

网管员书架系列

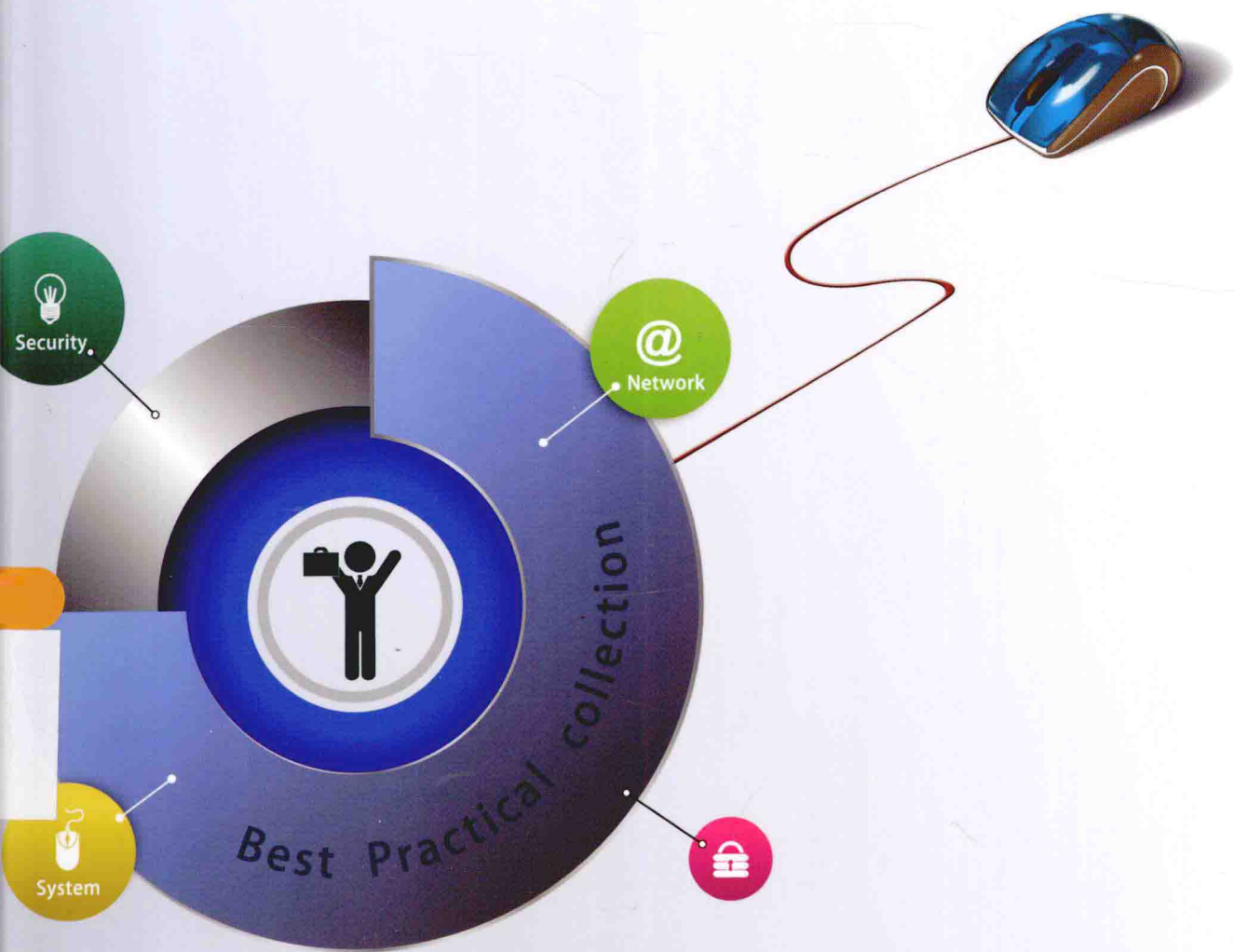
李源 编著

系统防护、网络安全

黑客攻防|实用宝典|



书中内容涵盖系统安全与网络管理的方方面面，所有知识与技巧皆来自实际应用，浸透作者多年实践经验。

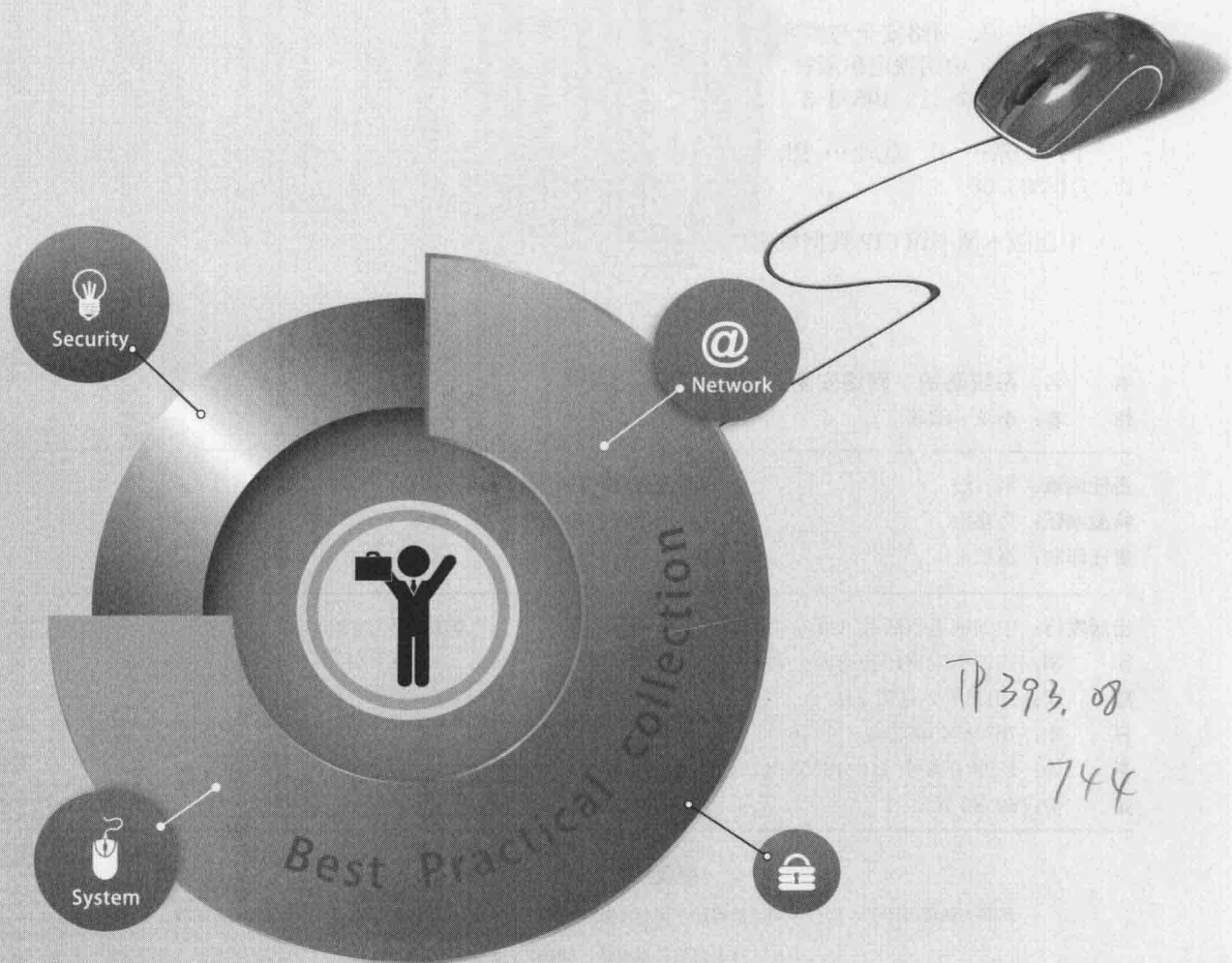


中国铁道出版社

CHINA RAILWAY PUBLISHING HOUSE

李源 编著

系统防护、网络安全 与 黑客攻防|实用宝典|



TP 393.08

744

中国铁道出版社

内 容 简 介

一直以来,计算机安全问题都是困扰众多用户的难题。本书从计算机系统安全、网络应用安全、黑客攻防技术、办公和移动存储数据安全保护、局域网安全等几个方面,全面详细地介绍了计算机网络安全和黑客攻防技术方面的应用技术。

本书在编写过程中突出知识的前沿性和内容的实用性,并使用了大量的图片及实例分析,使学习过程更加直观、明了。全书语言生动,图文并茂,深入浅出,旨在帮助网络管理员及计算机、网络安全从业人员积累实战经验,提升计算机、网络防护能力;同时本书也适合计算机家庭用户和办公用户阅读参考。

图书在版编目(CIP)数据

系统防护、网络安全与黑客攻防实用宝典 / 李源编

著. — 北京:中国铁道出版社,2015.2

ISBN 978-7-113-19553-3

I. ①系… II. ①李… 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(2014)第266214号

书 名:系统防护、网络安全与黑客攻防实用宝典

作 者:李源 编著

责任编辑:荆 波

读者服务热线:010-63560056

特邀编辑:马寒梅

封面设计:多宝格·付 巍

责任印制:赵星辰

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:三河市宏盛印务有限公司

版 次:2015年2月第1版

2015年2月第1次印刷

开 本:787mm×1092mm 1/16

印张:33 字数:769千

书 号:ISBN 978-7-113-19553-3

定 价:69.80元

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社教材图书营销部联系调换。电话:(010)51873174

打击盗版举报电话:(010)51873659

网络安全现状

在这个网络大普及的时代，利用网络办公，进行各种娱乐活动、商业活动、网上购物和网上银行交易已经渐渐成为人们生活中不可或缺的一部分。然而，系统中毒、网站被黑、商业信息泄密、QQ 号码被盗等事件更是层出不穷，给计算机用户造成了不同程度的损失。更加严重的是，随着电子商务及网上银行作为购物与金融交易的手段被广泛采用，利用网络进行以获取经济利益为目的的犯罪活动也越发猖獗，计算机的安全问题，尤其是网络安全问题也变得越来越重要。

从更长远的角度看，人们的生活正在迅速被计算机化、网络化。目前手机已经基本实现计算机化、网络化，新推出的手机基本都是智能手机，其数据安全也是问题多多而堪忧；家里的电视也正在被智能化，智能电视是下一波技术浪潮，我们总不想自己的电视机突然黑屏或者播放节目的账号被人盗用吧；而可以预见的未来，汽车也将被计算机化、网络化，新的智能汽车一旦被黑客攻破，也许会产生令人意想不到的事故。而这些新的计算机化产品的安全问题与计算机的安全问题在原理上是相通的，掌握了计算机安全问题的解决方法，就可以应对网络时代所有终端的安全问题。所以，对任何希望在未来数码时代成功驾驭新设备，而不被安全问题所烦恼的人来说，一定要学习计算机安全知识和技能。这在今天的社会，就像从小要学习防火防盗安全常识一样，人类已经进入一个新时代。

本书的读者

本书主要面向为数众多的中小企业专职或兼职的网络管理员，帮助他们从最实用的角度去理解系统与网络安全的维护理念；书中给出了大量维护系统和网络安全运行的经验与技巧，是具体工作实践中的随身宝典。

由于传统的观念个人计算机的安全问题无足轻重，加上计算机使用者的水平参差不齐，安全意识和安全习惯的缺乏，使个人计算机要面对的安全问题非常严峻。因此，本书也值得普通计算机用户选择阅读，帮助他们提高防范意识、掌握必要的安全手段，有效保障个人数据和财产安全。

本书的优势

本书内容覆盖计算机网络安全和黑客攻防技术的方方面面。知识面广，条理性强，从实际应用的角度出发，减少了枯燥死板的理论概念，加强应用性和可操作性。使用大量形象、清晰的图片，加强可读性，同时也会对读者的操作起到有效的参考作用。

本书由浅入深、循序渐进地介绍计算机网络安全知识体系。内容丰富，讲解精练。全书以

操作为主，提供了尽可能详细的操作步骤和分解图片，使所有操作一目了然。书中所涉及的各种方面的安全问题都是用户经常遇到的，并且是困扰大多数用户的常见问题。通过本书，读者可以结合自己的实际问题，逐步深入地学习计算机及其网络安全方面的基本知识、方法和技巧。

本书知识结构

全书共分 24 章，内容涵盖了计算机系统安全、网络应用安全、黑客攻防技术、办公和移动存储数据安全保护、局域网安全等多个方面。

计算机系统安全篇（1~6 章）主要介绍计算机系统安全方面的内容，包括密码设置、用注册表和组策略增强系统安全、系统安全功能设置、病毒木马的查杀和防护等内容。

网络应用安全篇（7~9 章）主要介绍网络浏览与应用安全方面的内容，内容涵盖网络浏览、网络邮件、网络购物等方面。

黑客攻防技术篇（10~15 章）主要介绍黑客攻防技术方面的内容，包含黑客常用的命令与工具、黑客入侵前期工作、常用密码破解、远程控制攻防、Windows 安全漏洞与端口检查和 Windows 系统防黑设置等方面的内容。

办公和移动存储数据安全保护篇（16~22 章）主要介绍办公和移动存储数据的安全保护与恢复方面的内容，包括重要文件和隐私保护、办公文档数据的保护和修复、移动存储设备的安全保护、重要数据丢失后的挽救、应用程序的备份与恢复和 Windows 系统备份与恢复方面的内容。

局域网安全篇（23~24 章）分别介绍有限局域网和无线局域网在安全方面需要注意的问题和应对之道。

网络学习资料下载

为了增加本书附加价值，我们特意在中国铁道出版社下载专区 <http://tdpress.com/zyzx/tsscflwj> 中放置了一整套的网络学习资料，供读者下载使用。

作者与感谢

本书由解放军第三〇二医院计算机信息中心李源编写。由于时间仓促，书中难免会出现一些错误和缺漏之处，望广大读者朋友评判指正。

编者

2014 年 12 月

第 1 篇 计算机系统安全篇

第 1 章 计算机安全的第一道防线

1.1 设置系统登录密码和启动密码.....	1
1.1.1 创建账户的方法.....	1
1.1.2 设置账户登录密码.....	3
1.1.3 设置系统启动密码.....	5
1.2 在 BIOS 中设置开机密码.....	6
1.2.1 设置 CMOS 进入密码.....	6
1.2.2 设置开机密码.....	7
1.3 计算机不用时及时锁定.....	8
1.3.1 快捷方式法.....	8
1.3.2 快捷组合键法.....	9
1.3.3 使用休眠功能.....	9
1.3.4 使用“关机”菜单.....	11
1.3.5 设置屏保密码.....	11
1.4 系统默认账户安全设置.....	12
1.4.1 启用 Administrator 账户.....	12
1.4.2 Administrator 账号设置.....	14
1.4.3 Guest 账号设置.....	16
1.4.4 为用户设置合适的身份.....	17
1.5 系统服务安全设置.....	20
1.5.1 查看启用的服务项目.....	20
1.5.2 关闭、禁止与重新启用服务.....	21
1.5.3 Windows 7 服务优化设置.....	22

第 2 章 用注册表增强安全

2.1 认识注册表.....	27
2.1.1 注册表的作用.....	27

2.1.2	注册表的基本结构.....	29
2.2	注册表中启动项管理.....	35
2.2.1	了解系统启动项.....	35
2.2.2	Load 键值.....	37
2.2.3	Userinit 键值——用户相关.....	37
2.2.4	Run 子键.....	37
2.2.5	RunOnce 子键.....	38
2.2.6	Windows 中加载的服务.....	39
2.2.7	Windows Shell——系统接口.....	40
2.2.8	BootExecute——属于启动执行的一个项目.....	40
2.2.9	组策略加载程序.....	41
2.3	设置注册表加强网络安全.....	42
2.3.1	网络连接限制.....	42
2.3.2	系统启动时弹出对话框.....	42
2.3.3	IE 默认连接首页被修改.....	43
2.3.4	篡改 IE 的默认页.....	44
2.3.5	IE 右键菜单被修改.....	44
2.3.6	IE 工具栏被添加网站链接.....	45
2.4	注册表的备份和恢复.....	45
2.4.1	使用系统自带工具备份和恢复注册表.....	45
2.4.2	使用第三方软件备份和恢复注册表.....	46

第 3 章 用组策略增强系统安全

3.1	认识组策略.....	49
3.1.1	组策略与注册表.....	49
3.1.2	组策略的运行方式.....	50
3.2	系统安全防护策略.....	52
3.2.1	禁止运行指定程序.....	52
3.2.2	禁止修改系统还原配置.....	53
3.2.3	保护虚拟内存页面文件中的秘密.....	53
3.2.4	阻止访问命令提示符.....	54
3.2.5	锁定注册表编辑器.....	55
3.2.6	禁止用户访问指定驱动器.....	56
3.2.7	防止搜索泄露隐私.....	57
3.2.8	记录上次登录系统的时间.....	57

3.2.9	限制密码“尝试”次数.....	57
3.3	“桌面”、“任务栏”和“开始”菜单安全策略.....	58
3.3.1	拒绝使用没有签证的桌面小工具.....	58
3.3.2	我的桌面你别改.....	59
3.3.3	关闭“气球”通知.....	60
3.3.4	不保留最近打开文档的历史.....	60
3.3.5	阻止用户重新安排工具栏.....	61
3.4	移动存储设备安全策略.....	61
3.4.1	禁止数据写入U盘.....	61
3.4.2	完全禁止使用U盘.....	62
3.4.3	禁止安装移动设备.....	62
3.4.4	禁用移动设备执行权限.....	63
3.4.5	禁止光盘自动播放.....	63
3.5	IE安全策略.....	64
3.5.1	锁定主页.....	65
3.5.2	禁止更改分级审查.....	65
3.5.3	禁止保存密码.....	66
3.5.4	禁用更改高级页设置.....	66
3.5.5	禁用“Internet选项”菜单选项.....	67

第4章 Windows安全功能

4.1	通过“操作中心”了解系统安全.....	68
4.1.1	“操作中心”概述.....	68
4.1.2	实时报告安全功能是否禁用.....	69
4.1.3	自定义“操作中心”的报警信息.....	70
4.2	UAC设置.....	70
4.2.1	UAC的作用.....	71
4.2.2	调整UAC授权等级.....	72
4.3	使用BitLocker保护数据.....	72
4.3.1	使用BitLocker加密驱动器.....	72
4.3.2	访问BitLocker加密的驱动器.....	75
4.3.3	BitLocker加密的恢复.....	76
4.4	事件查看器.....	77
4.4.1	启动事件查看器.....	77
4.4.2	查看事件日志的详细属性.....	79

4.4.3	利用事件日志对故障进行分析.....	79
4.4.4	将任务附加到指定事件.....	80
4.5	使用 Windows 7 防火墙保护计算机.....	83
4.5.1	Windows 7 防火墙常规设置.....	83
4.5.2	Windows 7 防火墙高级设置.....	86
4.5.3	查看 Windows 防火墙的日志.....	94

第 5 章 病毒的防范和查杀

5.1	认识计算机病毒.....	95
5.1.1	什么是计算机病毒.....	95
5.1.2	计算机病毒的特点.....	96
5.1.3	病毒对计算机的危害.....	97
5.2	病毒的防治常识.....	100
5.2.1	识别计算机病毒类型.....	100
5.2.2	计算机病毒防治建议.....	102
5.3	卡巴斯基杀毒软件的使用.....	104
5.3.1	安装卡巴斯基安全软件 2014.....	104
5.3.2	及时更新杀毒软件.....	105
5.3.3	全盘扫描.....	106
5.3.4	快速扫描.....	107
5.3.5	自定义扫描.....	107

第 6 章 木马的防范和查杀

6.1	认识木马.....	110
6.1.1	木马简介.....	110
6.1.2	木马的危害.....	112
6.1.3	木马的类型.....	112
6.1.4	中木马病毒后出现的状况.....	114
6.2	找出计算机中的木马.....	114
6.2.1	木马常用端口.....	114
6.2.2	木马运行机制.....	117
6.2.3	木马隐身方法.....	119
6.3	手动查杀病毒、木马的弊端.....	121
6.4	使用 Windows 木马清道夫查杀木马.....	121
6.4.1	安装 Windows 木马清道夫.....	121

6.4.2	查杀进程中的木马.....	123
6.4.3	扫描硬盘.....	124
6.5	使用 360 安全卫士查杀木马.....	126
6.5.1	安装 360 安全卫士.....	126
6.5.2	使用 360 安全卫士查杀木马.....	127
6.5.3	使用 360 系统急救箱.....	129

第 2 篇 网络应用安全篇

第 7 章 网络浏览安全

7.1	网页浏览安全概述.....	131
7.1.1	网络广告.....	131
7.1.2	恶意网站.....	132
7.1.3	网络偷窥.....	133
7.2	浏览器安全防范.....	134
7.2.1	Cookies 问题.....	134
7.2.2	浏览器安全设置.....	135
7.2.3	防范恶意脚本.....	138
7.2.4	使用第三方浏览器.....	140
7.3	浏览器修复.....	148
7.3.1	修复首页更改.....	148
7.3.2	修复右键菜单.....	149
7.3.3	修复工具栏.....	150
7.3.4	锁定 IE 主页.....	150

第 8 章 网络邮件安全

8.1	电子邮件的安全问题.....	153
8.1.1	垃圾邮件.....	153
8.1.2	邮件病毒.....	155
8.1.3	注册邮箱时的安全隐患.....	156
8.2	Web 邮箱的安全设置.....	157
8.2.1	QQ 邮箱反垃圾邮件设置.....	157
8.2.2	QQ 邮箱账户安全设置.....	160
8.2.3	网易邮箱反垃圾邮件设置.....	161
8.2.4	网易邮箱账户安全设置.....	164

8.2.5	网易邮箱安全设置.....	171
8.3	Foxmail 的安全设置.....	178
8.3.1	设置 Foxmail 中的账号口令.....	178
8.3.2	在 Foxmail 中设置垃圾邮件过滤.....	180

第 9 章 网络购物安全

9.1	网络购物概述.....	182
9.1.1	网络购物的优点.....	182
9.1.2	网络购物的缺点.....	183
9.2	网上购物的安全隐患.....	183
9.2.1	虚假信息.....	183
9.2.2	支付安全.....	184
9.2.3	钓鱼式陷阱.....	185
9.3	安全交易措施.....	186
9.3.1	详细了解商品.....	186
9.3.2	详细了解商家信誉.....	186
9.3.3	使用货到付款.....	187
9.3.4	维护正当权益.....	188
9.4	网上个人信息的保密.....	188
9.4.1	设置 IE 防止 Cookies 泄露个人资料.....	188
9.4.2	修改注册表防止 Cookies 泄露个人资料.....	188
9.4.3	使用隐私保护器保护网络隐私.....	190
9.5	用户账号、密码的保密.....	193
9.5.1	删除保存用户上网登录账号和密码的临时文件.....	193
9.5.2	使用“金山密码专家”保护密码.....	194
9.6	使用“金山网购保镖”保障网购安全.....	196
9.6.1	设置网购保护.....	196
9.6.2	使用网购敢赔功能.....	197

第 3 篇 黑客攻防技术篇

第 10 章 黑客常用的命令与工具

10.1	黑客常用的 DOS 命令.....	200
10.1.1	DOS 命令的格式.....	200
10.1.2	黑客常用的目录操作命令.....	201

10.1.3	黑客常用的文件操作命令.....	207
10.2	黑客常用的网络命令.....	213
10.2.1	远程登录命令——telnet.....	213
10.2.2	文件上传、下载命令——ftp.....	216
10.2.3	显示和修改本地 ARP 列表——arp.....	218
10.2.4	计划管理程序——at.....	219
10.2.5	网络测试命令.....	221
10.2.6	使用 net 命令管理网络.....	228
10.3	黑客常用工具介绍.....	232
10.3.1	流光扫描器的使用.....	232
10.3.2	HostScan 扫描器.....	236
10.3.3	网络神偷远程控制器的使用.....	238

第 11 章 黑客入侵前期工作

11.1	网络信息采集.....	241
11.1.1	使用 Ping 命令获取 IP 地址.....	241
11.1.2	使用网站获取 IP 地址.....	242
11.1.3	使用软件查询目标的地理位置.....	242
11.1.4	通过网站查询 IP 地址所在地理位置.....	244
11.1.5	查询网站备案信息.....	244
11.2	扫描系统漏洞.....	245
11.2.1	使用 X-Scan 检查系统漏洞.....	246
11.2.2	使用瑞星安全助手扫描系统漏洞.....	249
11.3	扫描系统服务和端口.....	250
11.3.1	使用 SuperScan 扫描器扫描服务和端口.....	250
11.3.2	使用 LanSee 局域网查看工具查看他人计算机中的端口.....	252
11.3.3	使用黑客字典编辑弱口令的扫描规则.....	254
11.3.4	使用弱口令扫描器获取口令.....	257

第 12 章 常用密码的破解

12.1	BIOS 密码的破解.....	259
12.1.1	使用放电的方法破解 BIOS 密码.....	259
12.1.2	使用跳线短接法破解 BIOS 密码.....	260
12.2	破解 Windows 7 系统登录密码.....	261
12.2.1	利用密码重置盘破解.....	261

12.2.2	利用 Windows 7 PE 破解.....	264
12.3	办公文档密码的破解.....	267
12.3.1	Passware Password Recovery Kit 简介.....	267
12.3.2	使用预定设置破解 Word 文档打开密码.....	269
12.3.3	使用向导破解 Excel 文档打开密码.....	271
12.3.4	使用破解编辑器破解 WinRAR 压缩文件密码.....	273

第 13 章 远程控制攻防

13.1	Windows 7 远程桌面连接的使用.....	276
13.1.1	开启远程桌面连接.....	276
13.1.2	使用远程桌面连接功能.....	277
13.1.3	向远程桌面传送文件.....	278
13.2	Windows 7 远程协助的使用.....	279
13.2.1	远程协助和远程桌面连接的区别.....	280
13.2.2	允许远程协助.....	280
13.2.3	邀请他人远程协助.....	280
13.2.4	利用远程协助帮助他人.....	281
13.3	使用腾讯 QQ 进行远程协助.....	283
13.3.1	使用腾讯 QQ 实现远程协助.....	283
13.3.2	使用 QQ 远程控制获取被控端计算机文件.....	285
13.4	使用 pcAnywhere 实现远程控制.....	286
13.4.1	主控端和被控端的安装.....	287
13.4.2	建立一个新的连接并连接到远程计算机.....	290
13.4.3	优化连接速率.....	292
13.4.4	对被控端计算机进行远程管理.....	292
13.4.5	在主控端和被控端之间实现文件传送.....	296

第 14 章 Windows 安全漏洞与端口检查

14.1	认识安全漏洞.....	297
14.1.1	安全漏洞产生的原因.....	297
14.1.2	安全漏洞的分类.....	298
14.1.3	漏洞等级评定.....	299
14.2	系统安全漏洞扫描.....	299
14.2.1	使用 MBSA 检查计算机系统安全.....	300
14.2.2	使用 Nmap 扫描系统安全漏洞.....	303

14.3 服务端口检查.....	306
14.3.1 计算机端口概述.....	306
14.3.2 监视计算机端口.....	307
14.3.3 在线检测计算机端口.....	307

第 15 章 Windows 系统防黑设置

15.1 了解系统进程.....	311
15.1.1 查看系统中运行的进程.....	311
15.1.2 关闭正在运行的危险进程.....	314
15.1.3 新建系统进程.....	315
15.1.4 查杀病毒进程.....	315
15.2 及时更新系统补丁防范黑客.....	317
15.2.1 Windows 更新概述.....	317
15.2.2 Windows 更新的配置.....	317
15.2.3 检查并安装 Windows 更新.....	318
15.2.4 查看 Windows 更新记录.....	320
15.2.5 删除 Windows 更新.....	320
15.3 系统方面的防黑设置.....	320
15.3.1 查看和关闭默认共享.....	320
15.3.2 设置代理服务器隐藏 IP 地址.....	322
15.4 注册表防黑设置.....	322
15.4.1 禁止远程修改注册表.....	322
15.4.2 永久关闭默认共享.....	323
15.4.3 禁止普通用户查看事件记录.....	324
15.4.4 找出隐藏的超级用户.....	324

第 4 篇 办公和移动存储数据安全保护篇

第 16 章 重要文件和隐私信息的安全保护

16.1 系统操作痕迹清理.....	326
16.1.1 文档操作痕迹清理.....	326
16.1.2 程序运行痕迹清理.....	327
16.1.3 网络浏览痕迹清理.....	329
16.1.4 利用工具软件清除系统的操作痕迹.....	331
16.2 隐藏重要驱动器.....	332

16.2.1	利用注册表隐藏驱动器.....	332
16.2.2	利用组策略隐藏驱动器.....	333
16.2.3	利用软件隐藏驱动器.....	334
16.3	彻底隐藏重要文件.....	335
16.3.1	用 Txt to bmp 将文本隐藏到图片中.....	335
16.3.2	用 Easy File Locker 隐藏文件或文件夹.....	335
16.3.3	使用 WinMend Folder Hidden 隐藏文件和文件夹.....	337
16.4	重要文件与文件夹的加密和解密.....	338
16.4.1	用类标识符加密文件夹.....	338
16.4.2	使用 NTFS 特性加密.....	343
16.4.3	导出与保存加密证书.....	344
16.4.4	使用“E-钻文件夹加密大师”加密文件夹.....	347
16.4.5	使用“Windows 优化大师”加密文件.....	349

第 17 章 办公文档安全保护

17.1	Word 文档安全保护.....	352
17.1.1	隐藏最近使用文档记录.....	352
17.1.2	快速“隐藏”文档内容.....	353
17.1.3	设置文档打开/修改密码.....	354
17.1.4	限制他人编辑文档.....	355
17.1.5	设置文档自动保存时间间隔.....	357
17.1.6	防范宏病毒.....	357
17.2	Excel 电子表格安全保护.....	358
17.2.1	设置允许用户进行的操作.....	358
17.2.2	隐藏含有重要数据的工作表.....	359
17.2.3	指定工作表中的可编辑区域.....	361
17.2.4	设置可编辑区域的权限.....	361
17.2.5	保护工作簿不能被修改.....	362
17.2.6	设置工作簿修改权限密码.....	363
17.2.7	设置工作簿打开权限密码.....	363
17.2.8	保护公式不被更改.....	364
17.2.9	禁用文档中的 ActiveX 控件.....	365
17.3	PowerPoint 演示文稿安全保护.....	366
17.3.1	将演示文稿设置为最终状态.....	366
17.3.2	受损演示文稿的恢复.....	367

17.3.3	设置保存时从文件属性中删除个人信息.....	367
17.3.4	加密演示文稿.....	368
17.4	压缩文件安全保护.....	369
17.4.1	设置 WinRAR 压缩密码.....	369
17.4.2	设置 WinZip 压缩密码.....	371
第 18 章 光盘、移动存储设备的安全保护		
18.1	光盘的使用和养护.....	373
18.1.1	正确使用光盘的方法.....	373
18.1.2	正确清洁光盘的方法.....	374
18.1.3	保存光盘的注意事项.....	375
18.1.4	光盘的修复.....	375
18.2	光盘数据损坏时的恢复.....	375
18.2.1	使用 CDCheck 恢复光盘数据.....	376
18.2.2	使用 BadCopy 恢复光盘数据.....	377
18.3	U 盘、移动硬盘内容的加密与保护.....	381
18.3.1	“迅软 U 密-优盘加密专家”简介.....	381
18.3.2	制作迅软 U 密安全盘.....	381
18.3.3	重新制作迅软 U 密安全盘.....	384
18.4	数码设备数据恢复方法.....	386
18.4.1	PHOTORECOVERY 的使用.....	386
18.4.2	Active@UNDELETE 的使用.....	387
第 19 章 重要数据丢失后的挽救		
19.1	数据恢复概述.....	391
19.1.1	数据丢失的原因.....	391
19.1.2	数据的可恢复性.....	392
19.1.3	数据类型影响恢复的成功率.....	393
19.1.4	物理恢复不可能 100%成功.....	393
19.2	数据恢复的原则和步骤.....	395
19.2.1	数据恢复的一般原则.....	395
19.2.2	数据恢复的一般步骤.....	396
19.3	可恢复的数据类型.....	396
19.3.1	硬件设备的数据恢复.....	396
19.3.2	软件故障数据恢复.....	398

19.4	使用 EasyRecovery 恢复硬盘数据.....	400
19.4.1	EasyRecovery 功能概述.....	400
19.4.2	提高数据恢复成功率.....	400
19.4.3	找回被误删除的数据.....	401
19.4.4	恢复被格式化的数据.....	404
19.4.5	恢复因其他原因丢失的数据.....	407
19.4.6	检测硬盘故障.....	408
19.5	使用 FinalData 恢复硬盘数据.....	409
19.5.1	FinalData 功能特点.....	409
19.5.2	FinalData 使用方法.....	410

第 20 章 办公文档数据的挽救

20.1	Word 文档的修复.....	414
20.1.1	使用自动恢复功能修复 Word 文档.....	414
20.1.2	手动打开恢复文件修复 Word 文档.....	415
20.1.3	“打开并修复”修复 Word 文档.....	417
20.1.4	“从任意文件还原文本”修复 Word 文档.....	418
20.1.5	禁止自动运行宏修复损坏的 Word 文档.....	419
20.1.6	文档格式法修复损坏的 Word 文档.....	419
20.1.7	重设格式法修复损坏的 Word 文档.....	419
20.1.8	创建新的 Normal 模板修复损坏的 Word 文档.....	420
20.2	Excel 文档的修复.....	421
20.2.1	转换格式修复 Excel 文档.....	421
20.2.2	转换为较早的版本修复 Excel 文档.....	421
20.2.3	“打开并修复”Excel 自行修复.....	421
20.3	Office 文档通用修复方法.....	422
20.3.1	OfficeFIX 修复 Office 文档.....	422
20.3.2	EasyRecovery 修复 Office 文档.....	426
20.4	WinRAR 压缩文件的修复.....	428
20.4.1	使用 WinRAR 自带的修复功能.....	428
20.4.2	使用 Advanced RAR Repair 修复 RAR 文档.....	429

第 21 章 应用程序的备份与恢复

21.1	IE 数据的备份与恢复.....	431
21.1.1	IE 收藏夹的备份与恢复.....	431