丛书部分品种曾获 全行业优秀畅销品种、全国大学出版社优秀畅销书 丛书累计销售 150 万册

一学就会

魔法书

(第 3 版)

像看电影一样学电脑

电脑黑客攻防

九州书源 曾福全 向利 编著

103 节大型同步互动多媒体教学演示

☑ 情景式教学 ☑ 模拟操作练习 ☑ 丰富的实例 ☑ 大量学习技巧等

可快进慢放的、可模拟操作的、同步的全程多媒体演示，手把手教您

提供丰富的实例和学习技巧，让学习轻松快捷

提供素材源文件，方便对照实例练习

赠 116 节拓展学习视频

本书内容相关的各类实用技巧 149 个

清華大學出版社

一学就会

魔法书

（第3版）

电脑黑客攻防

（第2版）

九州书源

曾福全　向　利　编著

清華大學出版社

北京

内 容 简 介

《电脑黑客攻防（第2版）》讲述了成为电脑黑客所需使用的工具和方法的相关知识，主要内容包括走进黑客世界、黑客常用命令和工具、系统漏洞扫描与防范、木马攻击与防范、局域网干扰与防御、密码破解与保护、IE浏览器攻击与防御、QQ与电子邮件攻防、网络远程控制攻防、U盘攻击与防御、常见后门开启与痕迹清除和打造安全电脑环境等知识。通过介绍各种工具的使用技巧让读者的防黑客技能更上一个台阶。

本书深入浅出，以小魔女对黑客攻击一窍不通到熟练掌握黑客攻击和防御的方法为线索贯穿始终，引导初学者学习。本书使用了大量黑客工具和防御软件进行讲解，以帮助读者掌握相关知识。

本书及光盘还有如下特点及资源：情景式教学、互动教学演示、模拟操作练习、丰富的实例、大量学习技巧、素材源文件、电子书阅读、大量拓展资源等。

本书定位于有意学习防黑客技术的初学者，适合在校学生、办公人员、教师以及对黑客知识有兴趣的人员等学习和参考，也可以作为网络操作以及网络管理等职场人员的参考用书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

电脑黑客攻防/九州书源编著. —2版. —北京：清华大学出版社，2013
（一学就会魔法书）

ISBN 978-7-302-31542-1

I. ①电… II. ①九… 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（2013）第030582号

责任编辑：赵洛育
封面设计：刘洪利
版式设计：文森时代
责任校对：张兴旺
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　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 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16　　**字　　数**：370千字
（附光盘1张）
版　　次：2005年8月第1版　2013年10月第2版　　**印　　次**：2013年10月第1次印刷
印　　数：15001～20200
定　　价：39.80元

产品编号：046254-01

再致亲爱的读者

——一学就会魔法书（第3版）序

首先感谢您对“一学就会魔法书”的支持与厚爱！

“一学就会魔法书”（第1版）自2005年8月出版以来，曾在全国各大书店畅销一时，2009年7月“一学就会魔法书”（第2版）出版，备受市场瞩目。截止目前，先后有百余万读者通过这套书学习了电脑相关技能，被全国各地550多家电脑培训机构、机关、社区、企业、学校选作培训教材，累计销售近150万册。其中丛书第1版本5种荣获2006年度“全行业优秀畅销品种”，丛书第2版1种荣获第2届“全国大学出版社优秀畅销书”，丛书第1版、第2版荣获清华大学出版社优秀畅销系列书，连续8年在市场上表现良好。

许多热心读者反映，通过“一学就会魔法书”学会了电脑操作，为自己的工作与生活带来了乐趣。有的读者希望增加一些新的品种；有的读者反映一些知识落后了，希望能出新的版本。为了满足广大读者的需求，我们对“一学就会魔法书”（第2版）进行了大幅度更新，包括内容、版式、封面和光盘运行环境的更新与优化，同时还增加了很多新的、流行的品种，使内容更加贴近读者，与时俱进。

“一学就会魔法书”（第3版）继承了第2版的优点：“轻松活泼”“起点低，入门快，实例多”和“情景式学习”等，光盘则“可快慢调节、可模拟操作练习、包含素材源文件”，还有大量学习技巧和拓展视频等。

一、丛书内容特点

本丛书内容有以下特点：

（一）情景式教学，让电脑学习轻松愉快

本丛书为读者设置了一个轻松、活泼的学习情境，书中以“小魔女”的学习历程为线索，循着她学习的脚步，解决日常电脑应用的常见知识，同时还有“魔法师”深入浅出讲解各个知识点，并及时提出常见问题、学习技巧、学习建议等。情景式学习，寓教于乐，让学习轻松、充满乐趣。

（二）动态教学，操作流程一目了然

为了让读者更为直观地看到操作的动态过程，本丛书在讲解时尽量采用图示方式，并用醒目的序号标示操作顺序，且在关键处用简单的文字描述，在有联系的图与图之间用箭头连接起来，将电脑上的操作过程动态地体现在纸上，让读者在看书的同时感觉就像在电脑上操作一样直观。

（三）解疑释惑让学习畅通无阻，动手练习让学习由被动变主动

“魔力测试”让您可以随时动手，“常见问题解答”帮您清除学习路上的“拦路虎”，“过关练习”让您能强化操作技能，这些都是为了让读者主动学习而精心设计的。

本丛书中穿插的“小魔女”的各种疑问就是读者常见的问题，而“魔法师”的回答则让读者豁然开朗。这种一问一答的互动模式让学习畅通无阻。

二、光盘内容及其特点

本丛书的光盘是一套专业级交互式多媒体光盘，采用全程语音讲解、情景式教学、详细的图文对照方式，通过全方位的结合引导读者由浅至深，一步一步地完成各个知识点的学习。

（一）同步、互动多媒体教学演示，手把手教您

多媒体演示中，提出各式各样的问题，引出了各个知识点的学习任务；安排了一个知识渊博的“魔法师”耐心、详细地解答问题；另外还安排了一个调皮的“小精灵”，总是在不经意间让您了解一些学习的窍门。

（二）多媒体模拟操作练习，边看边练

通过“新手练习”按钮，用户可以边学边练；通过“交互”按钮，用户可以进行模拟操作，巩固学到的知识。

（三）素材、源文件等学习辅助资料

模仿是最快的学习方式，为了便于读者直接模仿书中内容进行操作，本书光盘提供所有实例的素材和源文件，读者可直接调用，非常方便。

（四）常见问题与学习技巧

光盘中给出了百余个与本书内容相关的各类实用技巧和常见问题，帮读者扫清学习障碍，提高学习效率。

（五）深入拓展学习资源

为了便于读者后续深入学习，开拓视野，本光盘赠送了较为深入的“视频教程”。

（六）电子阅读

为了方便读者在电脑上学习，光盘中配备了电子书，读者可直接在电脑或者部分手机上学习。

九州书源

前 言

黑客攻击一直是互联网中的热门话题，使用黑客工具收集电脑信息，应用黑客软件窃取密码，使用安全防御软件保护电脑已经成为众多职场人员以及网络安全技术人员必不可少的技能。本书根据不同人群的需要，以浅显易懂的讲解方式，介绍黑客攻防中最基本以及最需要掌握的内容，包括黑客攻击电脑的方式、常用的黑客攻击软件和命令、防御黑客攻击的方法以及怎样使电脑安全地运行等知识。配合各章的“本章小结”和“过关练习”，让读者可以在最短时间内以最快捷的方式掌握最实用的知识。

本书内容

本书从黑客初学者的角度出发，以循序渐进的方式将内容分为以下4个部分进行讲解。

章　节	内　容	目　的
第1部分（第1~2章）	走进黑客世界、黑客常用命令和工具	了解黑客的含义以及黑客想要收集的信息，掌握黑客常用的入侵命令
第2部分（第3~10章）	系统漏洞扫描与防范、木马攻击与防范、局域网干扰与防御、密码破解与保护、IE浏览器攻击与防御、QQ与电子邮件攻防、网络远程控制攻防、U盘攻击与防御	了解黑客常见的攻击对象和方法，掌握常见黑客工具的使用，了解针对不同黑客工具的防御知识
第3部分（第11章）	常见后门开启与痕迹清除	了解实施黑客攻击后，后门的开启以及攻击痕迹的清理方法
第4部分（第12章）	打造安全电脑环境等	了解如何使用软件、系统自带的安全防火墙以及工具对电脑的运行环境进行保护

本书适合的读者对象

本书适合以下读者：

（1）希望防范黑客攻击，使电脑安全运行的人员。

（2）希望掌握简单的黑客知识以及对黑客攻击有兴趣的电脑爱好者及学生。

（3）在公司进行网络维护以及网络管理的职场人员。

如何阅读本书

本书每章按“内容导读+学习要点+本章内容+本章小结+过关练习”的结构进行讲述。

■ 内容导读：通过“小魔女”和“魔法师”的对话引出本章内容，活泼生动的语言读来趣味盎然，同时了解学习本章的原因和重要性。

学习要点：以简练的语言列出本章要点，使读者对本章将要讲解的内容一目了然。

本章内容：将实例贯穿于知识点中讲解，将知识点和实例融为一体，以图示方式进行讲解，并通过典型实例强化与巩固知识点。

本章小结：由“小魔女”提出在学习和应用本章相关知识时遇到的疑难问题，“魔法师”给出具体回答，并传授几招给“小魔女”，既能帮读者解惑还能扩展所学的知识。

过关练习：列举一些上机操作题，以提高读者的实际动手能力。

另外，了解以下几点更有利于学习本书。

（1）本书设计了调皮好学的“小魔女”和知识渊博的“魔法师”两个人物，分别扮演学生和老师的角色，这两个人物将一直引导读者进行学习，在多媒体光盘中更是可以随着小魔女的学习步伐，掌握所需的知识。

（2）本书在讲解知识点时尽量采用图示方式，用1、2、3表示操作顺序，并在关键步骤用简单的文字描述，将有联系的图用箭头连接起来，体现操作的动态变化过程。

（3）本书将丰富生动的实例贯穿于知识点中，读者学完一个实例就学会了一种技能，能解决一个实际问题，读者在学习时可以有意识地用它来完成某个任务，帮助理解知识点。

（4）本书中穿插了“小魔女”和“魔法师”的提示语言以及“魔法档案”和“晋级秘诀”两个小栏目，这些讲解将帮助读者进一步了解知识的应用方法和技巧。

（5）过关练习是巩固所学知识点和提高动手能力的关键，必须综合运用前面所学的知识点才可能做出来。建议读者一定要正确做完所有题目后再进入下一章的学习。

（6）本书配有多媒体互动式教学光盘，读者可以在模拟环境下边学边练，达到事半功倍的效果。若读者想获取相关的软件，则需要自行购买正版软件或在网站上下载试用版使用。

本书的创作团队

本书由九州书源组织编写，由曾福全、向利主笔，其他参与本书编写、资料整理、多媒体开发及程序调试的人员有向萍、丛威、简超、宋玉霞、张娟、羊清忠、贺丽娟、宋晓均、刘凡馨、常开忠、付琦、杨明宇、陈晓颖、陆小平、张良军、徐云江、廖宵、杨颖、李伟、赵云、赵华君、张永雄、余洪、唐青、范晶晶、牟俊、陈良、张笑、穆仁龙、黄沄、刘斌、骆源、夏帮贵、王君、朱非、杨学林、何周和卢炜等，在此对大家的辛勤工作表示衷心的感谢。

若您在阅读本书的过程中遇到困难或疑问，可以给我们写信，我们的E-mail是book@jzbooks.com。我们还专门开通了一个网站，以解答您的疑难问题，网址是http://www.jzbooks.com。另外，您也可以申请加入九州书源QQ群：122144955，进行交流与答疑。

编　者

目 录

Chapter 1

第1章

走进黑客世界

小魔女：我今天上网看到一则新闻：某个国家的军用网站被黑客攻击了。太不可思议了!黑客到底是什么啊？这么厉害!

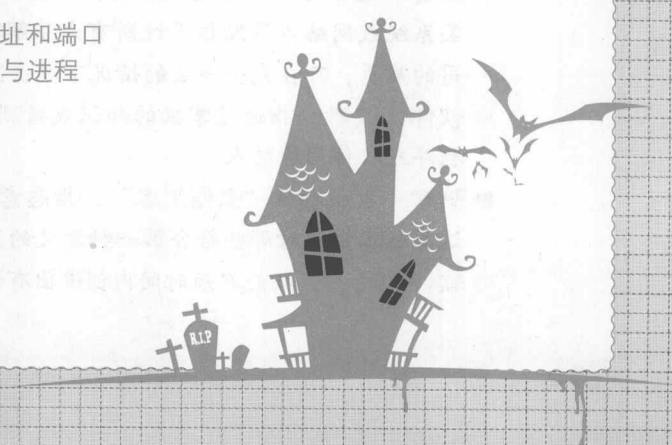
魔法师：其实黑客在很久以前就有了，他们是具有高超电脑技术的电脑爱好者。

小魔女：那要怎样才能成为一名黑客呢？我也想成为他们那样的人，那我就可以在网络中任意驰骋了。

魔法师：要想成为黑客可没那么简单！但是掌握一些黑客技术，能进行一些简单的黑客攻击和防御黑客入侵还是不错的。下面我将给你讲解一些关于黑客的基本知识，带你走进黑客的世界。

学习要点：

- 认识黑客
- 查看IP地址和端口
- 系统服务与进程



1.1 认识黑客

魔法师：要想学习黑客技术，首先需要知道什么是黑客以及黑客应掌握的技能。

小魔女：那么，要怎样才能成为黑客呢？黑客是怎样对电脑进行攻击的呢？

魔法师：黑客可以发现计算机系统及网络的缺陷和漏洞，并针对这些缺陷实施攻击。同时，黑客攻击电脑的手段多种多样，下面将分别进行介绍。

1.1.1 如何成为黑客

黑客（hacker）原指那些热衷于电脑技术，并具有一定编程水平的电脑爱好者。目前，黑客也泛指那些利用电脑网络搞破坏的人，也可将这类人称为骇客（cracker）。要成为一个黑客应满足以下几点要求。

- **解决问题的态度：**将遇到的需要解决的各种问题当做生活的乐趣和动力，将已经解决的问题作为信息进行共享。这样，黑客技术将不断地被人们掌握并有更多的精力去探索与解决新问题。
- **掌握黑客的基本技能：**首先应掌握一些黑客软件，并学会一门编程语言，重要的是，学会如何以一个通用的方法思考编程问题，独立于任何语言。也应该会写HTML与Web的标记语言。
- **制订有效的学习计划：**通过对系统的逐步了解逐渐掌握配置Windows的一些服务的方法，能熟练配置各种网络设备进行联网，并具有一定的英语基础。

1.1.2 黑客的类型

由于系统、网络和软件不可避免地会存在安全漏洞，而黑客能够找出并弥补这些漏洞，因此，从某种意义上来讲，电脑的安全需要黑客去维护。但一些黑客在找出安全漏洞之后，为了显示其本领和成就，会对电脑大肆进行恶意破坏，所以黑客也被人们认为是在网络上进行破坏的人。因此，黑客可分为以下几种：

- **黑客：**也被称作“白帽黑客”、“匿名客”（sneaker）或“红客”，指那些试图破解某系统或网络以帮助该系统所有者了解存在的安全隐患的人。他们大多是电脑安全公司的雇员，可在完全合法的情况下攻击某系统。
- **软件修改者：**指通过掌握的知识或猜测对某段程序或软件做出更完善的修改，以增强程序或软件用途的人。
- **骇客：**也被称作“黑帽黑客”，指恶意破解或破坏某个程序、系统及网络安全的人。这类骇客常常对那些符合第一种意义的黑客造成严重困扰。
- **软件编辑者：**指能在短时间内创造出有价值软件的人，他们精通某领域内的编程语言。

1.1.3 黑客的攻击手段

黑客的攻击手段可分为非破坏性攻击和破坏性攻击两类。其中，非破坏性攻击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的方式进行；而破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的的。下面将介绍以下几种常见的攻击手段。

- **后门程序**：当程序员设计一些功能复杂的程序时，开启后门将便于测试、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，但有时由于疏忽或其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去除，这时黑客就可以利用这些后门进入系统并发动攻击 。
- **信息炸弹**：信息炸弹是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、网络堵塞或系统崩溃的攻击手段。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。
- **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（包括消耗系统可用空间、带宽资源），最后使网络服务瘫痪的一种攻击手段。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，因而影响巨大，顷刻就可使被攻击目标带宽资源耗尽，导致服务器瘫痪。
- **网络监听**：网络监听是一种监视网络状态、数据流以及网上传输信息的管理工具，它可以将网络接口设置为监听模式，并可截获网上传输的信息。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，可使用网络监听来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，通常被用来获取用户口令。

1.1.4 常见的黑客攻击平台——DOS

DOS（Disk Operating System，磁盘操作系统）是一种非常实用的操作系统，它采用的是命令提示符界面。DOS的核心启动程序只有几个文件，包括Boot系统引导程序、IO.sys、MSDOS.sys和COMMAND.com。它们是构成DOS系统的基础，且这些文件占用的存储空间非常小，甚至不到1MB。

目前，安装DOS可以通过在Windows操作系统中安装MaxDos软件来实现，也可以直接运行Windows操作系统中的命令提示符来完成。后者的具体操作为：选择【开始】/【运行】命令，在“运行”对话框的“打开”下拉列表框中输入“cmd”（见图1-1），然后按Enter键即可打开命令提示符窗口，如图1-2所示。在使用DOS时，其所有的核心启动程序都是被临时存储在内存中的，用户可随意使用。

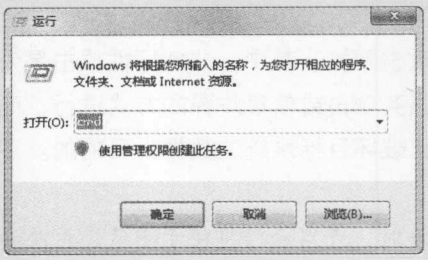


图1-1 “运行”窗口

图1-2 命令提示符窗口

晋级秘诀——在“开始”菜单中添加“运行”命令

在Windows7操作系统中，默认状态下“运行”命令是隐藏的，用户需通过设置才能将其显示在“开始”菜单中。其方法为：单击“开始”按钮，在“开始”菜单空白处单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开“任务栏和「开始」菜单属性”对话框的“「开始」菜单”选项卡中单击 自定义(C)... 按钮，打开“自定义「开始」菜单”对话框，在其下方的列表框中选中 ☑ 运行命令 复选框，然后单击 确定 按钮，保存更改，此时在“开始”菜单中将显示“运行”命令，如图1-3所示。

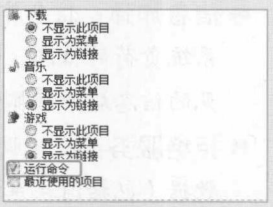


图1-3 添加“运行”命令

1.2 查看IP地址和端口

魔法师：黑客攻击电脑时，通常需要知道电脑的IP地址和开放的端口，他们通过IP地址和端口可控制电脑并进行各种操作。

小魔女：IP地址和端口是什么东西啊？它们具体有什么作用呢？我怎样才能获取它们呢？魔法师，你能教教我吗？

魔法师：就像街道上的住户都有各自的牌号一样，每台网络上的电脑都被分配了一个唯一的数字序列，这样，在查找网络中的某台电脑时，不会出现“冒名顶替”的现象，这个数字序列就是IP地址；端口可用于传输电脑数据信息，它们是虚拟存在的事物，也是电脑中必不可少的元素，下面将给你介绍IP地址和端口的相关知识。

1.2.1 认识IP地址和端口

电脑的IP地址和端口具有重要的意义，电脑的正常使用也离不开IP地址和端口的支持，下面将分别介绍IP地址和端口的意义。

- IP地址：电脑网络中使用的协议是一种类似于技术手册的数字化文本，可用来规范电

脑间的信息交流，使电脑能顺畅地发送和接收所需的信息。网络中的协议有很多，其中最常用到的协议就是TCP/IP协议。IP地址是TCP/IP协议的一个重要组成部分，它可用来给Internet上的电脑编号。网络中的每台电脑都需有IP地址才能正常通信。

- 端口：端口是一种由操作系统或软件提供，专为电脑通信而存在，用于传输数据信息的连接端，它不是一个硬件，是通过TCP/IP协议定义的一个TCP连接的连接端。通常一台电脑中可以存在成千上万个端口。要有效地防御黑客攻击，需要学会如何查看本地电脑开放的端口，并了解它的服务信息和安全状况。

1.2.2 获取IP地址

获取的电脑IP地址分为本地电脑的IP地址和其他电脑的IP地址，这两种IP地址都可以使用命令的方法来获取，下面将分别对其进行介绍。

1. 获取本地电脑的IP地址

要获取本地电脑的IP地址需要使用ipconfig命令，该命令是Windows操作系统中调试电脑网络的常用命令，通常用于显示电脑中网络适配器的IP地址、子网掩码以及默认网关。

ipconfig命令的格式为ipconfig[/all][/batch][/release_all][release N][/renew_all][/renew N]，当在DOS中直接输入ipconfig时，将显示用户的本地电脑的IP信息。下面将使用ipconfig命令查看本地电脑的IP信息，其具体操作如下：

步骤 01 选择【开始】/【运行】命令，在打开的“运行”对话框中的“打开”下拉列表框中输入“cmd”，然后单击 确定 按钮，如图1-4所示。

步骤 02 打开命令提示符窗口，在其中输入“ipconfig”命令，按Enter键即可显示当前主机的IP信息，如图1-5所示。

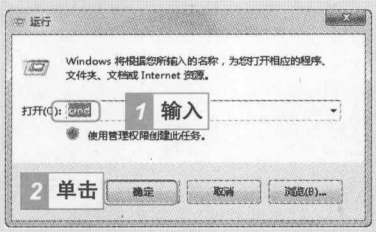


图1-4 “运行”对话框

图1-5 查看本地电脑的IP信息

2. 获取其他电脑的IP地址

使用ping命令可以测试目标主机的主机名、IP地址信息以及验证本地主机与远程主机的连接情况。ping命令是基于TCP/IP连接的，只有在安装了TCP/IP协议后才能使用该命令。

由于网站的域名比IP地址更直观，因此人们普遍会记下某个网站的域名。在已知域名的

情况下，可以搜集目标网站的IP地址信息，如获取新浪服务器的IP地址，其具体操作如下：

步骤 01 选择【开始】/【运行】命令，在打开的“运行”对话框中的“打开”下拉列表框中输入“cmd”，然后单击 确定 按钮。

步骤 02 打开命令提示符窗口，在其中输入“ping www.sina.com”命令，按Enter键，返回的“221.236.31.143”即为搜集到的“www.sina.com”网站的IP地址，如图1-6所示。

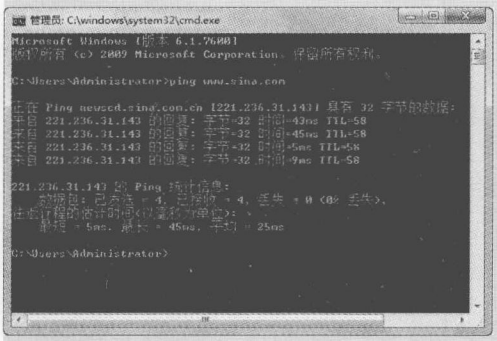


图1-6 查看新浪网的IP地址

魔法档案——ping命令的格式与含义

ping命令的格式为：ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL]。其中，[-t]表示ping指定的主机；[-a]表示将地址解析成主机名；[-n count]表示要发送的回显请求数；[-l size]表示发送缓冲区大小；[-f]表示在数据包中设置“不分段”标志（仅适用于IPv4）；[-i TTL]表示生存时间。

1.2.3 获取端口信息

与IP地址的获取相似，端口信息的获取也可以通过DOS命令来实现。除此之外，还可以借助一些黑客工具来获取电脑的端口信息，相关知识将在后面的章节中讲到。

netstat命令是Windows操作系统自带的查看网络状况的命令。其格式为：netstat [-a] [-e] [-n] [-o] [-s] [-p protocol] [-r] [interval]。其中[-a]参数是显示所有连接和监听的端口，[-n]参数是以数字格式显示地址和端口号。查看本地电脑开放的端口信息，其具体操作如下：

步骤 01 选择【开始】/【运行】命令，在打开的“运行”对话框中的“打开”下拉列表框中输入“cmd”，然后单击 确定 按钮。

步骤 02 打开命令提示符窗口，在其中输入“netstat -an”命令，按Enter键即可查看本地电脑所开放的端口信息，如图1-7所示。

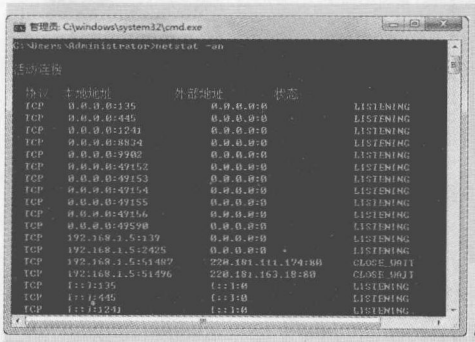


图1-7的端口信息列表中的“TCP”指使用的协议名称；“本地地址”栏的数据指本地IP地址和正在使用的端口号；“外部地址”栏的数据指连接某端口的远程主机的IP地址和端口号；“LISTENING”指该远程端口是开放的，正在监听等待连接。

图1-7 查看电脑端口信息