽性更强，使得当前法律和技术缺乏针对网络犯罪卓有成效的法纪和跟踪手段，无规范的黑客活动已经成为网络安全的重要威胁。

提示：红客

“红客”一词源于黑客，它是指维护国家利益，不利用网络技术入侵自己国家的电脑，而是维护正义，为自己国家争光的黑客。在中国，红色有着特定的价值含义，代表正义、道德、进步、强大等。红客是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神并热爱着计算机技术的人都可称为红客。红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击。

1.2 网络攻击基础——认识网络协议

关键字
TCP/IP、ARP、ICMP

视频学习 无

难度水平
◆◇◇◇◇

网络协议是指为在计算机网络中进行数据交换而建立的规则、标准或约定的集合。常见的网络协议有TCP/IP协议族、ARP协议、ICMP协议和SMTP协议，除此之外，还有UDP协议、IPX/SPX协议等。

1.2.1 网络连接标准接口——TCP/IP协议

TCP/IP协议，全称是Transmission Control Protocol/Internet Protocol，中文译为传输控制协议/因特网互联协议，又叫网络通信协议。众所周知，如今计算机接入互联网后都要设置TCP/IP，因此TCP/IP协议是互联网最基本的协议，也是国际互联网络的基础。

TCP/IP 定义了计算机如何连入因特网，以及数据如何在其中传输的标准。

TCP/IP包含两层协议，即TCP协议和IP协议。其中高层的TCP协议负责收集信息或者把

文件拆分成更小的数据包。发送端将这些数据包通过网络传送到接收端的TCP层，接收端的TCP层把数据包还原为原始文件；而低层的IP协议则处理每个数据包的地址部分，使得网络上的网关计算机能够识别数据包的地址并进行路由选择，从而让这些数据包能够正确到达目的地。

1.2.2 ARP欺骗攻击必知——ARP协议

ARP，即地址解析协议，它能够通过已知的IP地址来获取与其对应的物理地址（MAC地址）。在TCP/IP网络环境下，每个主机都分配了一个32bit（比特）的IP地址（如220.248.138.166），它是在网络中标识主机的一种逻辑地址，如果想要成功地将报文（网络中主机之间交换与传输的数据单元）传送给目的主机，则必须知道目的主机的物理地址，此时就可以使用ARP协议将目的主机的IP地址转换为物理地址。

简单地说，ARP协议就是主机在发送报文之前将目标主机的IP地址转换成与之对应的MAC地址的过程。谈到ARP就离不开ARP欺骗，本书将在第5章向读者具体介绍ARP欺骗的工作原理及防范方法。

1.2.3 洪水攻击必知——ICMP协议

ICMP，即Internet控制报文协议，它是TCP/IP协议族中的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息包括网络通不通、主机是否存在、路由是否可用等网络本身的消息，这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着非常重要的作用。

ICMP在网络中提供了一致、易懂的出错报告信息，将发送的出错报文返回到发送数据的主机。ICMP唯一的功能是报告问题而不是解决问题，解决问题的任务由发送方完成。

正是这一特点使得它非常容易被用于攻击网络上的路由器和主机。例如“Ping Of Death”攻击，在还没有发布限制发送ICMP数据包大小的补丁之前，操作系统规定了ICMP数据包的最大尺寸不超过64KB，因此“Ping Of Death”根据这一规定向主机发起攻击。其工作原理是：如果ICMP数据包的尺寸超过64KB上限时，主机出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。

提示：洪水攻击

洪水攻击是现在黑客比较常用的一种攻击技术，特点是实施简单，威力强大，无论电脑的防护防御措施做得多么好，都很难保证不遭受该类攻击。常见的洪水攻击包含MAC泛洪、网络泛洪和应用程序泛洪。

MAC泛洪是指攻击者进入局域网内，将假冒的源MAC地址和目的MAC地址数据帧发送到以太网上，使得假冒的源MAC地址和目标MAC地址塞满交换机的MAC地址表，导致交换机无法正确地传送数据。

网络泛洪包括Smurf和DDoS。其中Smurf是指攻击者假冒ICMP广播ping，如果路由器没有关闭定向广播，那攻击者就可以在某个网络内对其他网络发送定向广播ping，网络中的主机越多，造成的结果就越严重，因为每个主机都会默认响应这个ping，导致链路流量过大而拒绝服务。而DDoS是指攻击者将DDoS控制软件安装到连接到互联网的系统中，并使其感染其他系统，然后攻击者将攻击指令发送给DDoS控制软件，让受DDoS控制

的系统向某个IP发送大量假冒的网络流量，受攻击者的网络将被这些假的流量所占据，导致无法为它们的正常用户提供服务。

应用程序泛洪的目的就是消耗应用程序或者系统资源，常见的形式就是垃圾邮件。

1.2.4 邮件攻击必知——SMTP协议

SMTP，即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地，通过SMTP协议所指定的服务器就可以把电子邮件寄到收信人的服务器上了，整个过程只需要几分钟。

由于SMTP协议是与邮件传输有关的协议，因此提到SMTP就不得不让人想起邮件攻击，本书将在第9章具体介绍邮件攻击与防范的相关内容。

1.3 黑客必经的两道门——IP地址与端口

关键字
IP地址、端口

视频学习 光盘\第1章 黑客攻防基础知识\1-3 黑客必经的两道门——IP地址与端口

难度水平
◆◆◇◇◇

黑客攻击其他人的电脑必须确定目标主机的IP地址和扫描目标主机的开放端口。因此目标主机的IP地址和开放端口对于黑客来说是非常重要的信息，也是黑客入侵目标主机的必备信息。

1.3.1 IP地址与端口概述

端口是计算机与外界通信交流的端口，而IP地址则是网络中主机的重要标识之一，因此用户如果想要了解黑客是怎样获取IP地址和扫描开放端口的，则必须首先知道什么是IP地址和端口。

1. IP地址

IP地址就是给每个连接在互联网上的主机分配的一个32bit（比特）地址。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“11000000101010000000000100000001”，这么长的IP地址处理起来会很费劲，因此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，所以上面的IP地址可以写成192.168.1.1。IP地址的这种记法叫做“点分十进制表示法”，这显然比一长串的1和0要好记得多。

互联网中的每个接口都必须有一个唯一的IP地址，该地址并不是采用平面形式的地址空间，它具有一定的结构，一般情况下IP地址可分为A、B、C、D、E 5大类。

A类IP地址由1个字节的网络地址和3个字节主机地址组成，网络地址的最高位必须是“0”，其地址范围为1.0.0.1～126.255.255.254。可用的A类网络有126个，每个网络能够容纳16 777 214个主机。

B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高位必须是

“10”，其地址范围为128.0.0.1～191.255.255.254。可用的B类网络有16 384个，每个网络能够容纳65 534个主机。

C类IP地址由3个字节的网络地址和1个字节的主机地址组成，网络地址的最高位必须是“110”，其地址范围为192.0.0.1～223.255.255.254。其中192.168.0.0～192.168.255.255为私有IP地址，C类网络可达2 097 150个，每个网络能容纳254个主机。

D类IP地址用于多点广播，其第一个字节以“1110”开始。它是一个专门保留的地址，不能在互联网上作为接点地址使用。其地址范围为224.0.0.1～239.255.255.254。

E类IP地址用于实验和开发，也不能在互联网上使用。其第一个字节以“1111”开始，为将来使用保留。

除了以上5类IP地址之外，还有两个IP地址，即全“0”地址（0.0.0.0）和全“1”地址（255.255.255.255），其中全“0”地址是指任意网络，全“1”地址是广播地址（现在CISCO上可以使用全0地址）。一般常用的为A、B、C 3类地址。

2. 端口

简单地说，端口就是计算机和外界连接的通道。

为了解释清楚端口，接下来用房子来打个比方，端口就好比房子的门窗，它是信息出入的必经通道。另外，就如不同的门窗有不同的用处一样，不同的端口也有不同的功能，例如使用浏览器浏览网页用的是80号端口。计算机上可开启的端口数值范围为1～65 535。

常用的端口有21号端口（FTP——文件传输协议）、23号端口（Telnet——远程登录协议）、53号端口（DNS——域名服务器）、79号端口（finger——查看机器的运行情况）、80号端口（HTTP——超文本传输协议）、110号端口（POP——邮局协议）、139号端口（NetBIOS服务，即共享服务）、3389号端口（用于远程登录）。

端口按照端口号的分布可分为公认端口、注册端口以及动态和私有端口。

公认端口，也称常用端口。这类端口包括0～1023号端口，它们紧密地绑定一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这类端口不可再重新定义它的作用对象。

注册端口，包括1024～49151号端口，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的目的。这些端口多数没有明确的定义服务对象，不同程序可以根据实际需要自己定义。这些端口会定义一些远程控制软件和木马程序，因此对这些端口的防护和查杀是非常有必要的。

动态和私有端口，包括49152～65535号端口，从理论上讲不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起注意，容易隐藏。

1.3.2 设置IP地址

IP地址是网络中主机的重要标识之一，因此电脑中安装了网卡之后，需要对电脑设置IP地址后才可以连接到网络。设置IP地址的操作方法如下所示。

步骤1：单击“属性”命令

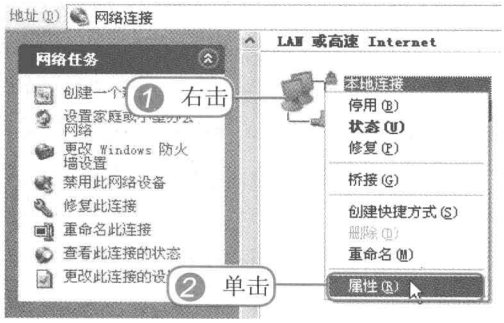
❶ 在桌面上右击“网上邻居”图标。

❷ 弹出快捷菜单，在菜单中单击“属性”命令，打开“网络连接”窗口。

步骤2：单击“属性”命令

❶ 在“网络连接”窗口中右击“本地连接”图标。

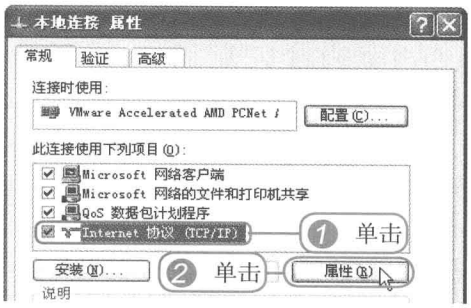
❷ 弹出快捷菜单，在菜单中单击“属性”命令，打开“本地连接 属性”对话框。



步骤3：单击【属性】按钮

❶ 在“此连接使用下列项目”列表框中选中“Internet协议（TCP/IP）”选项。

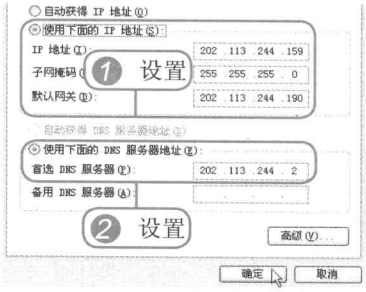
❷ 然后单击【属性】按钮。



步骤4：设置IP地址

❶ 在“Internet协议 属性”对话框中单击选中“使用下面的IP地址”单选按钮，然后在下方设置IP地址、子网掩码和默认网关。

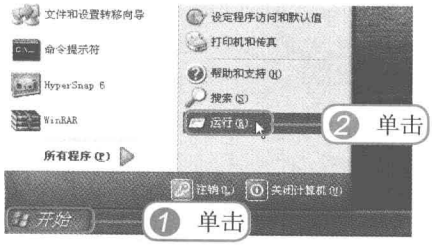
❷ 接着单击选中“使用下面的DNS服务器地址”单选按钮，然后在下方设置首选DNS服务器。



步骤5：单击“运行”命令

❶ 连续单击两次【确定】按钮后返回到桌面，单击左下角的【开始】按钮。

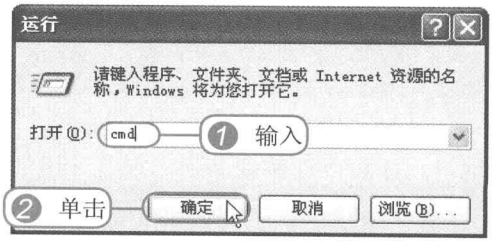
❷ 在弹出的“开始”菜单中单击“运行”命令。



步骤6：输入cmd命令

❶ 弹出“运行”对话框，在“打开”文本框中输入cmd命令。

❷ 输入完毕后单击【确定】按钮或者按下【Enter】键。



步骤7：查看设置的IP地址

在弹出的DOS命令对话框中输入ipconfig命令后按下【Enter】键，接着便可在下方看见当前电脑的IP地址、子网掩码和默认网关。

提示：设置连接了路由器的电脑IP地址

当用户使用路由器实现共享上网时，由于路由器具有自动分配IP地址的功能，因此用户在设置电脑IP地址时只需选择自动获取IP地址和DNS服务器即可。

1.3.3 查看端口

查看目标主机的端口除了使用后面介绍的端口扫描软件（X-Scan、SuperScan）之外，还可以在Windows XP系统中使用netstat命令进行查看。端口扫描软件不仅能够查看本台电脑的端口，还能查看网络中其他电脑的端口，而netstat命令只能查看本台电脑中已开放的端口。

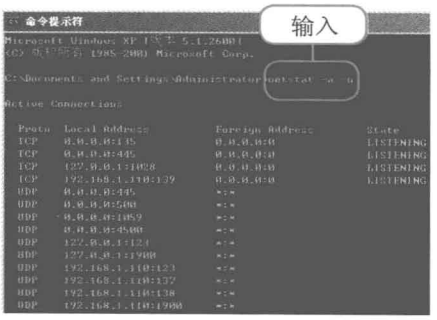
步骤1：单击“命令提示符”命令

❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中依次单击“所有程序>附件>命令提示符”命令。

步骤2：查看端口号

弹出“命令提示符”对话框，输入netstat -a -n后按下【Enter】键，即可看到以数字形式显示的TCP和UDP连接的端口号及状态。



1.3.4 关闭与限制端口

系统在默认的情况下有很多不安全或者是没有用的端口是开启的，因此用户需要对这些端口进行关闭或者限制操作。

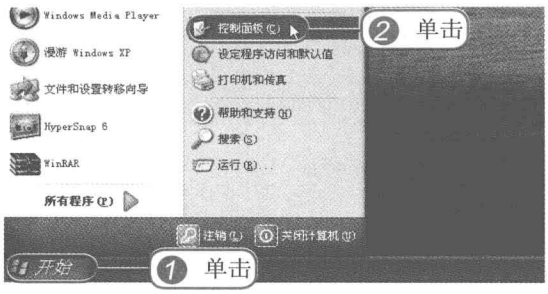
1. 关闭端口

当用户安装了Windows XP操作系统之后，系统中一些不安全的端口在默认情况下是开启的，例如Telnet服务的23号端口、FTP服务的21号端口等，这里以Telnet服务的23号端口为例介绍关闭端口的操作步骤。

步骤1：单击“控制面板”命令

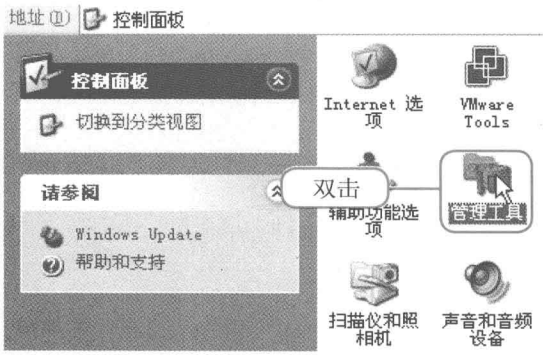
❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中单击“控制面板”命令。



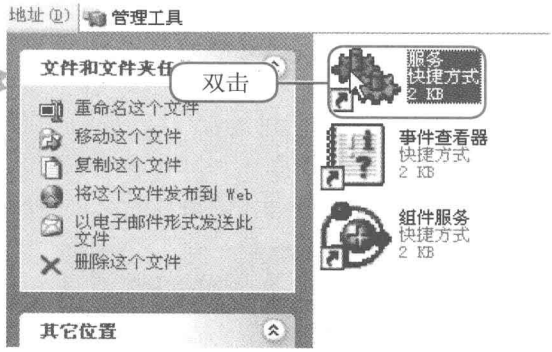
步骤2：双击“管理工具”图标

打开“控制面板”窗口，双击“管理工具”图标。



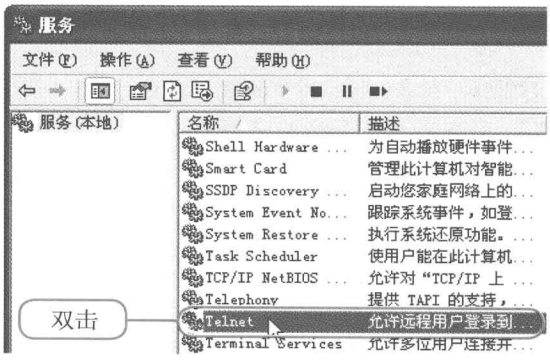
步骤3：双击“服务”图标

打开“管理工具”窗口，双击“服务”图标。



步骤4：双击Telnet选项

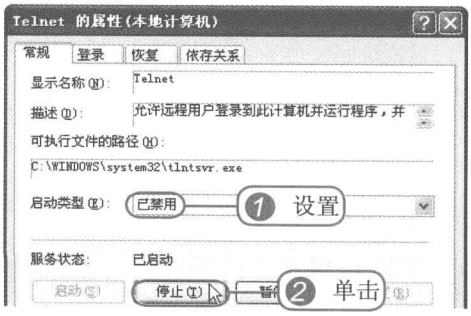
打开“服务”窗口，在窗口的右侧选中Telnet选项，然后双击该选项。



步骤5：设置Telnet属性

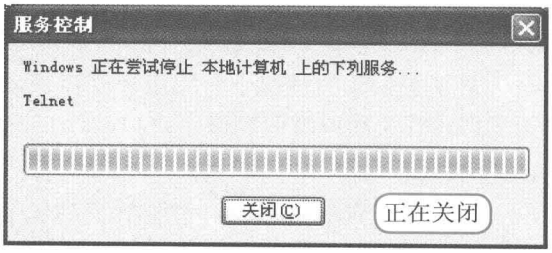
❶ 弹出“Telnet 的属性本地计算机”对话框，设置“启动类型”为“已禁用”。

❷ 接着在“服务状态”选项组中单击【停止】按钮。



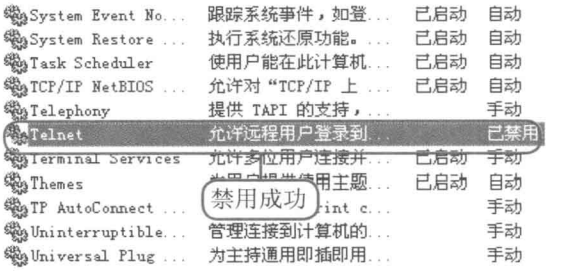
步骤6：正在关闭Telnet服务

弹出“服务控制”对话框，此时Windows正在尝试停止本地计算机上的Telnet服务。



步骤7：禁用成功

在“Telnet 的属性本地计算机”对话框中单击“确定”按钮返回“服务”窗口，此时可看见Telnet服务已经被成功禁用。



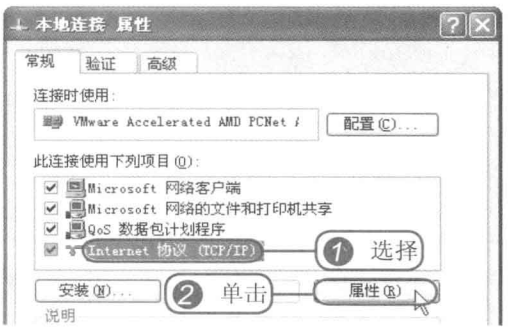
2. 限制端口

在Windows XP操作系统中，除了关闭端口对应的服务之外，还可以使用“TCP/IP筛选”功能限制电脑的某些端口。

步骤1：单击【属性】按钮

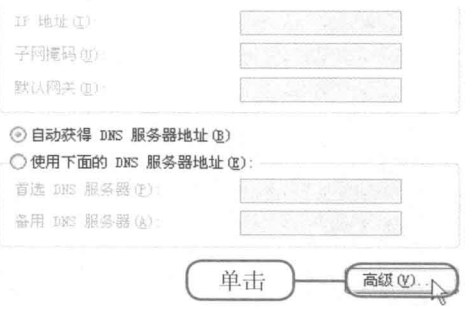
❶ 按照1.3.2小节介绍的方法打开“本地连接属性”对话框，在“此连接使用下列项目”列表框中选中“Internet协议（TCP/IP）”选项。

❷ 然后单击【属性】按钮。



步骤2：单击【高级】按钮

弹出“Internet协议 属性”对话框，在对话框的底部单击【高级】按钮。

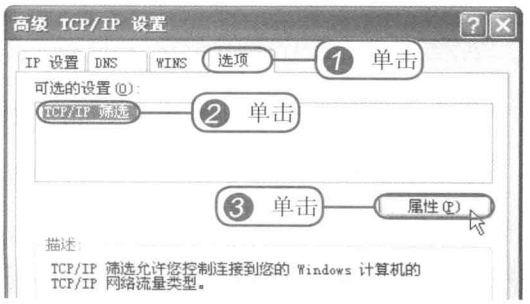


步骤3：选中TCP/IP筛选

❶ 弹出“高级TCP/IP设置”对话框，单击“选项”标签。

❷ 在“可选的设置”选项组中单击选中“TCP/IP筛选”选项。

❸ 然后单击【属性】按钮。



步骤4：添加TCP端口

❶ 弹出“TCP/IP筛选”对话框，勾选“启用TCP/IP筛选（所有适配器）”复选框。

❷ 选择显示的端口型号，例如在“TCP端口”选项组中单击选中“只允许”单选按钮。

❸ 单击【添加】按钮。