

中小企业 网络管理员工作实践

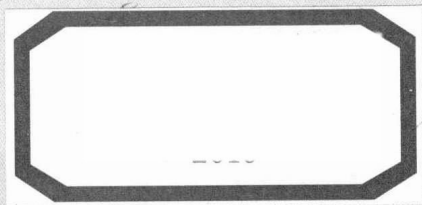
黑客攻防安全卷

黄治国
李颖
编著



精彩定制
视频
扫码即看

中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.



中小企业 网络管理员工作实践

黑客攻防安全卷

黄治国
李颖
——
编著

RFID



中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.

内 容 简 介

全书由浅入深地讲解了黑客攻防的基础知识、常用命令及工具、操作系统漏洞与注册表防黑实战、电脑木马的防黑实战、电脑病毒的防黑实战、系统入侵与远程控制的防黑实战、系统账户数据的防黑实战、文件数据的防黑实战、网络账号的防黑实战、局域网安全的防黑实战、无线网络安全的防黑实战、磁盘数据安全攻防等内容。通过对本书的学习，读者在了解黑客入侵攻击的原理、工具和方式后，能掌握防御入侵攻击的相应手段，并将其应用到实际的计算机安全防护领域。

本书内容丰富全面，图文并茂，讲解深入浅出，旨在帮助中小型企业中的网络管理员梳理黑客攻防知识，提升应用技能，增加实践经验。除此之外，本书对于网络安全知识进行了系统地讲解，可作为各种计算机培训班的辅导用书。

图书在版编目（CIP）数据

中小企业网络管理员工作实践. 黑客攻防安全卷 /黄治国, 李颖
编著. —北京: 中国铁道出版社有限公司, 2019. 6

ISBN 978-7-113-25766-8

I. ①中… II. ①黄… ②李… III. ①中小企业—计算机网络管理
②黑客—网络防御 IV. ①TP393.18②TP393.081

中国版本图书馆 CIP 数据核字(2019)第 087779 号

书 名: 中小企业网络管理员工作实践: 黑客攻防安全卷

作 者: 黄治国 李 颖

责任编辑: 荆 波

读者热线电话: 010-63560056

责任印制: 赵星辰

封面设计: **MX** DESIGN
STUDIO

出版发行: 中国铁道出版社有限公司 (100054, 北京市西城区右安门西街 8 号)

印 刷: 中国铁道出版社印刷厂

版 次: 2019 年 6 月第 1 版 2019 年 6 月第 1 次印刷

开 本: 787 mm×1 092 mm 1/16 印张: 23 字数: 578 千

书 号: ISBN 978-7-113-25766-8

定 价: 59.80 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, 请与本社读者服务部联系调换。电话: (010) 51873174

打击盗版举报电话: (010) 51873659

在互联网+时代，黑客通常都是一类拥有超高计算机技术的人，他们甚至不需要亲自接触用户的计算机，就可以偷窥其中的账户、密码登录信息，设置破坏操作系统，随着越来越多的信息要通过互联网来实现，因此，防御黑客入侵已经成为中小企业网络管理最为直观、最为重要的工作。

本书内容

本书站在中小企业网络管理员的角度，全面且详细地介绍了黑客攻防的基础知识，主要包括黑客常用命令及工具、操作系统漏洞与注册表防黑实战、电脑木马的防黑实战、电脑病毒的防黑实战、系统入侵与远程控制的防黑实战、系统账户数据的防黑实战、文件数据的防黑实战、网络账号的防黑实战、VPN 网的防黑实战、Web 网站安全的防黑实战、局域网安全的防黑实战、无线网络安全的防黑实战、磁盘数据安全攻防等内容。

本书的重点在于介绍如何采取有效的防范措施来防御黑客入侵攻击局域网内的计算机，让用户真正掌握网络安全攻防的能力。

本书内容丰富全面，图文并茂，深入浅出，旨在帮助中小企业中的网络管理员梳理黑客攻防知识与技能，增加实践经验。同时也可作为各种计算机培训班的辅导用书。

本书特色

本书主要有以下几个特点：

（1）内容全面

本书由浅入深，安排有 3 篇内容：网络安全基础篇、网络安全攻防实战篇、数据资料攻防篇。

（2）内容新

本书紧跟网络安全技术发展，以 Windows 7 操作系统平台为主，Windows 10 操作系统为辅，讲解网络安全的全新知识与应用技能。

（3）案例新

本书精选目前网络安全攻防前沿的案例，以及主流的攻防工具软件，来帮助读者进行实际操作，加深学习印象，力争让读者做到学以致用。

（4）步骤操作详细

本书采用图文并茂的写作方式，读者在学习时只要跟着操作步骤进行操作，就可以完成案例。

(5) 扫码看视频

我们特意为本书制作了精彩视频，二维码嵌入书中相应章节，读者可根据需求，扫码看相应的视频进行在线学习。

(6) PPT 讲义

为了帮助读者尽快理清本书的知识脉络，我们特别制作了 PPT 讲义，通过 PPT 讲义了解每章的重点和难点。

作者团队

除封面署名作者外，参加编写的人员还有陈玉琪、陈志凯、刘术、黄兰娟、刘静、黄丽平、李桂生、向金华、苏风华、许文胜、许昌胜、谭成德、唐小红、魏兆丰、苏晨光、周晓峰、李雅、黄丽娟、罗艳清等人。由于作者水平有限，书中难免存在疏漏与不妥之处，欢迎广大读者批评指正。

版权声明

本书及下载包中所采用的照片、图片、模型、赠品等素材，均为其相关的个人、公司、网站所有，本书引用仅为说明（教学）之用，读者不可将相关内容用于其他商业用途或进行网络传播。

郑重声明

根据国家有关法律规定，任何利用黑客技术攻击他人计算机的行为都属于违法行为。希望读者在阅读本书后绝对不要使用本书中介绍的黑客技术对别人的计算机进行攻击，否则后果自负，切记切记！

编者

2019年4月

第 1 章 掀起黑客的神秘面纱

1.1 认识黑客	1
1.1.1 什么是黑客	1
1.1.2 黑客常用术语	1
1.2 黑客入侵及异常表现	3
1.3 黑客常用攻击手段	6
1.4 黑客的定位目标——IP 地址	7
1.4.1 认识 IP 地址	7
1.4.2 IP 地址的分类	7
1.4.3 查看 IP 地址	8
【实验 1-1】在 Windows 7 系统中查看内网 IP 地址	8
【实验 1-2】在 Windows 10 系统中查看内网 IP 地址	8
【实验 1-3】查看外网 IP 地址	9
1.5 黑客的专用通道——端口	10
1.5.1 端口的分类	10
1.5.2 关闭端口	11
1.5.3 限制指定的端口	13
1.6 黑客藏匿的首选地——系统进程	24
1.6.1 系统进程简介	24
1.6.2 关闭系统进程	25
【实验 1-4】在 Windows 7 系统中关闭系统进程	25
【实验 1-5】在 Windows 10 系统中关闭系统进程	25
1.6.3 新建系统进程	27
【实验 1-6】在 Windows 7 系统中新建系统进程	27
【实验 1-7】在 Windows 10 系统中新建系统进程	28

第 2 章 黑客常用命令及工具

2.1 黑客攻防常用命令	29
2.1.1 Ping 命令	29
【实验 2-1】测试网卡	30
【实验 2-2】判断与外界网络连通	31
【实验 2-3】解析 IP 地址的计算机名	32

2.1.2	Nbstat 命令	32
	【实验 2-4】查看 NetBIOS	33
2.1.3	Netstat 命令	35
	【实验 2-5】Netstat 命令应用	36
2.1.4	Tracert 命令	38
2.1.5	Telnet 命令	39
2.1.6	IPconfig 命令	41
	【实验 2-6】使用 Ipconfig 测试当前计算机的所有信息	41
2.1.7	FTP 命令	42
2.1.8	ARP 命令	43
2.1.9	NET 命令	44
	【实验 2-7】使用 NET 命令查看共享资源、创建和修改计算机上的用户账户、管理共享资源	45
2.2	黑客常用入侵工具	47
2.2.1	端口扫描工具	47
	【实验 2-8】使用 Nmap 扫描器扫描端口	47
	【实验 2-9】使用 ScanPort 扫描器扫描端口	50
2.2.2	嗅探工具	56
	【实验 2-10】使用 SmartSniff 捕获 TCP/IP 数据包	56
	【实验 2-11】使用网络数据包嗅探专家捕获 TCP/IP 数据包	58
2.2.3	目标入侵工具	60
2.2.4	加壳工具	64
2.2.5	脱壳工具	67

第 3 章 操作系统漏洞与注册表的防黑实战

3.1	认识操作系统漏洞	70
3.2	系统漏洞的防黑实战	71
3.2.1	Windows Update 更新系统	71
	【实验 3-1】在 Windows 7 系统中设置并安装更新	71
	【实验 3-2】在 Windows 10 系统中安装补丁	73
3.2.2	启用 Windows 防火墙	74
	【实验 3-3】在 Windows 7 系统中启用防火墙	75
	【实验 3-4】在 Windows 10 系统中启用防火墙	76
3.2.3	软件更新漏洞	77
	【实验 3-5】使用电脑管家修复漏洞	77
	【实验 3-6】使用 360 安全卫士修复漏洞	78
3.3	注册表的防黑实战	79
3.3.1	注册表的基本结构	79

3.3.2 注册表常见的入侵方式	81
3.3.3 关闭远程注册表管理服务	82
【实验 3-7】在 Windows 7 系统中关闭远程注册表管理服务	82
【实验 3-8】在 Windows 10 系统中关闭远程注册表管理服务	83
3.3.4 禁止使用注册表编辑器	84
【实验 3-9】在 Windows 7 系统中禁止使用注册表编辑器	85
【实验 3-10】在 Windows 10 系统中禁止使用注册表编辑器	86

第 4 章 电脑木马的防黑实战

4.1 认识电脑木马	88
4.1.1 常见的木马类型	88
4.1.2 木马常用的入侵方法	89
4.2 木马常用的伪装手段	90
4.3 木马常见的启动方式	91
4.3.1 利用注册表启动	91
4.3.2 利用系统文件启动	91
4.3.3 利用系统启动组启动	91
4.3.4 利用系统服务实现木马的加载	92
4.4 查询系统中的木马	92
4.4.1 通过启动文件检测木马	93
4.4.2 通过进程检测木马	93
4.4.3 通过网络连接检测木马	93
4.5 使用木马清除软件清除木马	94
4.5.1 木马专家	94
【实验 4-1】使用木马专家清除木马	94
4.5.2 木马清除大师	96
【实验 4-2】使用木马清除大师清除木马	96
4.5.3 木马清道夫	98
【实验 4-3】使用木马清道夫清除木马	98

第 5 章 电脑病毒的防黑实战

5.1 了解电脑病毒	102
5.1.1 电脑病毒的特点	102
5.1.2 电脑病毒的分类	103
5.1.3 电脑中病毒后的表现	104
5.1.4 常见的电脑病毒	104
5.2 预防电脑病毒	105

5.3	查杀电脑病毒.....	106
5.3.1	使用瑞星杀毒软件查杀病毒.....	106
5.3.2	使用 360 杀毒软件查杀病毒.....	108
5.4	防御 U 盘病毒.....	112
5.4.1	使用组策略关闭“自动播放”功能.....	113
	【实验 5-1】在 Windows 7 系统中使用组策略关闭“自动播放”功能.....	113
	【实验 5-2】在 Windows 10 系统中使用组策略关闭“自动播放”功能.....	114
5.4.2	修改注册表关闭“自动播放”功能.....	115
	【实验 5-3】在 Windows 7 系统中修改注册表关闭“自动播放”功能.....	115
	【实验 5-4】在 Windows 10 系统中修改注册表关闭“自动播放”功能.....	116
5.4.3	设置服务关闭“自动播放”功能.....	117
	【实验 5-5】在 Windows 7 系统中设置服务关闭“自动播放”功能.....	117
	【实验 5-6】在 Windows 10 系统中设置服务关闭“自动播放”功能.....	118
5.5	查杀 U 盘病毒.....	120
5.5.1	用 U 盘杀毒专家查杀.....	120
5.5.2	使用 U 盘病毒专杀工具查杀.....	122

第 6 章 系统入侵与远程控制的防黑实战

6.1	入侵系统的常用手段.....	125
6.1.1	在命令提示符中创建隐藏账号入侵.....	125
6.1.2	在注册表中创建隐藏账号入侵.....	127
6.2	抢救被账号入侵的系统.....	131
6.2.1	找出黑客创建的隐藏账号.....	131
6.2.2	批量关闭危险端口.....	133
6.3	通过远程工具入侵系统.....	134
6.3.1	通过 Windows 远程桌面控制.....	134
	【实验 6-1】启用 Windows 7 系统中远程桌面功能.....	134
	【实验 6-2】启用 Windows 10 系统远程桌面功能.....	135
	【实验 6-3】添加 Windows 7 系统远程桌面用户.....	137
	【实验 6-4】添加 Windows 10 系统远程桌面用户.....	137
	【实验 6-5】在 Windows 10 系统中远程连接 Windows 7 系统桌面.....	139
	【实验 6-6】在 Windows 7 系统中远程连接 Windows 10 系统桌面.....	141
	【实验 6-7】断开或注销 Windows 7 系统远程桌面.....	142
	【实验 6-8】断开或注销 Windows 10 系统远程桌面.....	143
6.3.2	通过远程控件工具控制.....	144
	【实验 6-9】使用 Team Viewer 远程控制目标主机.....	145
6.4	远程控制的防黑实战.....	146

6.4.1 关闭 Windows 远程桌面功能	146
【实验 6-10】在 Windows 7 系统中关闭远程桌面功能	147
【实验 6-11】在 Windows 10 系统中关闭远程桌面功能	147
6.4.2 使用瑞星防火墙保护系统安全	148

第 7 章 系统账户数据的防黑实战

7.1 认识系统账户	150
7.2 黑客破解密码的常用方法	151
7.3 系统账户数据的防黑实战	151
7.3.1 设置系统管理员密码	151
【实验 7-1】设置 Windows 7 系统管理员密码	152
【实验 7-2】设置 Windows 10 系统管理员密码	154
7.3.2 禁用来宾账户	156
7.3.3 设置屏幕保护密码	158
【实验 7-3】设置 Windows 7 系统屏幕保护程序密码	159
【实验 7-4】设置 Windows 10 系统屏幕保护程序密码	160
7.3.4 创建密码重置盘	161
7.4 系统账户密码丢失（破解）后的补救措施	165
7.4.1 跳过 Windows 7/10 系统密码	165
7.4.2 使用密码重置盘破解密码	166
【实验 7-5】使用密码重置盘破解 Windows 7 系统密码	166
【实验 7-6】使用密码重置盘破解 Windows 10 系统密码	169
7.4.3 使用第三方工具破解密码	170
【实验 7-7】使用 Active@ Password Changer Professional 破解密码	171
【实验 7-8】使用 NTPWEdit 工具重设 Windows 10 系统管理员密码	173
7.5 另类的系统账户数据的防黑实战	175
7.5.1 更改系统管理员账户名称	175
7.5.2 伪造陷阱账户保护管理员账户	176
7.6 通过组策略提升系统账户的安全	178
7.6.1 限制 Guest 账户的操作权限	178
7.6.2 设置账户密码的复杂性	180
7.6.3 开启账户的锁定功能	181
7.6.4 禁用 Guest 账户在本地系统登录	182

第 8 章 文件数据的防黑实战

8.1 黑客常用破解文件密码的方法	184
8.1.1 利用 Word Password Recovery 破解 Word 文档密码	184

8.1.2	利用 PassFab Word Password Recovery 破解 Word 文件密码	186
	【实验 8-1】利用 PassFab Word Password Recovery 破解 Word 文件密码	186
8.1.3	利用 Excel Password Recovery 破解 Excel 文件密码	187
	【实验 8-2】利用 Excel Password Recovery 破解 Excel 文件密码	187
8.1.4	利用 Office Password Recovery 破解工具破解 PPT 文件密码	189
	【实验 8-3】利用 Office Password Recovery 破解 PPT 文件密码	189
8.1.5	利用 APDFPR 密码破解工具破解 PDF 文件密码	190
	【实验 8-4】利用 APDFPR 破解 PDF 文件密码	190
8.2	文件数据的加密防黑	192
8.2.1	利用 Word 自身功能给 Word 文件加密	193
	【实验 8-5】利用 Word 自身功能给 Word 文件加密	193
8.2.2	利用 Excel 自身功能给 Excel 文件加密	194
8.2.3	利用 PDF 文件加密器加密 PDF 文件	195
8.2.4	利用 WinRAR 的自加密功能加密 RAR 文件	197

第 9 章 网络账号防黑实战

9.1	QQ 账号及密码攻防常用工具	199
9.2	增强 QQ 安全性的方法	200
9.2.1	定期更换 QQ 密码	200
9.2.2	申请密码保护	201
9.2.3	加密聊天记录	202
9.3	微博等自媒体账号的安全防范	203
9.3.1	网络自媒体账号被盗的途径	203
9.3.2	正确使用自媒体平台	204
9.4	微信等自媒体账号的安全防范	204
9.4.1	安全使用微信的原则	205
9.4.2	微信账号被盗的应对措施	205
9.5	邮箱账户的安全防范	206
9.5.1	隐藏邮箱账户	206
9.5.2	电子邮件攻击防范措施	206
9.6	支付账户的安全防范	207
9.6.1	加强支付宝账户的安全防护	207
	【实验 9-1】定期修改登录密码	207
	【实验 9-2】修改绑定手机	210
	【实验 9-3】设置安全保护问题	211
9.6.2	加强支付室内资金的安全防护	213
	【实验 9-4】定期修改支付密码	214

第 10 章 网页浏览器的防黑实战

10.1	了解网页恶意代码.....	217
10.2	常见恶意网页代码及攻击方法.....	218
10.2.1	启动时自动弹出对话框和网页.....	218
10.2.2	利用恶意代码禁用注册表.....	219
	【实验 10-1】使用 Registry Workshop 恢复注册表.....	219
10.3	恶意网页代码的预防和清除.....	219
10.3.1	预防恶意网页代码.....	219
10.3.2	清除恶意网页代码.....	220
	【实验 10-2】使用 IEScan 恶意网站清除软件.....	220
	【实验 10-3】使用 Windows 软件清理大师清除软件.....	221
10.4	攻击浏览器的常见方式.....	223
10.4.1	修改默认主页.....	223
	【实验 10-4】设置浏览器的主页.....	223
	【实验 10-5】锁定浏览器的主页.....	225
10.4.2	恶意更改浏览器标题栏.....	226
10.4.3	强行修改浏览器的右键菜单.....	227
	【实验 10-6】删除非法网站链接.....	227
	【实验 10-7】恢复右键菜单.....	228
10.4.4	强行修改浏览器的首页按钮.....	228
10.4.5	删除桌面上的浏览器图标.....	229
10.5	浏览器的自我防护.....	231
10.5.1	提高 IE 浏览器的安全防护等级.....	231
	【实验 10-8】提高 IE 浏览器的安全防护等级.....	231
10.5.2	清除浏览器中的表单.....	232
10.5.3	清除 Cookie 信息.....	232
10.6	使用第三方软件保护浏览器安全.....	233
10.6.1	使用 IE 修复专家.....	233
	【实验 10-9】使用 IE 修复专家修复浏览器.....	233
10.6.2	使用 IE 伴侣.....	235
	【实验 10-10】使用 IE 伴侣修复 IE 浏览器.....	235

第 11 章 局域网防黑安全实战

11.1	常见的几种局域网攻击类型.....	236
11.2	局域网安全共享.....	237
11.2.1	设置共享文件夹账户与密码.....	237

11.2.2	隐藏共享文件夹	240
11.3	局域网攻击工具	240
11.3.1	网络剪刀手 Netcut	240
11.3.2	WinArpAttacker 工具	243
11.4	局域网监控工具	245
11.4.1	LanSee 工具	245
	【实验 11-1】使用 LanSee 工具查看局域网状态信息	245
11.4.2	IPBook 工具	250
	【实验 11-2】使用 IPBook 工具搜索共享资源	250

第 12 章 Web 网站安全的防黑实战

12.1	Web 网站维护基础知识	254
12.2	Web 网站的常见攻击方式	255
12.2.1	DOS 攻击	255
12.2.2	DDOS 攻击	256
12.2.3	SQL 注入攻击	256
12.3	Web 网站安全的防黑	256
12.3.1	检测上传文件的安全性	257
12.3.2	设置网站访问权限	258
	【实验 12-1】通过设置用户访问权限来限制网站访问权限	259
12.3.3	预防 SYN 系统攻击	260
	【实验 12-2】通过修改注册表来防御 SYN 系统攻击	260
12.3.4	防范 DDOS 攻击	262
12.3.5	全面防范 SQL 注入攻击	264

第 13 章 VPN 网的防黑实战

13.1	VPN 基础知识	265
13.1.1	VPN 的协议	265
13.1.2	VPN 的组件	266
13.2	VPN 网的常见攻击方式	266
13.2.1	攻击 PPTP VPN	267
13.2.2	攻击启用 IPSec 加密的 VPN	267
13.2.3	破解 VPN 登录账户名及密码	267
	【实验 13-1】使用 Dialupass 工具破解 VPN 登录账户名及密码	267
13.3	VPN 网安全的防黑	268
13.3.1	VPN 用户权限	268
	【实验 13-2】加强 VPN 用户权限	268

13.3.2 加强客户端安全	270
【实验 13-3】在 Windows 7 系统中加强 VPN 安全	271
【实验 13-4】在 Windows 10 系统中加强 VPN 安全	274
13.3.3 使用 VPN 时的注意事项	277

第 14 章 无线网络安全的防黑实战

14.1 无线网络基础知识	278
14.1.1 无线局域网拓扑结构	278
14.1.2 无线局域网传输方式	279
14.2 组建无线网络	280
14.2.1 连接并配置无线路由器	280
【实验 14-1】配置无线路由器	281
14.2.2 客户端连接无线网络	284
【实验 14-2】在 Windows 7 系统中连接无线网络	284
【实验 14-3】在 Windows 10 系统中连接无线网络	286
14.3 Wi-Fi 攻击的常见方式	288
14.3.1 钓鱼陷阱	288
14.3.2 陷阱接入点	288
14.3.3 攻击无线路由器	288
14.3.4 内网监听	289
14.4 无线网络安全防范的常用方法	289
14.4.1 修改无线路由器的 IP 地址	289
【实验 14-4】修改无线路由器的 IP 地址 (192.168.1.1)	289
14.4.2 修改无线路由器管理员密码	291
【实验 14-5】修改无线路由器管理员初始密码	291
14.4.3 修改 Wi-Fi 名称及密码	292
【实验 14-6】修改 Wi-Fi 名称及密码	292

第 15 章 系统数据安全的防黑实战

15.1 使用“系统还原”备份与还原系统	293
15.1.1 使用“系统还原”备份系统	293
【实验 15-1】在 Windows 7 系统中使用“系统还原”备份系统	293
【实验 15-2】在 Windows 10 系统中使用“系统还原”备份系统	294
15.1.2 使用“系统还原”还原系统	296
【实验 15-3】在 Windows 7 系统中使用“系统还原”还原系统	296
【实验 15-4】在 Windows 10 系统中使用“系统还原”还原系统	297
15.2 创建系统映像文件备份与还原系统	299

15.2.1	创建系统映像文件	299
	【实验 15-5】在 Windows 7 系统中创建系统镜像文件	299
	【实验 15-6】在 Windows 10 系统中创建系统镜像文件	301
15.2.2	使用系统镜像文件还原系统	304
	【实验 15-7】在 Windows 7 系统安全模式状态下还原系统	305
	【实验 15-8】在 Windows 7 系统控制台中还原系统	307
	【实验 15-9】在 Windows 10 系统中使用镜像文件还原系统	308
15.3	利用 Ghost 快速备份与恢复数据	312
15.3.1	利用 Ghost 快速备份数据	312
	【实验 15-10】备份硬盘 C 区数据	312
15.3.2	利用 Ghost 快速恢复数据	317
	【实验 15-11】还原硬盘 C 区数据	317
15.4	使用“一键还原精灵”备份与还原系统	321
15.4.1	使用“一键还原精灵”备份系统	321
	【实验 15-12】使用“一键还原精灵”标准版备份系统（首次使用）	321
15.4.2	使用“一键还原精灵”还原系统	323
	【实验 15-13】使用“一键还原精灵”标准版还原故障系统	323

第 16 章 磁盘数据安全的防黑实战

16.1	磁盘数据安全的基础知识	324
16.1.1	磁盘数据丢失的原因	324
16.1.2	磁盘数据丢失后的注意事项	325
16.2	备份磁盘数据	325
16.2.1	备份磁盘分区表数据	325
	【实验 16-1】使用 DiskGenius 备份磁盘分区表数据	325
16.2.2	备份磁盘引导区数据	327
	【实验 16-2】使用 BOOTICE 备份磁盘引导区数据	327
16.2.3	备份驱动程序	328
	【实验 16-3】使用驱动人生工具备份驱动程序	328
16.2.4	备份 IE 收藏夹	329
	【实验 16-4】使用 IE 自带备份功能备份 IE 收藏夹	329
16.2.5	备份电子邮件	330
16.3	还原磁盘数据	333
16.3.1	还原分区表数据	333
	【实验 16-5】使用 Disk Genius 还原磁盘分区表数据	333
16.3.2	还原引导区数据	334
	【实验 16-6】使用 BOOTICE 还原磁盘引导区数据	334

16.3.3	还原驱动程序数据	335
	【实验 16-7】使用驱动人生工具还原驱动程序数据	335
16.3.4	还原 IE 收藏夹数据	336
	【实验 16-8】使用备份数据还原 IE 收藏夹数据	336
16.4	恢复丢失的磁盘数据	339
16.4.1	从回收站中还原	339
	【实验 16-9】将误删文件从回收站中还原	339
16.4.2	清空回收站后的恢复	340
	【实验 16-10】使用注册表恢复清空回收站之后的文件	340
16.4.3	恢复误删除的文件	341
	【实验 16-11】使用 Final Data 恢复	342
	【实验 16-12】使用 Undelete Plus 恢复	343
16.4.4	恢复硬盘被分区或格式化后的数据	345
	【实验 16-13】使用 Easy Recovery 恢复数据	345
	【实验 16-14】使用 DataExplore 数据恢复大师恢复数据	347
16.4.5	恢复 Word 文档损坏后的数据	348
	【实验 16-15】使用 OfficeFIX 恢复 Word 文档	349
16.4.6	Excel 文件损坏数据恢复	352
	【实验 16-16】使用 Excel Recovery 修复 Excel 文档	352

第 1 章 掀起黑客的神秘面纱

如今，互联网在人们的生活、工作和学习中起着十分重要的作用。但是，随之而来的却是互联网的安全问题越来越突出。在互联网中，有一类人，他们掌握高超的计算机技术，但他们会破坏互联网的安全，这就是黑客。

本章从黑客的定义、常用术语、黑客入侵及异常表现、常用攻击手段等方面来掀起黑客的神秘面纱，从而为更好地防范黑客攻击打下良好的基础。

1.1 认识黑客

黑客，一个神秘而又常见的名词，是一个与网络安全息息相关的群体。本节通过介绍黑客的定义和常用术语等方面的知识，让读者全面了解黑客。

1.1.1 什么是黑客

黑客（Hacker）最初是指那些热衷于电脑并能够把一些应用程序组合起来或拆开来解决问题的人。如今，黑客被定义为非法搜索和渗透互联网访问和使用数据的人。

对于黑客而言，他们所做的事情总是带有一定的目的，也许是为了炫耀，也许是为了报复。

提示：红客是英文单词 Honker 的中文音译，它代表着一种精神，即热爱祖国、坚持正义和开拓进取的精神。因此，只要具备这种精神并热衷于计算机技术的人都可以成为 Honker。Honker 是 Hacker 中的一部分人，这部分人以维护国家利益为己任，不利用掌握的计算机和网络技术入侵自己国家的计算机或服务器。

1.1.2 黑客常用术语

在互联网中，我们经常会看到肉鸡、挂马和后门等词语，这些词语可以统称为黑客术语。下面我们介绍一些黑客常用的术语。

1. 肉鸡

肉鸡比喻那些可以随意被黑客控制的电脑。黑客可以像操作自己的电脑那样来操作它们，而不