从入门到精通

指引入门捷径 直通高手殿堂

新编

黑客攻防

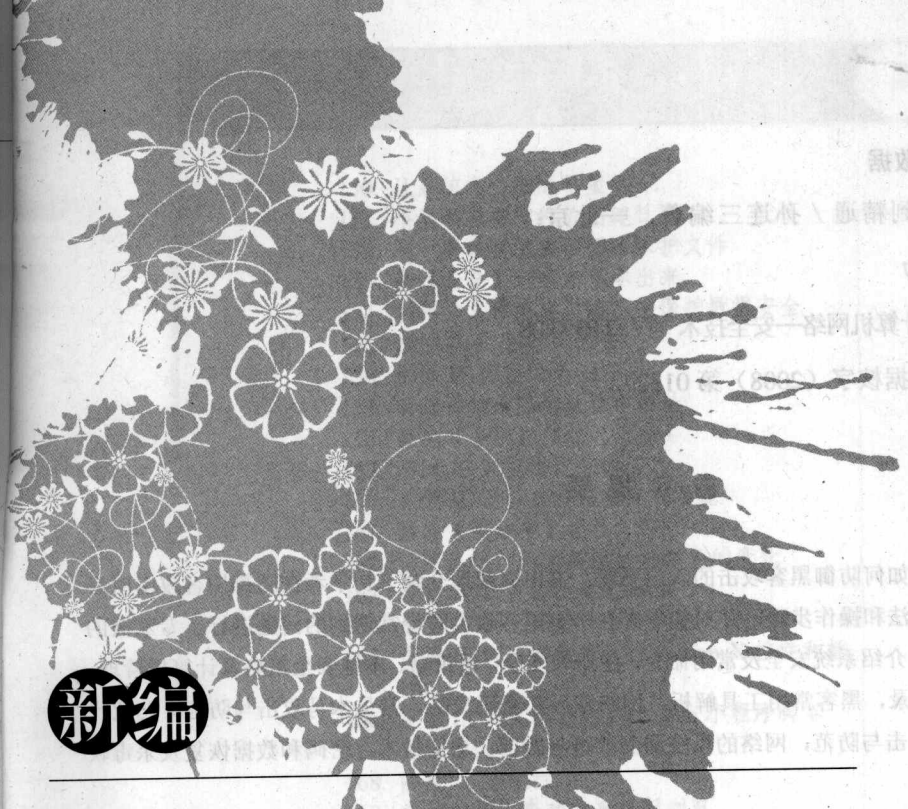
本套书由**“6度获得全国优秀畅销书的作者+教育专家”**组织编写，按照初学者接受知识的难易程度，由浅入深地布局内容，不仅能帮助初学者快速掌握黑客软件的基本操作，而且能教会初学者使用黑客软件进行网络攻防的技能。

超值光盘

包括**80**分钟多媒体教学录像，分**9**个大型的实例进行攻防分析。另赠送一本**492**页、内含**300**个经典的黑客攻防应用技巧的电子书。

◉ 神龙工作室 孙连三 编著

人民邮电出版社
POSTS & TELECOM PRESS



新编

黑客攻防

从入门到精通

◉ 神龙工作室 孙连三 编著

人民邮电出版社

北京

图书在版编目（CIP）数据

新编黑客攻防从入门到精通 / 孙连三编著. —北京：人民邮电出版社，2008.4
ISBN 978-7-115-17571-7

Ⅰ. 新… Ⅱ. 孙… 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（2008）第 013272 号

内 容 提 要

本书是指导初学者学习如何防御黑客攻击的入门书籍。书中详细地介绍了初学者在防御黑客攻击时必须掌握的基本知识、使用方法和操作步骤，并对初学者在防御黑客攻击时经常遇到的问题进行了专家级的指导。全书共分 13 章，分别介绍系统安全及常用命令，注册表安全，组策略、本地安全策略及计算机管理，清除系统、网络及软件的记录，黑客常用工具解析，网络账号和密码攻防，常见木马攻击与防范，恶意代码攻击与防范，U 盘病毒攻击与防范，网络的系统漏洞攻击与防范，加密技术，密码和数据恢复及杀毒软件和防火墙的使用等内容。

本书附带一张精心开发的专业级多媒体教学光盘，它采用全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行了深入的讲解，一步一步引导读者完成黑客攻击与防御的各种应用。光盘中还包括一本 492 页、内含 300 个经典的黑客攻防应用技巧的电子书，大大扩充了本书的知识范围。

本书既适合于刚刚接触 Internet 的初学者阅读，又可以作为大专院校或者企业的培训教材。

新编黑客攻防从入门到精通

◆ 编　　著　神龙工作室　孙连三
责任编辑　魏雪萍

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京精彩雅恒印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：24
字数：602 千字　　2008 年 4 月第 1 版
印数：1 – 6 000 册　　2008 年 4 月北京第 1 次印刷

ISBN 978-7-115-17571-7/TP

定价：49.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

配套光盘导航

介绍系统安全的相关知识和操作

介绍加密隐私文件的相关操作

介绍黑客的攻击工具并进行Web攻防演示

随书附赠大量应用技巧

介绍数据恢复的相关知识和黑客的基本命令

介绍chm电子书木马和远程控制任我行的知识

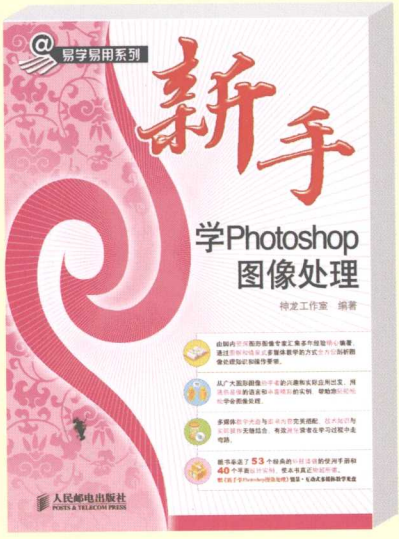
滑块的位置表示当前演示的进度，拖动滑块可以实现快进或快退

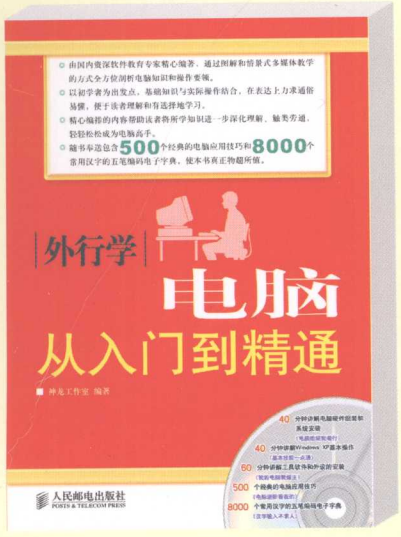
拖动“背景音量”和“解说音量”滑块可以调节相应音量的大小

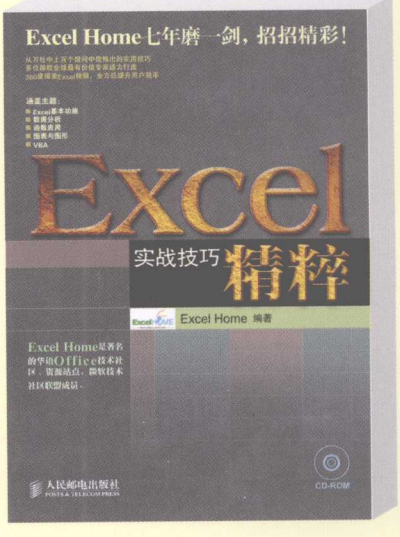
积淀孕育创新
品质铸就卓越

全国优秀
畅销书

全国优秀畅销书推荐







前 言

电脑是现代信息社会的重要标记，掌握丰富的电脑知识，正确熟练地操作电脑已成为信息化时代对每个人的要求。鉴于此，为满足广大读者学习电脑知识及电脑操作的需要，我们针对不同的学习对象的掌握能力，总结了多位电脑高手及计算机教育专家的经验，精心编写了这套“新编从入门到精通”丛书。

丛书主要内容

本套丛书涉及读者在日常工作和学习中各个常见的电脑应用领域，在介绍软硬件的基础知识及具体操作时都以大家经常使用的版本为主要讲述对象，在必要的地方也兼顾了其他的版本，以满足不同领域读者的需求。本套丛书主要包括以下图书。

新编 Windows Vista 中文版从入门到精通	新编办公软件从入门到精通
新编外行学电脑从入门到精通	新编 Excel 2003 中文版从入门到精通
新编外行学上网从入门到精通	新编 Word 2003 中文版从入门到精通
新编 Windows XP 中文版从入门到精通	新编 PowerPoint 2003 中文版从入门到精通
新编电脑组装与维护从入门到精通	新编 Access 2003 中文版从入门到精通
新编电脑家庭应用从入门到精通	新编 AutoCAD 2008 中文版从入门到精通
新编黑客攻防从入门到精通	新编 Word/Excel 高效办公从入门到精通
新编 Photoshop CS2 中文版从入门到精通	新编 Project 2003 项目管理从入门到精通
新编系统安装·重装·备份与还原从入门到精通	新编系统优化·安全设置·防杀电脑病毒从入门到精通
新编 Photoshop CS3 中文版从入门到精通	新编 Photoshop CS3 从入门到精通
新编 Flash CS3 动画制作从入门到精通	新编 ProENGINEER 野火版 3.0 中文版从入门到精通
新编 3ds Max 9 三维动画创作从入门到精通	新编 UG NX 4.0 中文版从入门到精通
新编 CorelDRAW X3 矢量绘图从入门到精通	新编 AutoCAD 2008 从入门到精通
新编 Premiere Pro 2.0 影视制作从入门到精通	新编 SQL Server 2005 数据库管理与开发从入门到精通
新编 HTML 网页设计从入门到精通	新编 Dreamweaver CS3 精彩网站制作从入门到精通
新编 Visual Basic 6.0 程序设计从入门到精通	新编 Visual FoxPro 6.0 数据库管理与开发从入门到精通
新编 VB.NET 2005 程序设计从入门到精通	新编 ASP.NET 2.0 网站开发从入门到精通
新编 Visual C# 2005 程序设计从入门到精通	新编 ASP.NET 2.0 + SQL Server 2005 从入门到精通
新编 Dreamweaver CS3、Flash CS3 与 Fireworks CS3 网页制作三剑客从入门到精通	

写作特色

❖ **双栏排版、超大容量：**本书采用双栏排版的格式，信息量大。在 370 多页的篇幅中容纳了传统版式 500 多页的内容。这样，我们就能在有限的篇幅中为读者奉送更多的知识和实战案例。

❖ **一步一图，图文并茂：**在介绍具体操作步骤的过程中，每一个操作步骤均配有对应的插图。这种图文结合的方法使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于理解和掌握。

❖ **提示技巧，贴心周到：**本书对读者在学习过程中可能会遇到的疑难问题以“提示”和“技巧”的形式进行了说明，以免读者在学习的过程中走弯路。

❖ **精心排版，实用至上**：双色印刷既美观大方又能够突出重点、难点，精心编排的内容可以使读者对所学知识进一步深化理解，触类旁通。

❖ **书盘结合，互动教学**：本书配套多媒体教学光盘内容与书中知识紧密结合并互相补充。在多媒体光盘中，我们仿真工作和生活中的真实场景，让读者体验实际工作环境，并借此掌握生活和工作中所需的知识以及技能，掌握处理各种问题的方法，知道在合适的场合使用合适的方法，以达到学以致用的目的，从而大大地扩充了本书的知识范围。

光盘特点

❖ **内容丰富**：光盘中不仅提供了9个来源于实际生活的涵盖黑客攻防全过程的典型实例，而且还附赠一本492页内含300个经典的黑客攻防应用技巧的电子书，使读者能够轻松、快速地掌握黑客攻防技术。

❖ **超大容量**：本书所配的光盘涵盖了书中绝大多数的知识点，并做了一定的扩展延伸，突破了目前市场上现有光盘内容含量少、播放时间短的缺点。

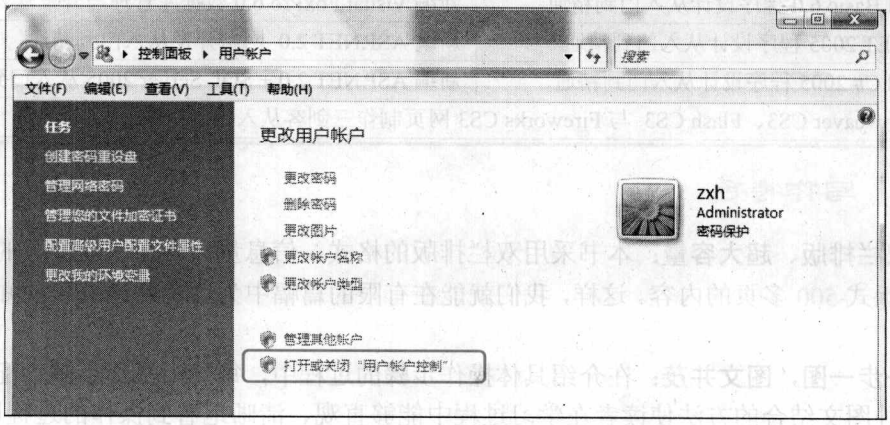
❖ **解说详尽**：光盘在演示黑客攻防经典实例的过程中，对每一个操作步骤都做了详细的解说，使读者能够身临其境，加快学习进度。

❖ **实用至上**：全面突破传统按部就班讲解知识的模式，以解决问题为出发点，通过光盘中9个经典的黑客攻防演示实例，全面涵盖了用户在学习黑客攻防过程中所遇到的问题及解决方案。

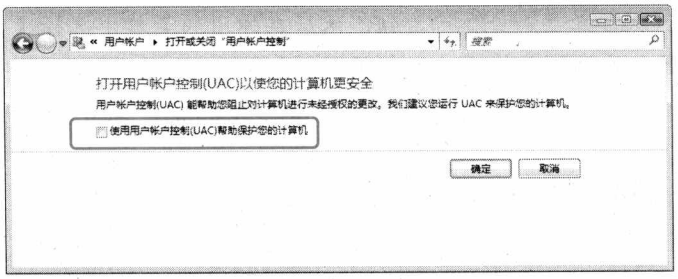
光盘使用须知

❖ **注意**：如果您在Windows Vista操作系统下使用本光盘，请在运行光盘之前关闭用户账户控制（UAC）功能，否则可能会出现报错（在Windows XP系统下不会出现报错）。

1. 单击【开始】➤【控制面板】菜单项，打开【控制面板】窗口。
2. 单击左侧窗格中的【经典视图】链接，切换到经典视图模式，然后双击右侧窗格中的【用户账户】图标，打开【用户账户】窗口。
3. 单击【打开或关闭“用户账户控制”】链接，打开【打开或关闭“用户账户控制”】窗口。



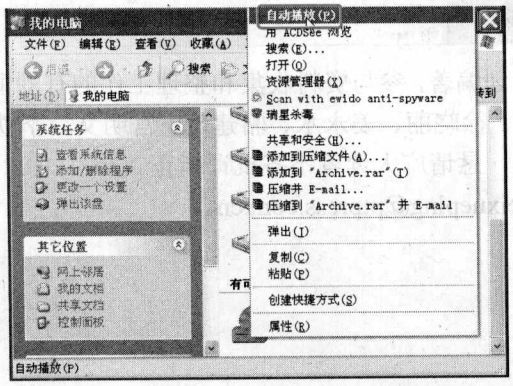
4. 在这里撤选【使用用户账户控制（UAC）帮助保护您的计算机】复选框，然后单击 确定 按钮即可完成更改。



配套光盘运行方法

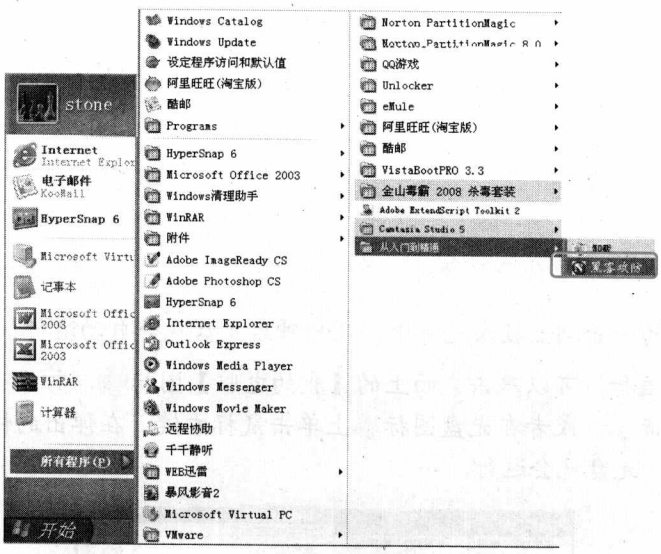
1 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。

2 若光盘没有自动运行，可以双击桌面上的【我的电脑】图标，打开【我的电脑】窗口，然后双击光盘图标，或者在光盘图标上单击鼠标右键，在弹出的快捷菜单中选择【自动播放】菜单项，光盘就会运行。



3 由于光盘长期使用会磨损，旧光驱读盘能力可能也比较差，因此最好将光盘内容安装到硬盘上观看，把配套光盘保存好作为备份。在光盘主界面中单击【安装光盘】按钮，就可以将光盘内容安装到硬盘中了。

④以后观看光盘时，只要单击 开始 按钮，然后在弹出的菜单中选择【所有程序】➢【从入门到精通】➢【黑客攻防】菜单项就可以了。



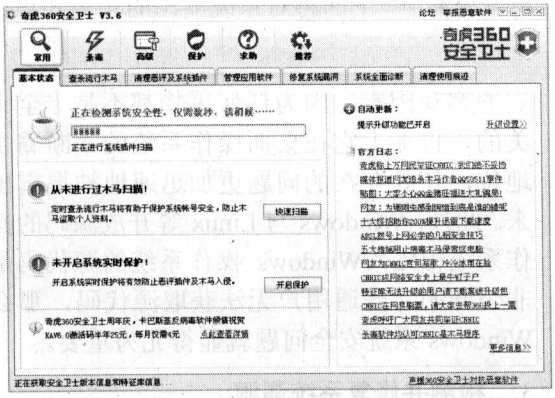
本书由神龙工作室策划编著，参与资料收集和整理工作的有刘恒、刘建、吕兴胜、邓淑文、蔡玉冬、张相红、王福艳、徐晓丽、姜永水、骆建玲、宫明文、李轶君等。由于时间仓促，书中难免有疏漏和不妥之处，恳请广大读者不吝批评指正。

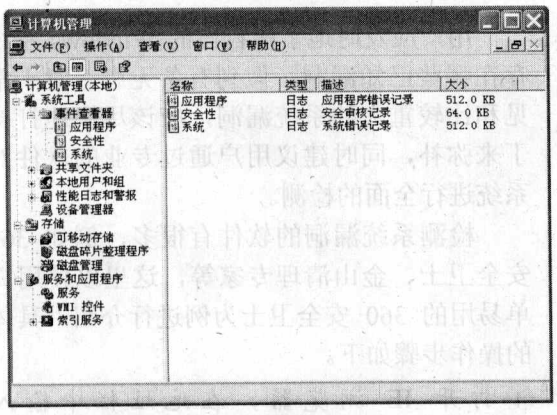
我们的联系信箱：weixueping@ptpress.com.cn。

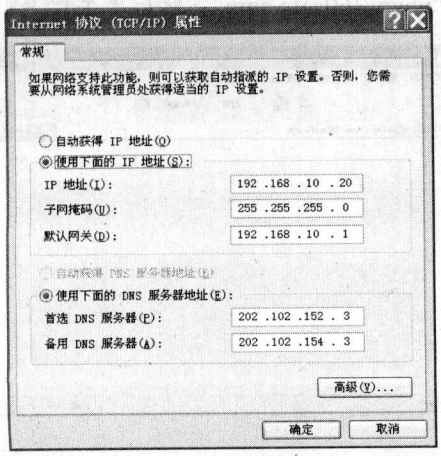
编者

目 录

第 1 章 系统安全和常用命令







利用系统安全漏洞和命令语句是黑客们常用的攻击方式，掌握了这些知识，才能更好地保护计算机的安全，并利用这些命令为黑客服务，小月想学习这些知识就来问小龙，下面就看看小龙是怎么介绍关于系统安全和常用命令的知识吧！

- 系统安全分析
- 黑客常用命令

1.1 系统安全分析

Windows 操作系统是当今主流的操作系统，自推出以来就得到了广大用户的认同并获得广泛的好评。其出色的兼容性和移动性也被业界所推崇，虽然如此，但在系统的安全性上也同样存在着漏洞，因此微软需要不断地推出补丁来弥补这些操作系统的漏洞。

1.1.1 系统漏洞

威胁 Windows 系统安全的最根本的原因就是系统漏洞，下面将对系统漏洞的相关知识进行介绍。

1. 什么是系统漏洞

漏洞是指某个程序或者操作系统在设计时没有考虑周全，当程序遇到一个看似合理，但实际却无法正确处理的问题时引发的不可预见的错误。

系统漏洞又称为安全缺陷，如果漏洞被别有用心的人利用，就会造成信息泄漏、数据丢失、用户的权限被恶意篡改等后果。例如黑客利用网络服务器操作系统的漏洞来攻击网站，可能会影响用户的操作，如计算机不明原因的死机蓝屏、隐藏的共享、丢失文件以及无法上网等。因此只有将系统的漏洞堵住，用户才会有一个安全和稳定的工作环境。

2. 产生漏洞的原因

产生漏洞的原因可以分为以下 3 种。

① 人为因素：编程人员在编写程序的过程中，为了实现一些特殊的目的，有意在程序代码的隐蔽处保留某些后门。

② 能力因素：由于编程人员的能力、经验和当时安全技术的差别，编程人员在程序设计的过程中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升，从而使计算机处于高度危险状态。

③ 硬件因素：由于硬件的原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现出来，例如软件的不兼容问题。

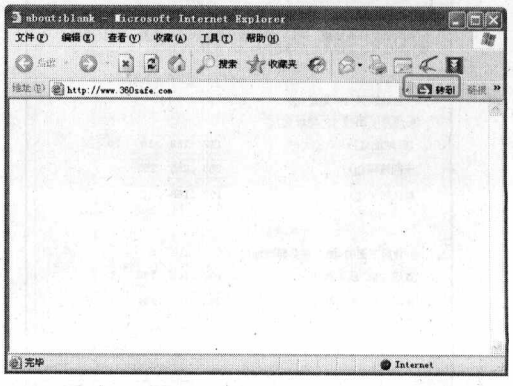
Windows 系统中的漏洞层出不穷也有一定的客观因素，因为任何事物都不是十全十美的，再加上它在桌面操作系统的垄断霸主地位，使其存在的问题更加迅速地被揭露出来。此外，Windows 与 Linux 等开放源码的操作系统相比，Windows 操作系统的源代码是非公开的，普通用户无法获取源代码，那么 Windows 系统安全问题就显得尤为重要。

3. 检测并修复系统漏洞

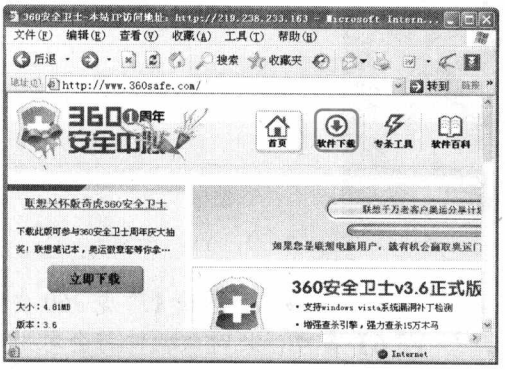
用户应及时地了解自己的 Windows 系统存在哪些已知漏洞，做到有备无患。对于常见和比较重大的系统漏洞，应该尽快地打补丁来弥补，同时建议用户通过专业的软件对系统进行全面的检测。

检测系统漏洞的软件有很多，例如 360 安全卫士、金山清理专家等，这里以使用简单易用的 360 安全卫士为例进行介绍，具体的操作步骤如下。

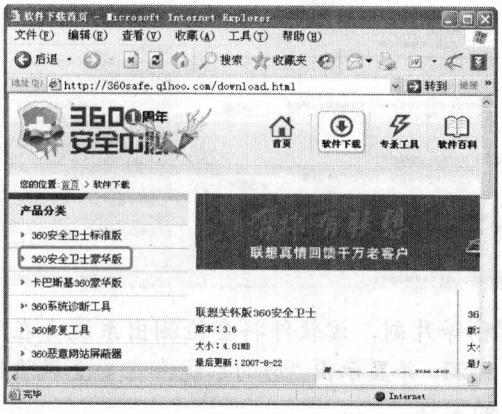
1 打开 IE 浏览器，在地址栏中输入“www.360safe.com”，然后单击 转到 按钮。



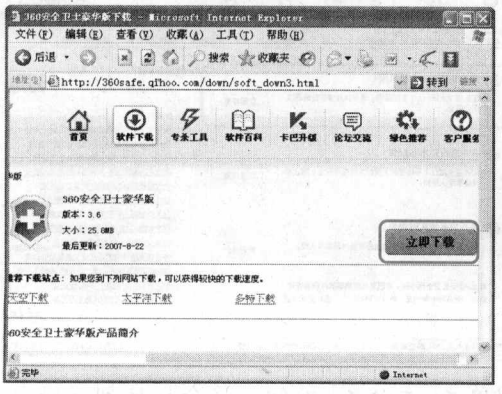
②稍等片刻即可进入 360 安全卫士的官方页面，然后单击【软件下载】按钮。



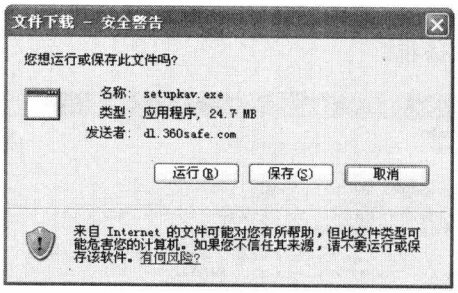
③随即弹出该软件的下载链接页面，用户可以看到在左侧的窗格中列出了好多种产品，这里单击【360 安全卫士豪华版】链接。



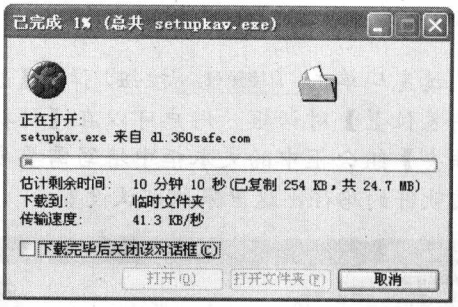
④随即弹出【360 安全卫士豪华版下载】页面。



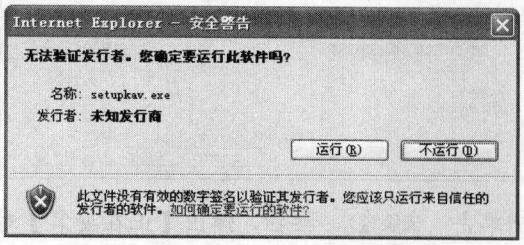
⑤单击 立即下载 按钮，弹出【文件下载 - 安全警告】对话框。



⑥单击 运行(R) 按钮进入自动下载软件的过程，并显示出下载进度。



⑦稍等片刻即可下载完毕，弹出【Internet Explorer – 安全警告】对话框。



⑧单击 运行(R) 按钮，弹出【卡巴 360 安装】对话框。