本丛书5种荣获“全国优秀畅销书奖”（科技类）
本丛书累计销售超过100万册
本丛书先后被400余所培训机构选作参考书

全国优秀畅销品种

一学就会魔法书

（第2版）

电脑黑客攻防入门

DVD VIDEO

全程动画、语音教学演示

九州书源 编著

DVD光盘：4.5G超大容量学习资料库

立体化学习资料6类：

◎ 高清多媒体教学演示，手把手演示
◎ 实例所需素材及源文件，直接调用很方便
◎ 常见问题解答300个，扫除学习障碍
◎ 应用技巧11000例，提高学习效率
… …

赠深度学习教学演示45小时：

◎ 15小时Windows XP深入学习多媒体教学演示
◎ 15小时Windows Vista深入学习多媒体教学演示
◎ 15小时电脑选购/组装/维护/故障排除深入学习多媒体教学演示

赠官方授权软件9款：

◎ Office 2007简体中文版（试用版）
卡巴斯基杀毒软件（免费使用1个月）
◎ 微点主动防御软件（第三代反病毒软件）免费使用3个月
◎ Camtasia Studio视频录制软件

清华大学出版社

一学就会魔法书（第2版）

电脑黑客攻防入门

九州书源　编著

清华大学出版社

北　京

内 容 简 介

本书主要讲述了目前最流行的黑客攻防的基础知识和操作以及各种应用实例，主要内容包括接触黑客攻击、常用黑客工具介绍、安装与清除木马、QQ 攻防、入侵和保护操作系统、攻击和保护 IE 浏览器、窥探和保护电子邮件、密码攻防战、ARP 欺骗攻防、远程监控攻防、开启后门与痕迹清除和建立电脑的防御体系等知识。

本书内容深入浅出，从黑客技术的基础知识入手，逐步提高到使用与防范常用黑客技术和黑客软件的水平，使读者的黑客攻防水平得到较大的提高。本书提供了大量实例，以帮助读者了解并掌握黑客技术和黑客软件的使用方法；每章后面附有大量丰富生动的练习题，以检验读者对本章知识点的掌握程度，达到巩固所学知识的目的。

本书定位于有一定电脑知识的用户，可供在校学生、电脑技术人员、各种电脑培训班学员以及不同年龄段想了解黑客技术的电脑爱好者学习参考。

图书在版编目（CIP）数据

电脑黑客攻防入门/九州书源编著. —2 版. —北京：清华大学出版社，2009.7
（一学就会魔法书）

ISBN 978-7-302-19461-3

I. 电… II. 九… 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 016228 号

责任编辑：刘利民　朱英彪　郭　伟
封面设计：刘洪利　刘　超
版式设计：刘　娟
责任校对：姜　彦
责任印制：李红英
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：北京鑫丰华彩印有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：17　**字　数**：393 千字
（附 DVD 光盘 1 张）
版　　次：2009 年 7 月第 2 版　　**印　　次**：2009 年 7 月第1 次印刷
印　　数：1～8000
定　　价：29.80 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：032047-01

“魔法书”传奇

——“一学就会魔法书”（第1版）故事

“一学就会魔法书”（第1版）自2005年出版以来，以其新颖的多媒体教学，翔实丰富的内容，轻松愉快的风格，受到广大读者的热烈欢迎，先后被400多所机构选为培训教材，累计销量逾百万册，创造了电脑基础类图书销售的奇迹，5种图书被评为“2006年度全行业优秀畅销品种”（全国优秀畅销书奖），轰动一时。

一学就会 魔法书 （第2版）

光盘使用说明

“一学就会魔法书”（第2版）是在第一版的基础上改进而来，它的光盘内容和使用说明如下：

一、打开光盘

1．把光盘放入光驱后，一般会自动运行，否则，可在光盘根目录下，双击autorun.exe文件。

2．光盘运行几秒钟后进入主界面。

单击，可在弹出的菜单中快速定位到目标章节

单击，可进入光盘根目录，方便您直接利用附赠的素材和软件进行学习

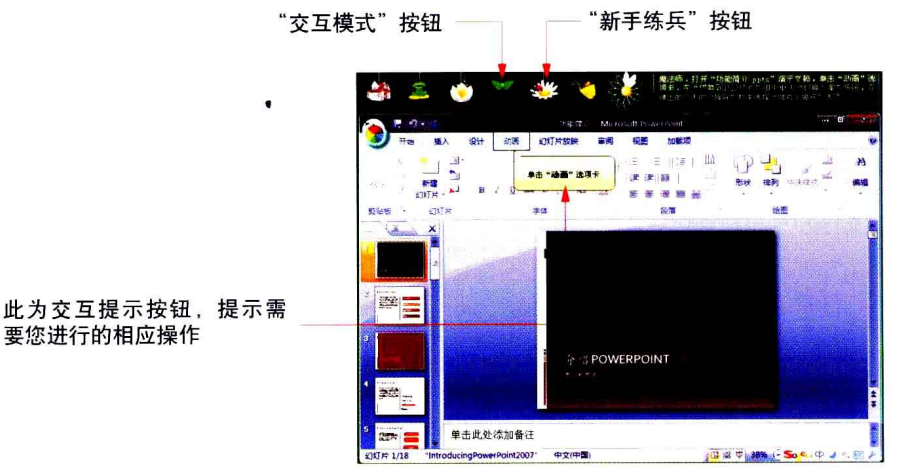
囊括各类电脑应用技巧。

（接封-）

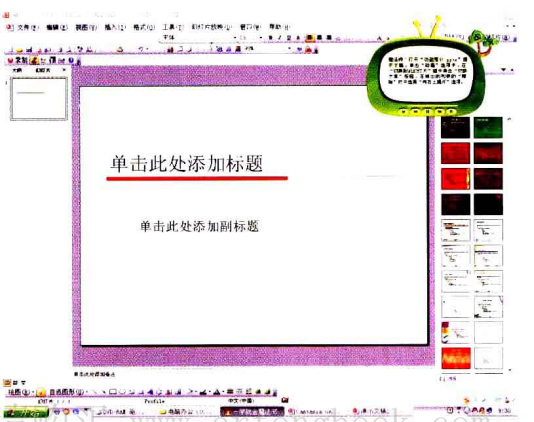
二、多媒体教学演示

三、教学互动

1. 在播放界面单击“交互模式”按钮，当出现  时，表明您已进入模拟操作状态，此状态下是模拟操作，您需要按照提示操作，才能向下进行，再次单击该按钮即可恢复正常播放。



2. 单击“新手练兵”按钮，播放界面将缩放至桌面右上角，此时您便可以在实际界面上根据语音讲解进行操作了。



再致亲爱的读者

——一学就会魔法书（第2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年出版以来，曾在全国各大书店畅销一时，先后有近百万读者通过这套书学习了电脑相关技能，被全国各地400多家电脑培训机构、机关、社区、企业、学校选作培训教材，截至目前，这套书累计销售近100万册，其中5种荣获2006年度“全国优秀畅销书”奖。

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”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2版）继承了第1版的优点：“轻松活泼”“起点低，入门快”和“情景式学习”等，力求让读者把一个个电脑技能当作“魔法”来学习，在惊叹电脑神奇的同时，轻松掌握操作电脑的技能。

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，书中以一个活泼可爱的“小魔女”的学习历程为线索，循着她学习的脚步，读者可以掌握一项项技能，解决一个个问题，同时还有一个“魔法师”循循善诱，深入浅出地讲解各个知识点，并不时提出学习建议。情景式学习，寓教于乐，让学习轻松、愉快、充满情趣。

（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）多媒体教学演示，如同老师在身边手把手教您

多媒体演示中，通过 3 个虚拟人物再现了一个学习过程：一个活泼可爱的“小魔女”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）多媒体教学练习，边看边练是最快的学习方式

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一应俱全

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）赠品：提供多款安装软件（试用版），不用额外去获取

为了方便读者，本光盘提供了“Office 2007”简体中文测试版软件、“卡巴斯基”杀毒软件（免费使用 1 个月）、微点主动防御软件——电脑病毒免疫专家（免费使用 3 个月），还附带了多种工具软件，如屏幕录制软件等。

（五）赠品：额外提供更加深入的多媒体演示和相关素材

为了便于读者深入学习，本光盘在“软件与赠品”目录下额外提供了更加深入的多媒体教学演示和相关素材，读者可根据该内容自行学习。

九州书源

前言

黑客的攻击手段越来越“高明”，而防御黑客攻击的方法也在不断地衍变，如果您对黑客攻击和防御还比较陌生，不了解常用黑客工具的使用方法，不会修补系统漏洞和应付漏洞攻击，对木马程序和远程监控毫无认识，并且常常因 QQ、电子邮件账户等出现故障而烦恼……那么本书将是您最好的朋友，它将引领您进入黑客的世界。本书将以 Windows XP 为操作平台来讲解黑客的各种攻击和防御方法。

本书内容

黑客技术所涉及的知识面很广，为了使读者掌握最实用的黑客攻击和防御知识，我们根据黑客技术的使用频率以及操作的难易程度精心安排了各章节，使初学者在本书的引导下可以循序渐进地掌握黑客攻防技术，并灵活运用于各个领域。本书共 12 章，可分为以下 5 个部分。

章　节	内　容	目　的
第 1 部分（第 1 章）	黑客攻击的特点、黑客常用的攻击命令	大致了解黑客攻击，熟悉常用黑客命令的操作界面和基本操作方法
第 2 部分（第 2～3 章）	使用和防范常用的黑客软件、木马	掌握黑客工具和木马的使用方法
第 3 部分（第 4～7 章）	了解和掌握 QQ、电脑操作系统、IE 浏览器和电子邮件的攻防知识	掌握常用软件和电脑系统的黑客攻防知识
第 4 部分（第 8～11 章）	使用黑客技术进行密码、ARP、远程监控和后门的攻防	掌握常用黑客技术的相关操作
第 5 部分（第 12 章）	使用各种手段保护电脑，免受黑客攻击	能利用系统自带的维护工具、防火墙、杀毒软件来保护电脑

本书适合的读者对象

本书适合以下读者：

（1）迫切需要提高黑客攻防综合技能的初学者。

（2）掌握一定的电脑技术，并想进一步学习黑客技术的电脑用户。

（3）对学习黑客技术非常有兴趣的电脑爱好者及学生。

如何阅读本书

本书每章均按照“本章要点+内容导读+本章内容+常见问题解答+过关练习”的结构进行讲述。

- ❖ **本章要点**：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。
- ❖ **内容导读**：通过“小魔女”和“魔法师”的对话引出本章内容，活泼生动的语言让人读来兴趣盎然，同时可以了解学习本章的原因和重要性。
- ❖ **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巩固知识点。
- ❖ **常见问题解答**：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”一一作答，达到帮助读者解惑、扩展知识面的目的。
- ❖ **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，本书内容就由他们贯穿始终。读者可以结合多媒体教学光盘，随着“小魔女”的学习步伐，听听“魔法师”的讲解，通过互动式学习，掌握电脑的基本操作。

（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，并在关键步骤加以简单的文字描述，有联系的图与图之间用箭头连接起来，体现操作的动态变化过程，读者只要结合文字讲解就可以很容易地学会相应操作。

（3）本书将丰富生动的实例贯穿于知识点中，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魔力测试两个小栏目。看到“小魔女”、“魔法师”卡通和“魔法档案”可要提高警惕哟，它们都是需要重点注意的地方。“魔力测试”实际就是强化知识点的小练习，只要即时练习，趁热打铁，就能记忆深刻。

（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。

创作队伍

本书由九州书源组织编著，参加编著的有向利、徐云江、明春梅、陆小平、袁松涛、杨明宇、段里、官小波、汪科、方坤、牟俊、陈良、范晶晶、唐青、张春梅、董娟娟、李伟、余洪、杨颖、张永雄、吴永恒、赵华君、李显进、赵云、林涛、朱鹏、蒲涛、徐倾鹏、程云飞、常开忠、孙兵、刘成林、李鹏、彭启良、张笑、骆源、张正荣。在此对大家的辛勤工作表示衷心的感谢！

对于本书，我们已经努力做到了“好”，您尽可以放心地阅读和学习，相信它会成为您的良师益友。若您在阅读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。我们还专门为本书开通了一个网站，以解答您的疑难问题，网址是 http://www.jzbooks.com。

编　者

目录 MULU

第1章

接触黑客攻击

多媒体教学演示：20分钟

- 黑客攻击的流程
- 获取电脑IP地址的方法
- 扫描开放的端口
- NET命令
- tracert命令
- route命令

魔法师：小魔女，你在书里找什么呢？

小魔女：今天上网的时候，看到一个网站显示一些乱码，同学说这个网站是被黑客攻击了，黑客到底是干什么的？真的这么厉害吗？

魔法师：你所看到的黑客并不是真正意义上的黑客，而是喜欢搞破坏的“骇客”。

小魔女：那魔法师你能让我也成为一名黑客吗？我好崇拜他们啊。

魔法师：其实黑客并不神秘，只要了解了黑客的一些基本技术，你也可以成为一名黑客。下面就先给你讲解一些黑客攻击的基础知识，以便能更好地防御黑客的攻击。

1.1 黑客攻击的特点

黑客（Hacker）原是指那些热衷于电脑，并具有一定编程水平的电脑爱好者。由于系统、网络和软件不可避免地存在某些安全漏洞，而黑客的出现就是为了找出并弥补这些漏洞。目前在国内黑客也泛指非法入侵他人电脑系统的电脑爱好者，但在国外常把那些破坏者另称为骇客（Cracker）。

1.1.1 黑客为什么要攻击

由于少数高水平的黑客可以随意入侵他人的电脑，并在被攻击者毫不知晓的情况下窃取电脑中的信息后悄悄退出，于是很多人对此产生较强的好奇心和学习黑客技术的欲望，并在了解了黑客攻击技术之后不计后果地进行尝试，给网络造成极大的安全威胁。下面是黑客进行攻击的常见理由：

- 想在别人面前炫耀一下自己的技术，如进入别人电脑修改一下文件和系统，算是打个招呼，也会让他对自己更加崇拜。
- 看不惯他人的某些做法，又不方便当面指责，于是攻击他的电脑教训一下。
- 好玩、恶作剧，这是许多人或学生入侵或破坏的主要原因，除了有练功的效果外还有些探险的感觉。
- 窃取数据，偷取他人的 QQ、网游密码等，然后从事商业活动。
- 对某个单位或组织表示抗议。

其实，黑客及黑客技术并不神秘，也并不高深。一个普通的网民在具备了一定的基础知识后，也可以成为一名黑客。另外，黑客技术是一把双刃剑，通过它既可以侵入他人的电脑，又可以了解黑客入侵的手段，掌握保护电脑、防范入侵的方法。我们在学习黑客技术时，首先应该明确学习的正确目的。

1.1.2 了解黑客攻击的流程

一般来说，黑客对电脑进行攻击的步骤大致相同，主要包括以下几步。

- **扫描漏洞**：目前大多数电脑安装的是 Windows 操作系统，Windows 操作系统的稳定性和安全性随着其版本的提升而得到不断的提高，但难免会出现这样或那样的安全隐患，这些安全隐患就是漏洞。黑客通过其专业的研究发现了这些漏洞，于是使用病毒和木马通过这些漏洞攻击和破坏电脑。
- **试探漏洞**：在了解了目标主机的漏洞和弱点之后，黑客就能使用缓冲区溢出和测试用户账号和密码等，达到对其进行试探性攻击的目的。
- **取得权限与提升权限**：如果试探出了可以利用的漏洞，那就意味着黑客获得了攻击该目标主机的初步权限，只要能登录目标主机，那么提升权限将变得易如反掌，借助木马等程序可以更顺利地达到目的。在某些情况下，黑客在取得权限与提升

权限时会采用破坏目标电脑操作系统的方法来实现。

- **木马入侵**：木马是一种能窃取用户存储在电脑中的账户、密码等信息的应用程序。黑客通过木马程序可以轻易地入侵并控制用户电脑，并在用户不知情的状况下通过用户的电脑进行各种破坏活动。在日常生活中经常出现的 QQ 号码被盗的情况，一般就是黑客通过木马进行窃取的。
- **建立后门与清理痕迹**：为了达到长期控制目标主机的目的，黑客在取得管理员权限之后会立刻在其中建立后门，这样就可以随时登录该主机。为了避免被目标主机的管理员发觉，在完成入侵之后需要清除其中的系统日志文件、应用程序日志文件和防火墙的日志文件等，清理完毕即可从目标主机中退出。至此，一次完整的黑客攻击便完成了。

1.1.3　认识常用的攻击平台——DOS

DOS（Disk Operating System，磁盘操作系统）是一种非常实用的操作系统，它采用命令提示符界面，如图 1-1 所示。要使用 DOS，必须先安装 DOS。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，因此过去常使用软驱来安装 DOS。目前较常用的安装 DOS 的方法是通过在 Windows 操作系统中安装 MaxDos 软件来实现，也可以直接运行 Windows XP 中的命令提示符来完成，如图 1-1 所示。在使用 DOS 时，其所有的核心启动程序都被临时存储在内存中，用户可随意使用。

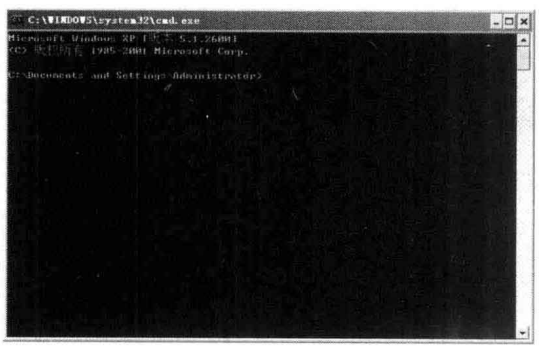


图 1-1　DOS 的操作界面

1.1.4　获取电脑的 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。现在网络中的协议有很多，其中最常用的协议就是 TCP/IP 协议。

IP 地址是 TCP/IP 协议中的一个重要组成部分。就像给街道上的住户编列门牌号一样，

它给网络上的每台电脑都分配了一个唯一的数字序列，使得在查找网络中的某台电脑时不会出现“冒名顶替”的现象。

1.1.5 获取本地电脑 IP 地址

要获取本地电脑 IP 地址需要用到 ipconfig 命令。ipconfig 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]。在 DOS 中直接输入“ipconfig”时，将显示本地电脑的 IP 信息。

使用 ipconfig 命令查看本地电脑 IP 信息的具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2 打开命令提示符窗口，输入“ipconfig”命令，按【Enter】键，即可显示当前主机的 IP 信息，如图 1-2 所示。

图 1-2 显示当前主机的 IP 信息

魔法档案

ipconfig 命令有 4 个参数，其中[/all]参数将显示所有网络适配器如网卡和拨号连接等的完整 TCP/IP 配置信息；[/batch]参数将所显示的 IP 信息以文本的方式写入指定文件；[/release_all]或[/release N]将释放全部或指定适配器中由 DHCP 分配的动态 IP 地址；[/renew_all]或[/renew N]参数将为全部或指定的适配器重新分配 IP 地址。

1.1.6 获取其他电脑 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。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、更好记，因此人们普遍记忆某个网站的域名，继而搜集目标网站的 IP 地址信息。下面以获取网易服务器的 IP 地址为例进行介绍，具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮，如图 1-3 所示。

步骤 2 打开命令提示符窗口，输入“ping www.163.com”命令，按【Enter】键，返回的 220.181.28.52 即为搜集到的 www.163.com 网站的 IP 地址，如图 1-4 所示。