

第一本根据人的思维特点设计的黑客攻防书

7天精通黑客攻防

雨辰资讯编著



权威的作者团队
国家重点网络安全团队和资深网络管理专家联手编著，
融合丰富的实战经验和优秀的管理理念



为网络从业者量身打造
以网络攻防过程为主线，通过7*24小时的学习方式，
以实用高效为原则，让读者真正做到快速上手



全图解操作，同步视频讲解
采用图解和同步多媒体相结合的教学方式，生动、直
观、全面地剖析黑客攻防过程中的各种应用技能

DVD光盘 (2.8GB)

1.45GB共36个视频演示录像

附送20多个无线网络安全工具

附送100个《7天精通网站建设实录》图书视频文件

附送网络安全等19本电子书

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

013025754

TP393.08
672

反天精通黑客攻防

雨辰资讯 编著



P
TP393.08
672



北航

C1633734

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

013052725

内 容 简 介

本书以完整的黑客攻防策略为主线,以7天为学习任务周期,将每天的学习任务分解为多个学习和上机实训项目,采用一小时掌握一项黑客技能的学习模式,具有较强的可操作性和实训性。以零基础讲解为宗旨,全面讲解了黑客基础知识、黑客侵入式攻防技巧、黑客系统核心攻防策略、黑客密码攻防策略、Web 网站攻防策略、无线网络攻防策略和手持数码设备攻防策略等知识。

随书附赠制作精良的多媒体互动教学光盘,让读者学以致用,达到最佳的学习效果。

本书不仅适合需要了解黑客攻防知识的初、中级读者学习使用,同时也可作为各类院校相关专业学生和电脑培训班学员的教材或辅导用书,同时也是广大电脑初级、中级用户,家庭电脑用户和中老年电脑爱好者的首选参考书。

图书在版编目(CIP)数据

7 天精通黑客攻防/雨辰资讯编著. — 北京:中国铁道出版社,2013.5
ISBN 978-7-113-16060-9

I. ①7… II. ①雨… 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 023157 号

书 名: 7 天精通黑客攻防
作 者: 雨辰资讯 编著

责任编辑: 刘 伟
责任印制: 赵星辰
封面设计: 多宝格

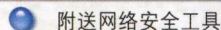
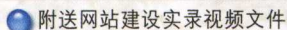
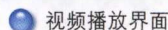
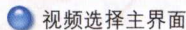
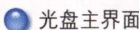
读者服务热线: 010-63560056
特邀编辑: 赵树刚

出版发行: 中国铁道出版社(北京市西城区右安门西街8号 邮政编码: 100054)
印 刷: 北京鑫正大印刷有限公司
版 次: 2013 年 5 月第 1 版 2013 年 5 月第 1 次印刷
开 本: 787mm×1092mm 1/16 印张: 29.5 字数: 584 千
书 号: ISBN 978-7-113-16060-9
定 价: 59.00 元(附赠 1DVD)

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社发行部联系调换。

100



前 言

《7天精通黑客攻防》是专门为网站建设者量身定做的学习用书,由黑客防线研究室策划,黑客攻防实训中心、雨辰资讯编著。

本书专门为研究黑客攻防学习者和爱好者打造,旨在使读者学会和用好网络黑客攻防的各项技能,保护好自己的数据和信息免受攻击。即便目前您还是初学者,在认真并系统学习本书之后,就可以骄傲地说:“我是一名网络黑客攻防专业人士!”

为什么要写这样一本书

网络安全事故的频繁发生,进一步激发了企业对网络安全防御人才的需求。据统计,黑客攻防人才是任何一个企业不可缺少的。随着网络行业的井喷式发展,黑客攻防类人才的需求量,尤其是网络安全方面的人才需求量呈直线上升。加之市场上黑客攻防实战型“后备人才”缺乏,理论知识与实践经验的脱节,恰恰是当前网络安全人员的写照。从项目实战入手,结合理论知识的讲解,便成了本书的立足点。我们的目标就是让初学者、应届毕业生、网络安全人员快速成为黑客攻防方面的专业人员,拥有较强的实战经验,在未来的职场中占有一个高起点。

本书特色

■ 零基础、入门级的讲解

无论您是否从事计算机相关行业,无论您是否接触过网络,无论您是否了解黑客攻防技术,您都能从本书中找到最佳起点。

■ 超多、实用、专业的范例和项目

本书在编排上紧密结合深入学习黑客攻防技术的先后过程,从黑客的基础知识开始,带读者逐步深入地学习各种黑客攻防技巧,侧重实战技能,抛弃晦涩难懂的技术理论,除适当的关键理论进行了简明扼要的阐述以外,绝大多数内容是基于实际案例的分析和操作指导,让读者读起来简明轻松,操作起来有章可循。

■ 随时检测自己的学习成果

每章首页均提供了学习目标,以指导读者重点学习及学后复习。

每章最后的“高手甜点”和“跟我学上机”板块均根据本章内容精选而成,读者可以随时检测自己的学习成果和实战能力,做到融会贯通。

■ 附送视频文件

光盘附赠全书中案例视频及演示文件，并超值赠送价值 1200 元的《21 天精通网站建设实录》视频，让你不但能预防黑客，更能自己搭建网站。

■ 细致入微、贴心提示

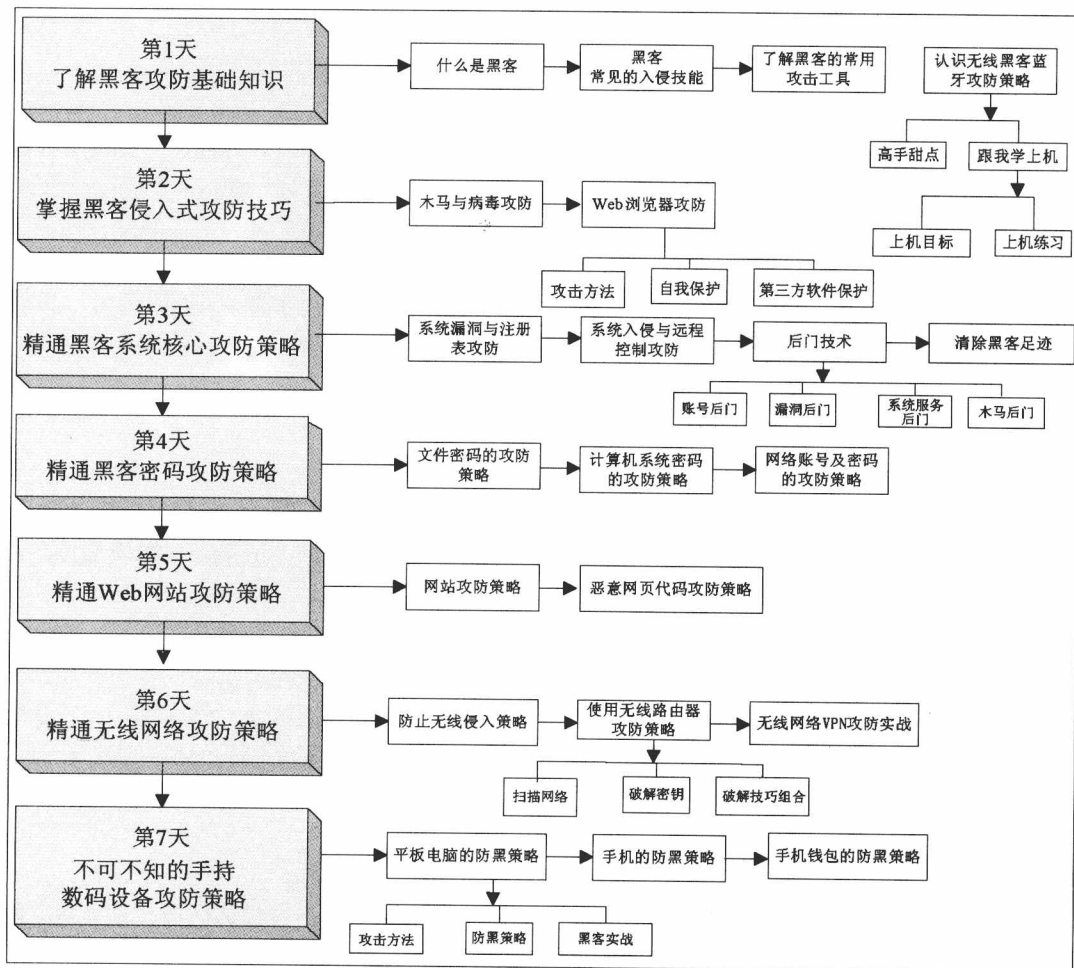
本书在讲解过程中，在各章中使用了“注意”、“提示”、“技巧”等小栏目，使读者在学习过程中更清楚地了解相关操作、理解相关概念，从而轻松掌握各种操作技巧。

■ 专业创作团队和技术支持

本书由黑客攻防实训中心、雨辰资讯编著并提供技术支持。

“黑客攻防”学习最佳途径

本书以学习“黑客攻防策略”的最佳制作流程来分配章节，从最初的学习黑客基础知识开始，然后讲解了黑客侵入式攻防策略、系统核心攻防策略、密码攻防策略、Web 网站攻防策略、无线网络攻防策略和手持数码设备攻防策略。同时在讲述中融入了很多攻防实战环节以便进一步提高大家攻防的实战技能。



读者对象

- 没有任何网络和黑客基础的初学者
- 有一定基础，想深入学习黑客攻防技能的人员
- 有一定的黑客攻防基础，没有实践经验的人员
- 大专院校及培训学校的老师和学生

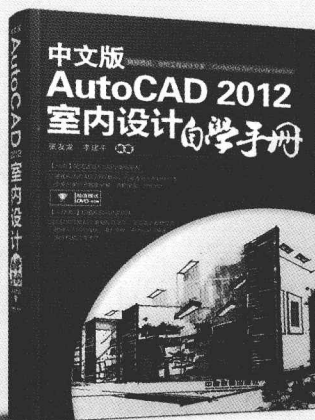
创作团队

本书由黑客防线研究室策划，黑客攻防实训中心、雨辰资讯编著，参加编写和资料收集的有孙若淞、刘玉萍、宋冰冰、张少军、王维维、肖品、周慧、刘伟、李坚明、徐明华、李欣、樊红、赵林勇、刘海松、裴东风等。

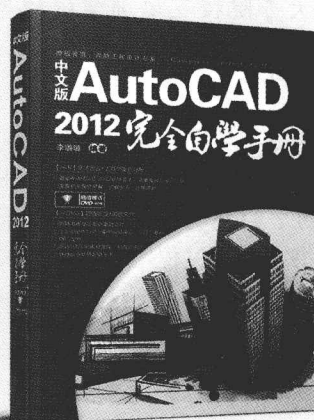
本书在编写过程中，力求将最佳的实战技巧呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有任何建议，可与我们联系，我们的电子邮箱为 6v1206@gmail.com。

编 者
2013 年 2 月

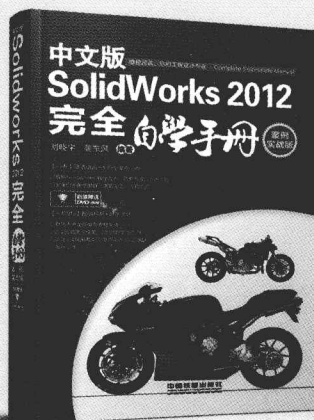
中国铁道出版社联系各行业一线工作者倾情打造入门与精通类图书，以最新国家标准为依据，以行业实操应用为主，使用最新的软件版本，现推荐如下：



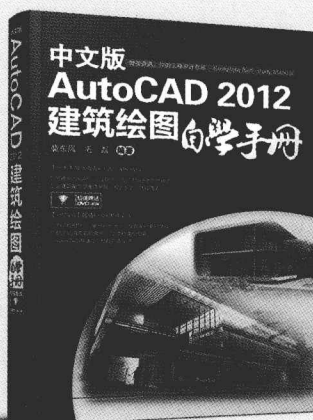
书名：中文版AutoCAD 2012室内设计自学手册
书号：ISBN 978-7-113-15001-3
定价：49.80元 编著 张有龙 李建平



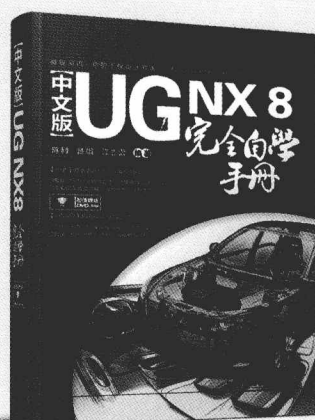
书名：15037-2 中文版AutoCAD 2012 完全自学手册
书号：ISBN 978-7-113-15037-2
定价：49.80元 编著 李璐璐



书名：中文版Solidworks 2012完全自学手册
书号：ISBN 978-7-113-15369-4
定价：49.80元 编著 刘晓宇 裴东风



书名：中文版AutoCAD 2012建筑绘图自学手册
书号：ISBN 978-7-113-15696-1
定价：49.80元 编著 裴东风 毛磊



书名：中文版UG NX 8 完全自学手册
书号：ISBN 978-7-113-14534-7
定价：49.80元 编著 陈丽 陈娟 江志磊



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

中国铁道出版社 计算机图书批销部
地址：北京市宣武区右安门西街8号
邮编：100054

网址：<http://www.tqbooks.net>
读者热线电话：(010) 63583215
销售服务电话：(010) 83550290/91

超实用！ 常识全知道！

每个人都看得懂 × 用得上 × 不求人！

编辑强烈推荐

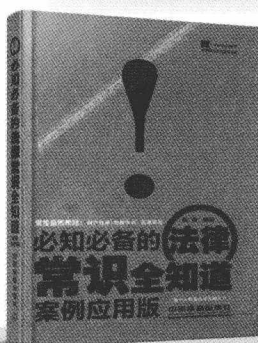
案例应用版



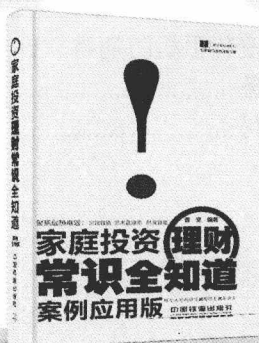
资深投资顾问卢明明多年经验全分享！
《投资理财必备的金融常识全知道（案例应用版）》
ISBN: 978-7-113-16104-0



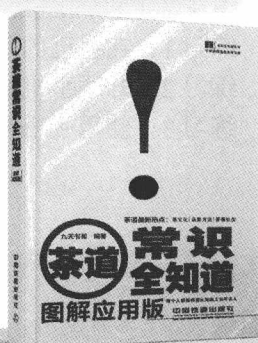
阳光保险专员韩晓辉十年心得总结！
《家庭必备的保险常识全知道（案例应用版）》
ISBN: 978-7-113-15648-0



法律顾问周舟十载从业经验指导！
《必知必备的法律常识全知道（案例应用版）》
ISBN: 978-7-113-15624-4



多位金融人士投资经验教会您理财！
《家庭投资理财常识全知道（案例应用版）》
ISBN: 978-7-113-15605-3



专家团队深入茶行打造茶事百科！
《茶道常识全知道（图解应用版）》
ISBN: 978-7-113-15914-6

- 常识全知道系列由各行业专家编写，可速查速用的家庭必备宝典！
- 删选并提炼读者最常遇到的问题，轻松严谨地做自己的顾问！



中国铁道出版社

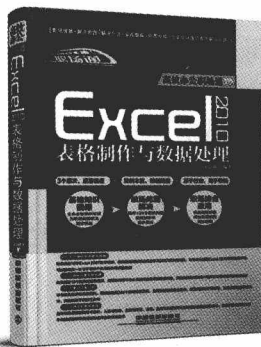
CHINA RAILWAY PUBLISHING HOUSE

地址：北京市西城区右安门西街8号
邮编：100054
网址：<http://www.tdpress.com>

高效办公职场通系列图书

职场通

《高效办公职场通》系列总共5本，本系列图书是针对实际办公环境量身打造的，其中分别涉及了办公过程中最为常用的Word、Excel和PowerPoint软件在不同方向上的应用，精选大量实战案例，全程图解，步步精讲，再配合多媒体教学和丰富的光盘配送，为读者提供最为实用的现代办公技能，提升职场效率。

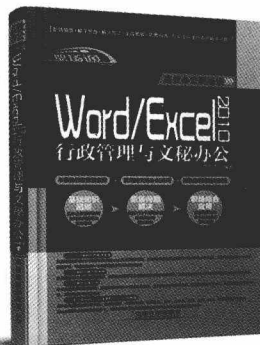


《Excel 2010表格制作与数据处理》

ISBN: 978-7-113-15112-6

作者: 杨小丽

定价: 55.00元

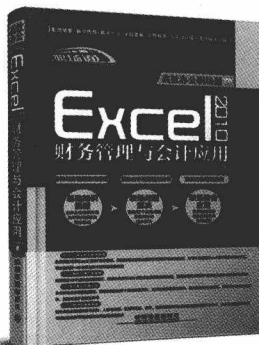


《Word/Excel 2010行政管理与文秘办公》

ISBN: 978-7-113-15321-2

作者: 李伦香

定价: 55.00元

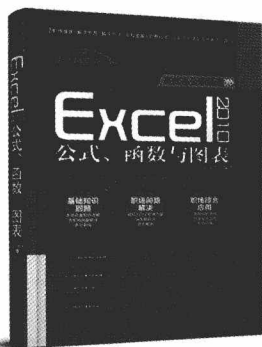


《Excel 2010财务管理与会计应用》

ISBN: 978-7-113-15113-3

作者: 高志清

定价: 55.00元

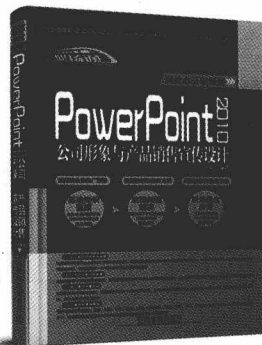


《Excel 2010公式、函数与图表》

ISBN: 978-7-113-15114-0

作者: 刘益杰

定价: 55.00元



《PowerPoint 2010企业形象与产品销售宣传设计》

ISBN: 978-7-113-15115-7

作者: 周娟

定价: 55.00元



中国铁道出版社

CHINA RAILWAY PUBLISHING HOUSE

地址: 北京市西城区右安门西街8号

邮编: 100054

网址: <http://www.tdpress.com>



北航

C1633734

第一套根据人的思维习惯，来设计学习路线的图书



权威的作者团队

国家重点网络安全团队和资深网络管理专家联手编著，融合丰富的实战经验和优秀的管理理念



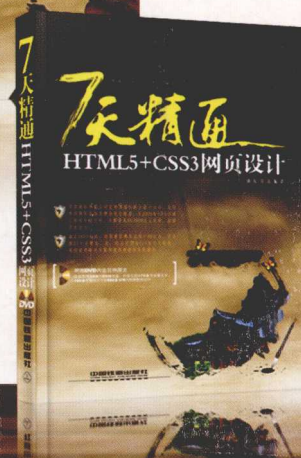
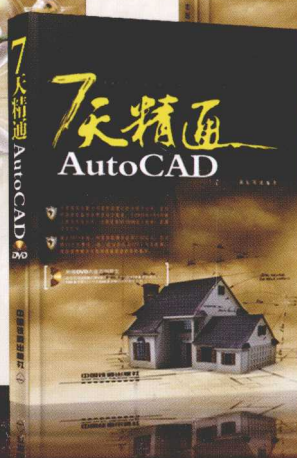
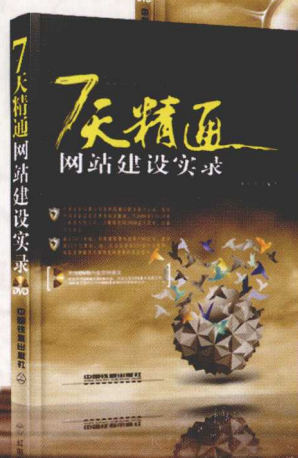
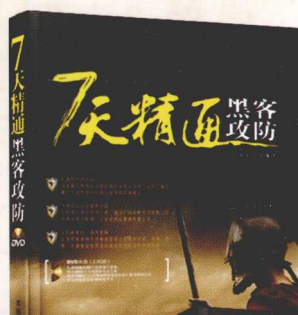
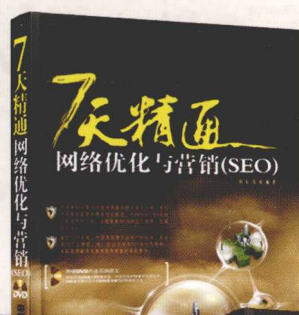
为从业者量身打造

以人的思维为主线，通过7*24小时的学习方式，以实用高效为原则，让读者真正做到快速上手



全图解操作，同步视频讲解

采用图解和同步多媒体相结合的教学方式，生动、直观、全面地剖析操作过程中的各种应用技能



想反馈，想建议或者想购买其他图书，通过以下方式联系我们！



E-mail: 6v1206@gmail.com

QQ: 17269702

微信公众账号: i6v1206或微视角或扫描左侧二维码

官方淘宝店: <http://shop63634738.taobao.com>

目 录

第 1 天 了解黑客攻防基础知识

第 1 小时 什么是黑客	3
1.1 黑客与红客	3
1.2 黑客是如何攻击计算机的	3
1.3 黑客攻击的流程	4
1.4 最近几年黑客制造的轰动性事件	5
第 2 小时 黑客常见的入侵技能	7
2.1 黑客行动的门牌号——IP 地址	7
案例 1——探知 IP 地址	8
2.2 黑客进出的门户——端口	8
2.2.1 认识 IP 地址	8
2.2.2 案例 2——查看系统的开放端口	9
2.2.3 案例 3——关闭不必要的端口	9
2.2.4 案例 4——开启端口	10
2.3 黑客常用的攻击命令	11
2.3.1 案例 5——ping 命令	11
2.3.2 案例 6——net 命令	13
2.3.3 案例 7——netstat 命令	14
2.3.4 案例 8——tracert 命令	16
2.3.5 案例 9——telnet 命令	17
2.3.6 案例 10——ftp 命令	19
2.4 高手甜点	21
2.5 跟我学上机	26
练习 1: 查询 IP 地址	26
练习 2: 查看系统开放的端口	26
练习 3: 黑客常用的攻击命令	26



--> 第3小时 了解黑客的常用攻击工具	27
3.1 目标扫描工具	27
3.1.1 案例1——端口扫描器	27
3.1.2 案例2——漏洞扫描器	31
3.1.3 案例3——Web 扫描器	35
3.2 目标攻击工具	36
3.2.1 案例4——局域网攻击工具（网络剪刀手 Netcut）	36
3.2.2 案例5——ARP 攻击工具（WinArpAttacker）	38
3.2.3 案例6——网站注入攻击工具（NBSI）	41
3.3 嗅探器工具	43
3.3.1 案例7——影音神探	43
3.3.2 案例8——SpyNet Sniffer 嗅探器	46
3.4 加壳工具	49
3.4.1 案例9——UPX 加壳工具	49
3.4.2 案例10——ASPack 加壳工具	50
3.4.3 案例11——Armadillo	51
3.4.4 案例12——ASProtect	52
3.5 脱壳工具	54
3.5.1 案例13——脱 PECompact 壳的软件	55
3.5.2 案例14——ProcDump 软件的使用	55
3.5.3 案例15——UN-PACK 软件的使用	56
3.6 高手甜点	56
3.7 跟我学上机	67
练习1：目标扫描工具的使用	67
练习2：目标攻击工具的使用	67
练习3：嗅探工具的使用	67
练习4：加壳工具的使用	67
练习5：脱壳工具的使用	67
第4小时 认识无线黑客蓝牙攻防策略	68
4.1 关于蓝牙	68
4.1.1 什么是蓝牙	68
4.1.2 蓝牙技术体系及相关术语	69
4.1.3 适配器的选择	72
4.1.4 蓝牙（驱动）工具安装	73
4.1.5 案例1——蓝牙设备配对操作	74
4.2 蓝牙基本 Hacking 技术	78
4.2.1 识别及激活蓝牙设备	78
4.2.2 查看蓝牙设备相关内容	79

4.2.3	案例 2——扫描蓝牙设备.....	80
4.2.4	蓝牙攻击技术	82
4.2.5	案例 3——修改蓝牙设备地址.....	83
4.3	蓝牙 DoS 攻击技术.....	84
4.3.1	关于蓝牙 DoS	85
4.3.2	案例 4——蓝牙 DoS 实战	85
4.4	安全防护及改进	87
4.4.1	关闭蓝牙功能	87
4.4.2	设置蓝牙设备不可见.....	87
4.4.3	限制蓝牙可见时长	88
4.4.4	升级操作系统至最新版本.....	88
4.4.5	设置高复杂度的 PIN 码	88
4.4.6	拒绝陌生蓝牙连接请求.....	88
4.4.7	拒绝可疑蓝牙匿名信件.....	88
4.4.8	启用蓝牙连接验证	88
4.5	高手甜点	89
4.6	跟我学上机	93
	练习 1: 蓝牙设备的配对操作.....	93
	练习 2: 识别并激活蓝牙设备.....	93
	练习 3: 蓝牙 DoS 攻击实战	93
	练习 4: 关闭蓝牙功能	93
	练习 5: 设置蓝牙设备的不可见.....	93

第 2 天 掌握黑客侵入式攻防技巧

第 5 小时	木马与病毒攻防	97
5.1	了解木马与病毒的真面目	97
5.1.1	什么是木马	97
5.1.2	什么是病毒	98
5.2	常见的木马攻击	98
5.2.1	案例 1——使用“黑暗天使”木马攻击.....	98
5.2.2	案例 2——使用“网络公牛”木马攻击.....	101
5.2.3	案例 3——使用“广外女生”木马攻击.....	104
5.3	木马去无踪——木马清除软件	107
5.3.1	案例 4——使用木马清除大师清除木马.....	107
5.3.2	案例 5——使用“木马克星”清除木马.....	109
5.3.3	案例 6——使用木马清除专家清除木马.....	111
5.4	常见病毒攻击	115

第 7 章 精通黑客攻防



5.4.1	Windows 系统病毒	116
5.4.2	案例 7——U 盘病毒	119
5.4.3	案例 8——邮箱病毒	121
5.5	病毒的防御	122
5.5.1	案例 9——U 盘病毒的防御	123
5.5.2	案例 10——邮箱病毒的防御	126
5.5.3	案例 11——使用软件查杀病毒	128
5.6	高手甜点	133
5.7	跟我学上机	134
	练习 1: 常见木马攻击演练	134
	练习 2: 清除木马软件的使用	134
	练习 3: 常见病毒攻击演练	134
	练习 4: 病毒的防御操作	134
第 6 小时 Web 浏览器攻防		135
6.1	常见 Web 浏览器攻防	135
6.1.1	案例 1——修改默认主页	135
6.1.2	案例 2——恶意更改浏览器标题栏	137
6.1.3	案例 3——强行修改右键菜单	138
6.1.4	案例 4——禁用 Web 浏览器的【源文件】菜单项	139
6.1.5	案例 5——强行修改浏览器的首页按钮	141
6.1.6	案例 6——删除桌面上的浏览器图标	142
6.1.7	案例 7——强行修改浏览器默认的搜索引擎	143
6.2	Web 浏览器的自我防护技巧	143
6.2.1	案例 8——限制访问不良站点	143
6.2.2	案例 9——提高 IE 的安全防护等级	144
6.2.3	案例 10——清除浏览器中的表单	145
6.2.4	案例 11——清除浏览器的上网历史痕迹	146
6.2.5	案例 12——清除浏览器的上网历史记录	146
6.2.6	案例 13——删除 Cookie 信息	147
6.2.7	案例 14——屏蔽浏览器窗口中的广告	148
6.3	使用第三方软件为 IE 浏览器保驾护航	149
6.3.1	案例 15——使用 IE 修复专家	149
6.3.2	案例 16——IE 修复免疫专家	150
6.3.3	案例 17——IE 伴侣 (IEMate)	155
6.4	其他浏览器	159
6.4.1	案例 18——火狐浏览器攻防	159
6.4.2	Safari 浏览器	162
6.4.3	Chrome 浏览器	163

6.5 高手甜点.....	163
6.6 跟我学上机.....	165
练习 1: 常见 Web 浏览器攻防	165
练习 2: Web 浏览器的自我保护技巧演练	165
练习 3: 使用软件保护 IE 浏览器.....	165
练习 4: 其他浏览器的攻防演练.....	165

第 3 天 精通黑客系统核心攻防策略

第 7 小时 系统漏洞与注册表攻防	169
7.1 什么是系统漏洞	169
7.2 系统漏洞之黑客入侵初体验	169
7.2.1 系统漏洞产生的原因.....	169
7.2.2 案例 1——X-Scan 快速抓鸡.....	170
7.2.3 案例 2——啊 D 光速抓鸡.....	172
7.3 经典系统漏洞实战之对抗管道入侵	174
7.3.1 IPC\$漏洞概述	174
7.3.2 案例 3——IPC\$漏洞入侵“挂马”	175
7.3.3 案例 4——IPC\$漏洞的防御	176
7.4 系统漏洞防御策略	177
7.4.1 案例 5——使用 Windows Update 及时为系统打补丁	177
7.4.2 案例 6——使用 360 安全卫士下载并安装补丁.....	179
7.4.3 案例 7——使用瑞星卡卡上网安全助手.....	180
7.5 常见注册表入侵方式	181
7.5.1 案例 8——连接远程注册表.....	181
7.5.2 案例 9——利用网页改写注册表.....	182
7.6 注册表的防护策略	183
7.6.1 案例 10——禁止访问和编辑注册表.....	183
7.6.2 案例 11——手工清理注册表垃圾.....	185
7.6.3 案例 12——关闭远程注册表管理服务	186
7.6.4 案例 13——设置注册表隐藏保护策略.....	187
7.7 高手甜点	188
7.8 跟我学上机	192
练习 1: 利用系统漏洞攻击目标主机.....	192
练习 2: 经典系统漏洞实战.....	192
练习 3: 系统漏洞的防御	192
练习 4: 常见注册表入侵方式.....	192
练习 5: 注册表的防护策略.....	192

第 8 小时 系统入侵与远程控制攻防	193
8.1 入侵计算机系统	193
8.1.1 案例 1——通过建立隐藏账号入侵系统	193
8.1.2 案例 2——通过开放的端口入侵系统	197
8.2 挽救被入侵的系统	199
8.2.1 案例 3——揪出黑客创建的隐藏账号	199
8.2.2 案例 4——批量关闭危险端口	200
8.3 利用系统自带的功能实现远程控制	201
8.3.1 什么是远程控制	202
8.3.2 案例 5——通过 Windows 远程桌面实现远程控制	202
8.4 经典远程控制工具——pcAnywhere	204
8.4.1 案例 6——安装 pcAnywhere	204
8.4.2 案例 7——配置 pcAnywhere	206
8.4.3 案例 8——用 pcAnywhere 进行远程控制	209
8.5 防止主机成为“肉鸡”的安全措施	212
8.5.1 案例 9——通过组策略提高系统安全	212
8.5.2 案例 10——禁用危险的系统服务	217
8.6 实时保护系统安全——360 安全卫士	218
8.6.1 案例 11——使用 360 安全卫士为电脑体检	218
8.6.2 案例 12——使用 360 安全卫士查杀木马	220
8.6.3 案例 13——使用 360 安全卫士清理插件	221
8.6.4 案例 14——使用 360 安全卫士优化加速	222
8.7 高手甜点	223
8.8 跟我学上机	227
练习 1: 入侵计算机系统	227
练习 2: 挽救被入侵的计算机系统	227
练习 3: 远程控制演练	227
练习 4: 防止主机成为“肉鸡”的演练	227
练习 5: 实时保护系统的安全	227
第 9 小时 黑客系统攻防——后门技术	228
9.1 认识后门	228
9.2 账号后门	228
9.2.1 案例 1——手动克隆账号	228
9.2.2 案例 2——在命令行方式下制作账号后门	232
9.2.3 案例 3——利用程序克隆账号	234
9.3 漏洞后门	236
9.3.1 案例 4——制造 Ubcodex 漏洞后门	236
9.3.2 案例 5——制造 idq 后门	238