

操作
讲解

技能
实训

实用
技巧

※ 内容全面 案例实用 ※

本书在内容上分为
“操作讲解、技能实训、实用技巧”三部分，
充分满足读者各种需求，
读者可以根据实际情况安排学习顺序，或选择性查阅。

在操作讲解部分，讲述了最基础的知识，
由浅入深让读者全面掌握电脑安全与黑客攻防；
在技能实训部分，精选了实际工作和应用中的典型实例，
让读者在学会理论知识的同时迅速掌握实际技能；

在实用技巧部分，汇总了
日常工作、生活中常见的问题和疑难杂症，
帮助读者有针对性地解决问题。

※ 讲解清晰 视频教学 ※

本书采用“步骤+图解”的方式进行编写，
操作简单明了，浅显易懂。
读者只要按书中的“图解步骤”一步一步地操作，
就可以掌握电脑安全与黑客攻防。
本书配1CD多媒体教学光盘，
帮助您更轻松地学习。

(超值升级版)

从入门到精通

前沿文化 ※ 编著

电脑安全与黑客攻防

多媒体教学光盘

- ☑ 78段教学视频
- ☑ 90分钟播放时间
- ☑ 附赠《电脑维护与故障排除》教学视频
- ☑ 附赠《系统安装与重装》教学视频



电脑安全与黑客攻防

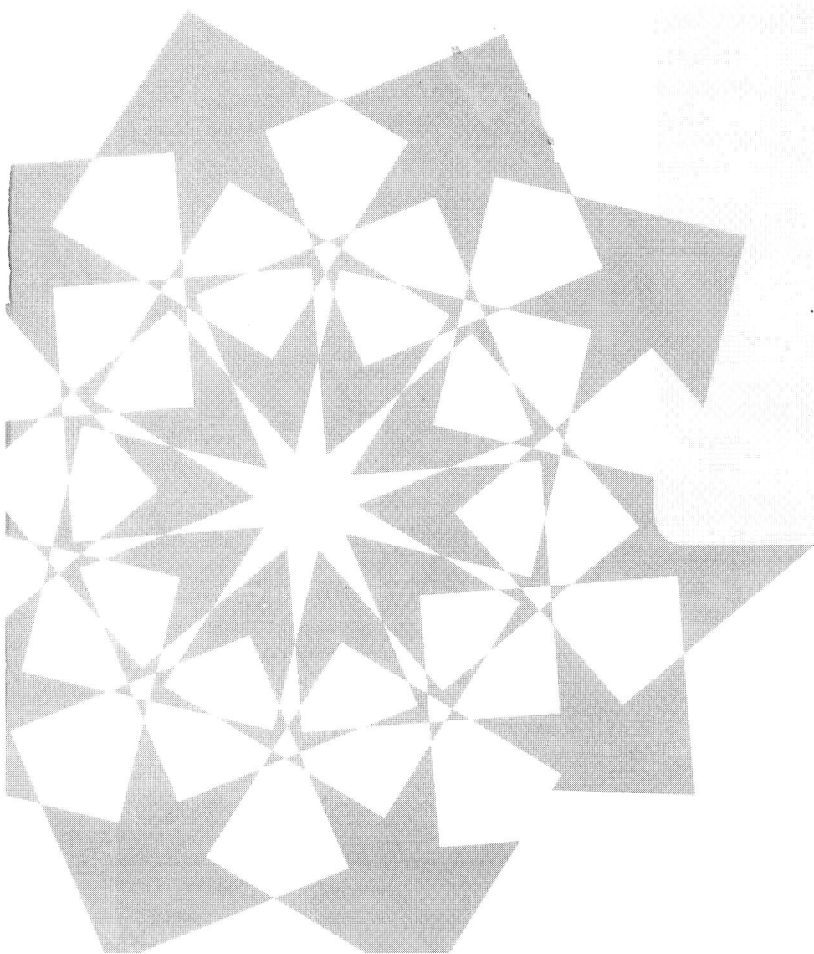
从入门到精通

(超值升级版)

TP393.08
675

前沿文化*编著

科学出版社
北京



内 容 简 介

《电脑安全与黑客攻防从入门到精通（超值升级版）》针对初学者的需求，全面、详细地讲解了电脑安全与黑客攻防的具体操作方法、疑难问题与实用技巧。本书在讲解上图文并茂，重视操作技巧的传授，在图片中清晰地标注出要进行操作的位置与操作内容，并对重点、难点操作均配有视频教程，以求读者能高效、完整地掌握本书内容。

本书共 20 章，分为两部分。第 1~10 章为操作讲解部分，详细讲解了电脑安全基础知识、电脑病毒、黑客与木马、修补 Windows 系统、注册表安全、Windows 操作系统的安全防护、网络攻击基础、远程搜集电脑信息、远程入侵、木马病毒等内容；第 11~20 章为进阶技巧部分，汇集了电脑安全与黑客攻防的典型问题和实用技巧，有利于读者提高操作技能，包含通信安全、加密与解密、网页安全、打击非法扫描与恶意软件、无线网络安全、数据保护、数据拯救、增强系统安全性、系统安全限制与隐私保护、办公文档与文件夹安全等 10 大类技巧。

本书在各章最后设置了大量实训，内容全部来自于实际工作与生活中，对读者进行针对性训练，务必使读者“不仅学会相关知识，更要学会如何解决实际问题”。本书配 1CD 多媒体教学光盘，包含 78 个重点实例的视频教学录像，播放时间达 90 分钟。此外，为了让您能够掌握更多的知识，特贴心赠送畅销图书《电脑维护与故障排除》和《系统安装与重装》的视频教程。

本书适合想要学习电脑安全与黑客攻防的读者使用。

图书在版编目（CIP）数据

电脑安全与黑客攻防从入门到精通：超值升级版/前沿文化

编著. —北京：科学出版社，2013. 1

ISBN 978-7-03-036343-5

I. ①电… II. ①前… III. ①电子计算机—安全技术
②计算机网络—安全技术 IV. ①TP309

中国版本图书馆 CIP 数据核字（2012）第 312156 号

责任编辑：周晓娟 陈 洁 / 责任校对：刘雪连

责任印刷：华 程 / 封面设计：彭琳君

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

<http://www.sciencep.com>

北京市艺辉印刷有限公司印刷

中国科技出版传媒股份有限公司新世纪书局发行 各地新华书店经销

*

2013 年 5 月第 一 版

开本：16 开

2013 年 5 月第一次印刷

印张：25.25

字数：614 000

定价：45.00 元（含 1CD 价格）

（如有印装质量问题，我社负责调换）

前言



为什么编写本书

随着电脑与互联网的发展,信息安全与网络安全逐渐成为人们日益关注的一个重要课题。本书从电脑安全与黑客攻防基础知识和基本操作入手,结合大量实例,采用知识点讲解与动手练习相结合的方式,详细介绍了电脑安全与黑客攻防的应用方法。



本书特色

全书拒绝单纯讲解软件,注重培养实际应用能力,内容由浅入深,文字通俗易懂,实例丰富实用,对每个操作步骤的介绍都清晰准确,读者学习起来更加轻松、快捷。

内容全面 本书在内容上分为“操作讲解、技能实训、实用技巧”三部分,充分满足读者各种需求,读者可以根据实际情况安排学习顺序,或选择性查阅,真正做到“一书在手、问题不愁”(具体请参见下页的“阅读帮助”)。

讲解清晰 本书采用“步骤+图解”的方式进行编写,操作简单明了,浅显易懂。读者只要按书中的“图解步骤”一步一步地操作,就可以掌握电脑安全与黑客攻防,本书还配有“提个醒”、“一点通”等小贴士,使读者能在轻松掌握相关内容的同时,将所学习到的知识应用到实际操作中(具体请参见下页的“阅读帮助”)。

视频教学 本书配1CD多媒体教学光盘,包含了78个重点实例的视频教学录像,播放时间达90分钟。此外,为了让您能够掌握更多的知识,特贴心赠送畅销图书《电脑维护与故障排除》和《系统安装与重装》的视频教程(具体请参见下页的“光盘使用说明”)。



您是否适合使用本书

如果您符合以下情况,建议您购买本书进行学习。

- 对电脑安全与黑客攻防不太熟悉,需要掌握相关知识、具体操作步骤的读者。
- 对电脑安全与黑客攻防能进行一定的基础操作,但对于工作中各类实际问题不知道该如何实现的读者。
- 对电脑安全与黑客攻防具有一定应用水平,但需要更多技巧来提高工作效率,或需要招数来解决各种疑难杂症的读者。



作者致谢

本书由前沿文化工作室负责全书的编写和校对工作。热切期盼广大读者对本书提出宝贵意见。

编著者

2013年1月

阅读帮助



三大内容

操作讲解 11.5.1，讲述了最基础的知识，由浅入深让读者全面掌握电脑安全与黑客攻防，建议按照顺序学习。

技能实训 实训一，精选了实际工作和应用中的典型实例，让读者在学会理论知识的同时迅速掌握实际技能，建议初学者按照顺序学习，中高级读者可以直接学习这部分内容。

实用技巧 002，汇总了日常工作、生活中常见的问题和疑难杂症，帮助读者有针对性地解决问题，在正常学习之余，还可作为查询手册使用。



光盘路径

此处注明了接下来的讲解中所涉及的视频教学文件在配套光盘中的位置。

电脑安全与黑客攻防从入门到精通（超值升级版）

11.5 Email攻击与防范

电子邮箱从来就是黑客攻击的重要目标之一。除了前面提到的密码破解以外，还有一些其他破坏性手段，如发送邮箱炸弹让对方邮箱失去作用，或往对方邮箱里发送病毒木马等程序，以图破坏对方电脑系统。

11.5.1 使用邮箱炸弹进行攻击

所谓的邮箱炸弹，是利用工具软件向一个邮箱中发送大量无用信件，该邮箱接收的信件达到容量上限后，就再也不接受新的邮件了，这样会导致该邮箱暂时失去收信功能，轰炸者的目的也就达到了。

11.5.2 对付邮箱攻击的方法

要对付邮箱攻击，最好的方法就是不暴露自己的邮箱地址，因此不要在论坛、聊天室等公共场合发布自己的邮箱地址。

电子邮箱一般都具有垃圾邮件过滤功能，善用这些功能可以减少受攻击的可能。先看看如何在Web邮箱中设置垃圾邮件过滤功能。这里以TOM邮箱为例进行讲解。



技能实训

增强动手能力

通过前面内容的学习，为了巩固读者所学的相关知识，下面安排实训任务来增强动手能力和技能的综合应用水平。

实训一 使用代理服务器隐藏QQ真实IP

前面介绍了两种减少被别人通过QQ探测到自己IP地址的可能性的方法，但这两种方法并不能完全杜绝探测。要完全不被人发现自己的真实IP地址，可以通过代理服务器来实现。QQ通过代理服务器上线之后，所有的消息都会从代理服务器中转一次，这样即使被人探测，泄露的也只是代理服务器的IP地址，而自己的真实地址对方是探测不到的。



光盘同步文件

同步视频文件

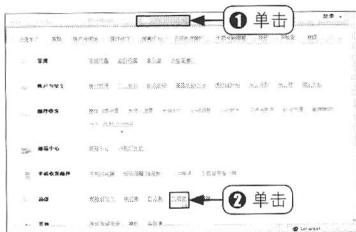
光盘\同步教学文件\第11章\技能实训1.mp4

QQ2012支持两种代理方式：http和socket。这两种代理在技术上不太相同，功能和作用差异也较大，不过，在QQ里设置的差别倒是不大。这里以http代理为例进行讲解，其具体方法如下。

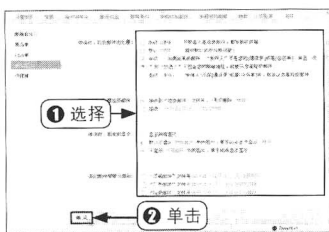


本书在内容上分为“操作讲解、技能实训、实用技巧”三部分，充分满足读者各种需求，可以根据自己的实际情况安排学习顺序，或选择性查阅，真正做到“一书在手、问题不愁”。本书在讲解上采用了全新的图解写作方式，特在此处进行简要说明。

STEP 01 进入邮箱，**①**单击“设置”连接：
②单击“反垃圾”链接，如下图所示。



STEP 02 **①**根据需要选择反垃圾选项；**②**单击“确定”按钮保存设置，如下图所示。



操作步骤

讲解了具体的操作步骤，要按照**STEP 01**、**STEP 02**的顺序进行操作；步骤中的**① ②**与图中的标注相对应，真正做到图文对照，让读者绝对不会找错位置。



一点通 http和socket的区别

简单地说，http代理主要用于网页浏览，限制较多，对速度的要求也不高；而socket代理则是一种“全能”代理，很多应用都可以通过它中转，比如telnet和各种游戏等。由于QQ对速度要求也不高，因此无论使用哪种代理都不影响聊天。



一点通

讲解一些提高性的知识与技巧。

002 为账号添加登录密码

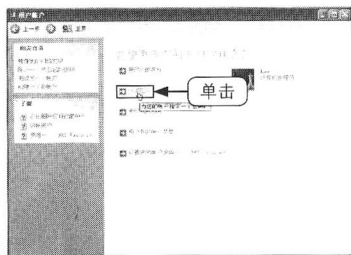
很多用户在安装Windows的时候，觉得直接登录操作系统很方便，殊不知没有密码的账号会带来很多不安全因素，任何人都可以直接进入操作系统，查看、复制或删除文件。

STEP 01 打开控制面板，双击“用户账户”图标。

STEP 02 单击要设置密码的账户，如下图所示。



STEP 03 单击“创建密码”文字链接，如下图所示。



提个醒 其他打开本地安全策略的方法

单击“开始”按钮，选择“运行”命令，在弹出的对话框中输入“secpol.msc”并按回车键，也可以打开本地安全策略窗口。



提个醒

主要指出初学者经常犯的错误或者需要重点注意的问题。

How to Use the CD-ROM

光盘使用说明



光盘使用方法

1. 将本书的配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如图1所示。
2. 单击光盘主界面上方的“多媒体视频教学”按钮，可显示“目录浏览区”和“视频播放区”，如图2所示。在“目录浏览区”中有以章序号顺序排列的按钮，单击按钮，将在下方显示以节标题命名的该章所有视频文件的链接。单击链接，对应的视频文件将在“视频播放区”中播放。
3. 单击光盘主界面上方的“超值附赠”按钮，可以看到本书附赠的视频教程和实用模板，有助于读者扩展能力。



图1 光盘主界面



提示

如果光盘没有自动运行，Windows XP用户只需在“我的电脑”窗口中双击光驱盘符进入配套光盘，然后双击 start.exe 文件即可（Windows 7 用户需打开“计算机”窗口，双击光驱盘符）。在播放视频前，请先安装视频插件，在图1中单击“视频播放插件安装”按钮即可。

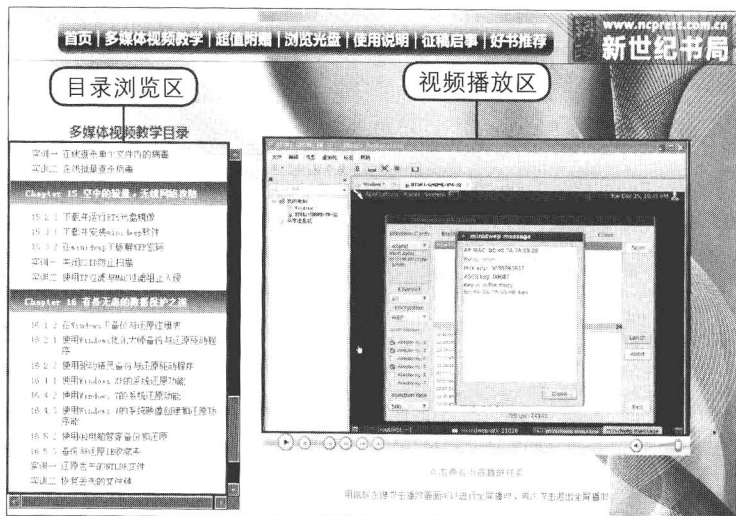


图2 视频播放界面



本书配套的多媒体教学光盘内容包含了78个重点实例的视频教学录像，播放时间达90分钟。此外，特贴心赠送畅销图书《电脑维护与故障排除》和《系统安装与重装》的视频教程。

目录浏览区和视频播放区

“目录浏览区”是书中所有视频教程的目录，“视频播放区”是播放视频文件的窗口，在“目录浏览区”中有以章序号顺序排列的按钮，单击按钮将在下方显示该章以小节标题命名的所有视频文件的链接，如图2所示。单击选择要学习的内容，对应的视频文件将在“视频播放区”中播放。

单击“视频播放区”中控制条上的按钮可以控制视频的播放，如暂停、快进；双击播放画面可以全屏播放视频，如图3所示；再次双击全屏播放的视频可以回到如图2所示的播放模式。

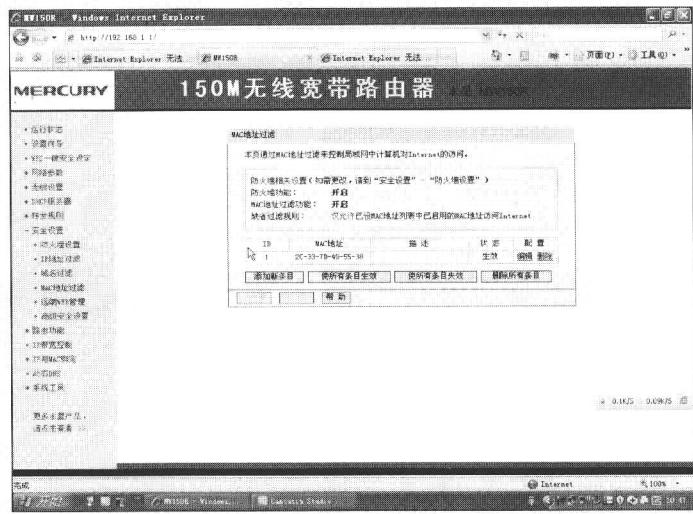


图3 全屏播放的视频文件

浏览其他内容

通过单击导航菜单（见图4）中不同的项目按钮，可浏览光盘中的其他内容。

- 单击“浏览光盘”按钮，进入光盘根目录，可以看到光盘中的相关文件，如图5所示。
- 单击“使用说明”按钮，可以查看使用光盘的设备要求及使用方法。
- 单击“征稿启事”按钮，有合作意向的作者可与本社取得联系。
- 单击“好书推荐”按钮，可以看到本社近期出版的畅销书。



图4 导航菜单

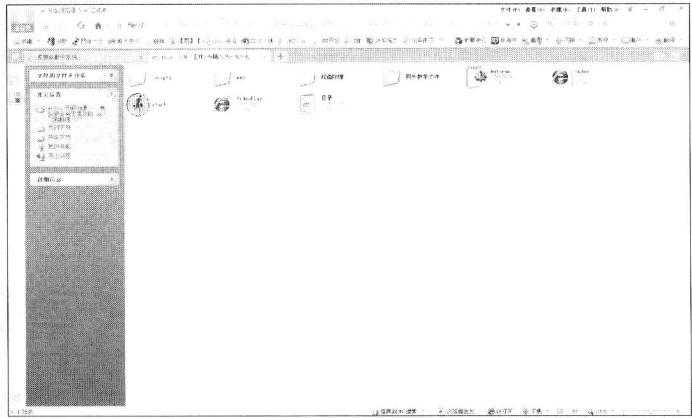


图5 查看光盘中的文件

CONTENTS

目 录

此图标代表该章节下有视频教学录像

► Chapter 01 谁动了我的电脑

1.1 电脑安全是什么002

1.1.1 电脑怎样才能安全002

1.1.2 什么是本地安全002

1.1.3 网络安全是重点003

1.2 网络安全ABC004

1.2.1 网络安全的四个方面004

1.2.2 常见的网络攻防手段006

1.3 什么在影响网络安全007

1.3.1 由网络本身带来的问题007

1.3.2 来自网络外部的安全威胁008

1.3.3 网络安全面临威胁的原因011

1.4 网络安全的现状和发展趋势012

1.4.1 网络安全的现状012

1.4.2 网络安全的发展趋势013

► Chapter 02 探秘电脑病毒

2.1 电脑病毒初接触016

2.1.1 电脑病毒追根溯源016

2.1.2 电脑病毒的发展历程016

2.1.3 如何定义电脑病毒020

2.1.4 详解电脑病毒的分类021

2.1.5 电脑病毒的命名方法023

2.1.6 剖析电脑病毒的结构024

2.2 电脑病毒不过如此027

2.2.1 电脑病毒有哪些表现027

2.2.2 电脑病毒有什么特征028

2.2.3 如何预防电脑病毒029

2.3 电脑病毒的类型031

2.3.1 文件型病毒031

2.3.2 引导型病毒032

2.3.3 宏病毒032

2.3.4 蠕虫病毒034

► Chapter 03 黑客与木马，西门吹雪与剑

3.1 不可不知的黑客历史037

3.1.1 黑客的由来037

3.1.2 黑客？骇客？038

3.1.3 黑客活动历史039

3.1.4 我国黑客发展历程041

3.2 黑客招式大曝光042

- 3.2.1 攻击目的042
- 3.2.2 攻击分类042

3.3 希腊美女与木马044

- 3.3.1 木马背景介绍044
- 3.3.2 什么是电脑木马045

- 3.3.3 木马的类型048

- 3.3.4 木马的发展历程050

3.4 木马应用，一点也不神秘051

- 3.4.1 经典木马介绍051
- 3.4.2 木马的加壳与脱壳053
- 3.4.3 木马的防范原则054

Chapter 04 修补浑身是洞的Windows系统

4.1 Windows系统是出了名的漏洞多057

- 4.1.1 Windows系统漏洞产生的原因057
- 4.1.2 Windows系统中的安全隐患058

4.2 详解Windows系统中的漏洞061

- 4.2.1 UPNP服务漏洞061
- 4.2.2 升级程序漏洞061
- 4.2.3 帮助和支持中心漏洞062
- 4.2.4 Windows Media Player漏洞062
- 4.2.5 压缩文件夹漏洞063
- 4.2.6 服务拒绝漏洞063
- 4.2.7 RDP漏洞063
- 4.2.8 VM漏洞064
- 4.2.9 热键漏洞064
- 4.2.10 账号快速切换漏洞064
- 4.2.11 输入法漏洞065
- 4.2.12 Unicode漏洞065
- 4.2.13 ISAPI缓冲区扩展溢出漏洞066
- 4.2.14 MS SQL Server的SA空密码漏洞066
- 4.2.15 系统管理权限漏洞066
- 4.2.16 路径优先漏洞067
- 4.2.17 NetDDE消息权限提升漏洞067

- 4.2.18 RDP拒绝服务漏洞068
- 4.2.19 域控制器拒绝服务漏洞068
- 4.2.20 事件查看器存在缓冲区溢出漏洞068
- 4.2.21 UDP套接字拒绝服务漏洞069
- 4.2.22 安全账户管理漏洞069
- 4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞069
- 4.2.24 IIS 5.0的ASP缓冲溢出漏洞070
- 4.2.25 Narrator本地密码信息泄露漏洞070
- 4.2.26 SMTP认证漏洞070
- 4.2.27 IIS 5.0/5.1验证漏洞070
- 4.2.28 SQL Server函数库漏洞071
- 4.2.29 IIS 5.0伪造拒绝服务漏洞071
- 4.2.30 调试寄存器漏洞071
- 4.2.31 drwtsn32.exe文件漏洞071
- 4.2.32 快捷方式漏洞072
- 4.2.33 UTF漏洞072
- 4.2.34 IIS 5.0 SEARCH方法远程攻击漏洞073
- 4.2.35 Telnet漏洞073
- 4.2.36 LDAP漏洞074
- 4.2.37 IIS 5.0拒绝服务漏洞074
- 4.2.38 默认注册许可漏洞074

4.2.39 登录服务恢复模式空密码漏洞·····	075
4.2.40 域账号锁定漏洞·····	075
4.2.41 终端服务器登录缓存溢出漏洞·····	075
4.2.42 ActiveX参数漏洞·····	075
4.2.43 IIS 5.0 Cross-Site Scripting 漏洞·····	076
4.2.44 组策略漏洞·····	076
4.2.45 数字签名缓冲区溢出漏洞·····	076

4.3 Windows漏洞入侵揭秘·····077

4.3.1 数据驱动攻击·····	077
4.3.2 伪造信息攻击·····	077
4.3.3 针对信息协议弱点攻击·····	077
4.3.4 登录欺骗·····	077
4.3.5 利用系统管理员失误攻击·····	077
4.3.6 重新发送（REPLAY）攻击·····	077
4.3.7 对ICMP报文进行攻击·····	078

4.3.8 针对源路径选项的弱点攻击·····	078
4.3.9 以太网广播攻击·····	078

4.4 回春妙手来堵漏·····078

4.4.1 杀毒软件不可少·····	078
4.4.2 个人防火墙不可替代·····	079
4.4.3 分类设置复杂密码·····	079
4.4.4 防止网络病毒与木马·····	079
4.4.5 警惕“网络钓鱼”·····	080
4.4.6 防范间谍软件·····	080
4.4.7 只在必要时共享文件夹·····	080
4.4.8 定期备份重要数据·····	080

技能实训 增强动手能力·····081

- 实训一 使用代码检测杀毒软件是否
正常工作·····081
- 实训二 添加与撤销文件夹及驱动器共享·····082

► Chapter 05 注册表的安全不可忽视

5.1 神马是注册表·····085

5.1.1 注册表的由来·····	085
5.1.2 了解注册表的结构与数据形式·····	086
5.1.3 熟悉注册表各分支·····	086
● 5.1.4 如何操作注册表·····	088

5.2 通过注册表进行系统 安全设置·····091

5.2.1 使用注册表进行系统安全设置·····	091
5.2.2 使用注册表进行网络安全设置·····	095

5.3 注册表的安全管理·····098

● 5.3.1 限制本地访问注册表·····	098
------------------------	-----

5.3.2 限制远程访问注册表·····	100
----------------------	-----

5.4 严查注册表启动项·····100

5.4.1 Load值项·····	101
5.4.2 Userinit值项·····	101
5.4.3 RunOnce子键·····	101
5.4.4 Installed Components子键·····	102
5.4.5 BootExecute值项·····	102

技能实训 增强动手能力·····102

- 实训一 使用注册表隐藏驱动器·····102
- 实训二 解决不能导入注册表文件的
问题·····103

► Chapter 06 为Windows系统筑起铜墙铁壁

6.1 组策略研究 106

- 6.1.1 认识组策略 106
- 6.1.2 开机策略 108
- 6.1.3 安全设置 111

6.2 活用本地安全策略 114

- 6.2.1 审核策略 114
- 6.2.2 系统安全管理 116

6.3 计算机管理三招 118

- 6.3.1 使用事件查看器 118
- 6.3.2 管理共享内容 123
- 6.3.3 性能日志和警报 125

技能实训 增强动手能力 127

- 实训一 检查并修复Windows系统文件 127
- 实训二 隐藏共享文件夹 128

► Chapter 07 网络攻击基本功

7.1 电脑的地址——IP和域名 131

- 7.1.1 什么是IP地址 131
- 7.1.2 IP地址的划分 131
- 7.1.3 分配IP的机构 133
- 7.1.4 公有IP与私有IP地址 133
- 7.1.5 什么是域名 133
- 7.1.6 域名的级别 134
- 7.1.7 Internet上的常见域名 134
- 7.1.8 域名与IP地址的纠葛 139

7.2 外联的通道——端口 139

- 7.2.1 端口的分类 139
- 7.2.2 查看端口 141
- 7.2.3 端口的关闭与限制 142

7.3 黑客常用命令一览 144

- 7.3.1 进入命令行窗口 145

- 7.3.2 net命令 146
- 7.3.3 远程登录命令telnet 148
- 7.3.4 文件传输命令ftp 148
- 7.3.5 添加计划任务命令at 150
- 7.3.6 查看修改文件夹权限命令cacls 150
- 7.3.7 回显命令echo 151
- 7.3.8 命令行下的注册表操作 152
- 7.3.9 查看当前系统用户情况命令query 153
- 7.3.10 终止会话命令logoff 153
- 7.3.11 物理网络查看命令ping 153
- 7.3.12 网络配置查看命令ipconfig 155
- 7.3.13 DNS查看命令nslookup 155
- 7.3.14 地址解析命令arp 155

技能实训 增强动手能力 157

- 实训一 查看QQ好友的IP地址 157
- 实训二 使用telnet命令远程访问BBS 158

► Chapter 08 悄悄搜集远程电脑的信息

8.1 轻松搜集网络中的信息162

8.1.1 获取目标电脑的IP地址及路由162

8.1.2 由IP地址获取目标电脑的地理位置... 163

8.1.3 了解网站备案信息163

8.2 检测系统漏洞也不难165

8.2.1 什么是扫描器166

8.2.2 搜索共享资源166

8.3 端口扫描速成168

8.3.1 端口扫描的原理与分类168

8.3.2 端口扫描工具X-Scan170

技能实训 增强动手能力 172

实训一 防止某些软件偷偷扫描并上传
用户信息 172

实训二 保护好端口，防止被扫描 174

► Chapter 09 远程入侵不可怕

9.1 深入学习基于认证的入侵...177

9.1.1 IPC\$入侵177

9.1.2 telnet入侵182

9.1.3 防范IPC\$连接入侵187

9.2.2 连接远程注册表190

9.2.3 通过注册表开启终端服务191

9.2 如何利用注册表入侵188

9.2.1 开启远程注册表服务189

9.3 深度解析常见问题192

技能实训 增强动手能力 193

实训一 设置本地安全策略防范IPC\$入侵... 193

实训二 设置注册表防范IPC\$入侵 194

► Chapter 10 骑着“木马”逛网络

10.1 深入了解木马197

10.1.1 木马常用的入侵手法197

10.1.2 深入了解木马的伪装手段198

10.1.3 识别木马有招数200

10.1.4 防范木马的入侵200

10.2.1 使用Exebinder捆绑木马202

10.2.2 经典木马“冰河”的使用方法...204

技能实训 增强动手能力 207

实训一 动手制作图片木马 208

实训二 在局域网外控制局域网内的
电脑 210

10.2 木马的捆绑与使用202

► Chapter 11 通信中请勿干扰

11.1 远程狙击QQ.....213

11.1.1 强制与对方聊天.....213

11.1.2 使用“QQ狙击手IpSniper”
进行IP探测.....214

● 11.1.3 使用QQ炸弹攻击器进行
信息轰炸.....214

11.2 QQ阵地战.....215

11.2.1 使用QQ聊天记录器记录
聊天内容.....215

11.2.2 强行查看本地QQ聊天记录.....217

11.2.3 破解本地QQ密码.....217

11.3 QQ防御术.....218

11.3.1 防止QQ密码被破解.....218

11.3.2 防范IP地址被探测.....220

11.3.3 防范QQ炸弹和木马.....220

11.4 Email密码偷天换日.....221

● 11.4.1 使用流光软件探测Email账号
与密码.....221

11.4.2 使用溯雪软件获取Email密码.....225

11.4.3 大批量获取邮箱地址.....227

11.4.4 对付密码探测的方法.....228

11.5 Email攻击与防范.....230

11.5.1 使用邮箱炸弹进行攻击.....231

● 11.5.2 对付邮箱攻击的方法.....231

技能实训 增强动手能力.....233

● 实训一 使用代理服务器隐藏QQ真实IP.....233

● 实训二 使用转信功能保护重要邮箱.....234

► Chapter 12 加密与解密的缠绵

12.1 加密技术的由来.....237

12.1.1 什么是加密技术.....237

12.1.2 加密技术分类.....237

12.1.3 常见的加密算法.....239

12.2 加密快速上手.....240

● 12.2.1 为Office文档加密.....240

● 12.2.2 使用文件夹加密精灵加密
文件夹.....240

● 12.2.3 使用金锋文件加密器加密文件.....242

● 12.2.4 使用WinRAR加密压缩文件.....243

12.3 密码破解有妙招.....245

● 12.3.1 破解Word文档密码.....245

● 12.3.2 破解WinRAR文件的密码.....246

技能实训 增强动手能力.....247

● 实训一 破解CMOS密码.....247

实训二 破解Windows启动密码.....248

► Chapter 13 网页有玄机

13.1 深入了解恶意代码·····251

- 13.1.1 恶意代码的特征·····251
- 13.1.2 非过滤性病毒·····251
- 13.1.3 恶意代码的传播方式·····252
- 13.1.4 恶意代码的传播趋势·····253

13.2 阻止恶意代码对注册表的侵袭·····254

- 13.2.1 开机后自动弹出网页·····254
- 13.2.2 浏览网页注册表被禁用·····254
- 13.2.3 IE默认首页被强行修改·····254
- 13.2.4 默认的微软主页被修改·····255
- 13.2.5 主页设置被屏蔽锁定，且设置选项无效不可更改·····255
- 13.2.6 默认的IE搜索引擎被修改·····255
- 13.2.7 IE标题栏被广告信息攻占·····256
- 13.2.8 Outlook标题栏被添加广告信息·····256
- 13.2.9 IE右键菜单被添加非法网站链接·····256

- 13.2.10 鼠标右键弹出菜单功能被禁用·····257
- 13.2.11 锁定地址栏的下拉菜单及其添加文字信息·····257
- 13.2.12 IE菜单“查看”下的“源文件”项被禁用·····257
- 13.2.13 系统启动时弹出对话框·····257

13.3 防范针对IE浏览器的攻击·····258

- 13.3.1 IE炸弹攻击类型、后果·····258
- 13.3.2 对IE炸弹的防范与补救·····258

13.4 网页攻防舞台剧·····260

- 13.4.1 常见ASP脚本攻击与防范·····260
- 13.4.2 跨站攻击和防范·····260

技能实训 增强动手能力·····262

- 实训一 默认IE搜索引擎被修改后的解决方法·····262
- 实训二 降权运行IE以增加安全性·····263

► Chapter 14 打击非法扫描与恶意软件

14.1 保护好自己的IP和端口·····267

- 14.1.1 设置代理服务器·····267
- 14.1.2 关闭端口·····268
- 14.1.3 配置安全策略保护端口·····269

14.2 毫不留情清除间谍软件·····274

- 14.2.1 使用Adaware驱逐恶意广告软件·····274
- 14.2.2 使用安博士驱逐恶意广告软件·····276

14.3 绝不手软清除木马·····276

- 14.3.1 使用Windows任务管理器管理进程·····276
- 14.3.2 使用TrojanRemover清除木马·····278
- 14.3.3 使用Unlocker删除顽固木马文件·····280
- 14.3.4 使用360安全卫士维护系统安全·····280

技能实训 增强动手能力·····282

- 实训一 在线查杀单个文件内的病毒·····282
- 实训二 在线批量查杀病毒·····283

► Chapter 15 空中的较量，无线网络攻防

15.1 永不消逝的电波 286

- 15.1.1 无线网络的常用术语 286
- 15.1.2 无线网络的运作原理 287
- 15.1.3 无线网络的硬件设备 287
- 15.1.4 认识WEP加密 288
- 15.1.5 认识WPA和WPA2加密 289

15.2 搭建测试环境 290

- 15.2.1 测试环境所需硬件 290
- 15.2.2 下载并安装虚拟机软件VMware 291

- 15.2.3 下载并运行BT5光盘镜像 292

15.3 Wi-Fi攻防入手 294

- 15.3.1 下载并安装minidwep软件 294
- 15.3.2 在minidwep下破解WEP密码 297

技能实训 增强动手能力 298

- 实训一 关闭SSID防止扫描 298
- 实训二 使用IP过滤与MAC过滤
阻止入侵 300

► Chapter 16 有备无患的数据保护之道

16.1 备份与还原系统注册表 303

- 16.1.1 在DOS下备份与还原注册表 303
- 16.1.2 在Windows下备份与还原
注册表 304

16.2 备份与还原驱动程序 306

- 16.2.1 使用Windows优化大师备份与
还原驱动程序 306
- 16.2.2 使用驱动精灵备份与还原
驱动程序 307

16.3 其他系统信息的备份 与还原 308

- 16.3.1 学用“备份与还原”功能 308
- 16.3.2 输入法自定义词组的备份
与还原 314
- 16.3.3 磁盘分区表的备份与还原 314

16.4 使用系统自带软件进行 备份和还原 315

- 16.4.1 使用Windows XP的系统还原功能 315
- 16.4.2 使用Windows 7的系统还原功能 317
- 16.4.3 使用Windows 7的系统映像创建
和还原功能 319

16.5 使用专业软件备份和 还原系统 322

- 16.5.1 使用GHOST软件进行备份
和还原 322
- 16.5.2 使用QQ电脑管家备份和还原 325
- 16.5.3 备份与还原IE收藏夹 327

技能实训 增强动手能力 329

- 实训一 还原丢失的NTLDR文件 329
- 实训二 恢复丢失的文件簇 330

► Chapter 17 拿什么来拯救你，我的数据

17.1 硬盘数据的生存之道 333

- 17.1.1 亡羊补牢不如未雨绸缪 333
- 17.1.2 正确安全使用移动存储设备以避免损坏数据 333
- 17.1.3 硬盘损坏的主要原因 333
- 17.1.4 警惕数据安全危机的前兆 334
- 17.1.5 电脑的良好工作环境 335

17.2 拯救硬盘中的数据 336

- 17.2.1 用EasyRecovery恢复硬盘数据 336
- 17.2.2 用FinalData恢复硬盘数据 341

技能实训 增强动手能力 343

- 实训一 用Recover My Photos恢复相片 343
- 实训二 用rmfixit恢复RM/RMVB视频文件 345

► Chapter 18 增强系统安全性

18.1 系统登录与退出设置 347

- 001 禁止系统启动时使用F8键启动功能键 347
- 002 为账号添加登录密码 347
- 003 使用屏保保护电脑 348
- 004 设置系统登录密码 349
- 005 将Administrator账号改名 350
- 006 禁用来宾账户 350
- 007 登录时不显示上次登录的用户名 350
- 008 找出隐藏的超级用户 351
- 009 退出时自动清除页面文件 352

18.2 系统查看与功能限制 352

- 010 从“添加或删除程序”中查看自动更新情况 352
- 011 添加安全的例外程序通过防火墙 353
- 012 限制例外程序仅适用于内网 353
- 013 管理IE加载项 354
- 014 一次性关闭多个Internet通信 354
- 015 对“脱机文件”缓存进行加密 355

18.3 Windows安全设置 355

- 016 清理安全日志 355
- 017 关机时清空页面文件 356
- 018 关闭快速切换功能 357
- 019 修复用户损坏的配置文件 358
- 020 使用系统文件完整性检查功能 358
- 021 更改系统安装目录 359

18.4 网络诈骗防范技巧 359

- 022 不要随便打开不明链接防止被盗号 359
- 023 警惕中奖信息的诈骗 359
- 024 注意识别相似的用户名或网址 360
- 025 留神QQ好友被盗号后发来诈骗信息 360

18.5 保护账号的安全 360

- 026 如何设置QQ安全保护问题 360
- 027 如何更改QQ密码 361
- 028 通过密保问题找回被盗的QQ号 362
- 029 如何通过账号申诉找回被盗的QQ 363