

独家赠送内容丰富的 **超值大礼包**



礼包1: 11小时与本书同步的视频立体教学录像

礼包2: 20小时Office 2003电脑办公视频教学录像

礼包3: 电脑维护与故障排除技巧**50招**

礼包4: 摆脱黑客攻击的**150招**秘籍

礼包5: Office 2010电脑办公技巧**300招**

礼包6: Excel 常用办公函数**177例**

礼包7: “轻轻松松学会五笔打字”电子书

礼包8: 本书教学用PPT课件

定制精品图书+同步多媒体教学视频+超值大礼包=21天最佳学习方案!



21天精通

黑客攻防策略

双色版

▶▶▶ 新奇e族 编著

本书特色

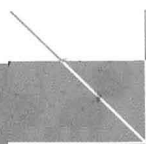
- ★ 黑客入门 → 系统类攻防策略 → 密码类攻防策略 → 黑客攻防策略与技能测评
- ★ 典型的攻防范例、实用的系统安全策略、隐私的密码攻防策略
- ★ 内容更全面、讲解更细致、案例更实用、赠送更超值、学习更轻松



化学工业出版社

 **21**天精通

黑客攻防策略



双色版

▶▶▶ 新奇e族 编著



化学工业出版社

· 北京 ·

本书以完整的黑客攻防策略为主线,以21天为学习任务周期(将每天的学习任务分解为今日探讨、今日目标以及要点导读和防黑实战等多个学习环节),一天掌握一项黑客攻击技能的学习模式,具有较强的可操作性和实训性。本书以零基础讲解为宗旨,全面讲解了黑客攻防入门、系统类攻防策略、密码类攻防策略、黑客攻防策略以及黑客攻防技能测评等内容,同时结合众多案例引导读者深入学习黑客攻防的各种方法、技巧与策略及实战技能以保护自己电脑及网络安全。

本书共计5周21天。其中,第1周黑客攻防入门主要讲解预防黑客必备知识、木马与病毒知识、常用扫描与嗅探工具以及预防黑客的常见攻击等知识;第2周系统类攻防策略主要讲解系统安全防守策略、IE浏览器攻防策略、注册表编辑器攻防策略、系统漏洞攻防策略以及系统入侵与远程控制攻防策略等知识;第3周密码类攻防策略主要讲解Windows密码攻防策略、文件密码攻防策略、QQ账号密码攻防策略、网络账号及密码攻防策略以及防范后门技术获取密码等知识;第4周黑客攻防策略主要讲解网站攻防策略、恶意网页代码攻防策略、木马与病毒攻防策略、数据安全攻防策略以及黑客痕迹清除技法等知识;第5周黑客攻防技能测评主要讲解如何通过关卡型黑客游戏和任务型黑客游戏来锻炼黑客攻防技能等知识。

随书赠送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。其采用环境教学、图文并茂的方式,使读者能够轻松上手,轻易学会。同时本书还赠送了大量的电脑使用技巧速查手册和电脑维护与故障处理技巧速查手册,以方便读者学习。

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、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

21天精通黑客攻防策略 / 新奇e族编著. —北京 :
化学工业出版社, 2013. 10

(办公高手成长日记)

ISBN 978-7-122-18513-6

I. ①2… II. ①新… 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227975号

责任编辑: 张 敏

装帧设计: 韩 飞

出版发行: 化学工业出版社(北京市东城区青年湖南街13号 邮政编码100011)

印 装: 化学工业出版社印刷厂

787mm×1092mm 1/16 印张24 字数585千字 2014年1月北京第1版第1次印刷

购书咨询: 010-64518888(传真: 010-64519686) 售后服务: 010-64518899

网 址: <http://www.cip.com.cn>

凡购买本书,如有缺损质量问题,本社销售中心负责调换。

定 价: 59.00元(1DVD-ROM)

版权所有 违者必究

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。当您认真、系统地学习本书之后，就可以非常自信地说：“我是一名网络黑客攻防专业人士！”，即便现在您还是一名计算机初学者。

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，从入门知识开始，引导读者以逐步深入的方式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、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，让读者学习起来轻松，操作起来有章可循。

► 随时检测自己的学习成果

每章首页中，均提供了今日探讨、今日目标以及要点导读等内容，便于读者掌握学习重点及学后检查。

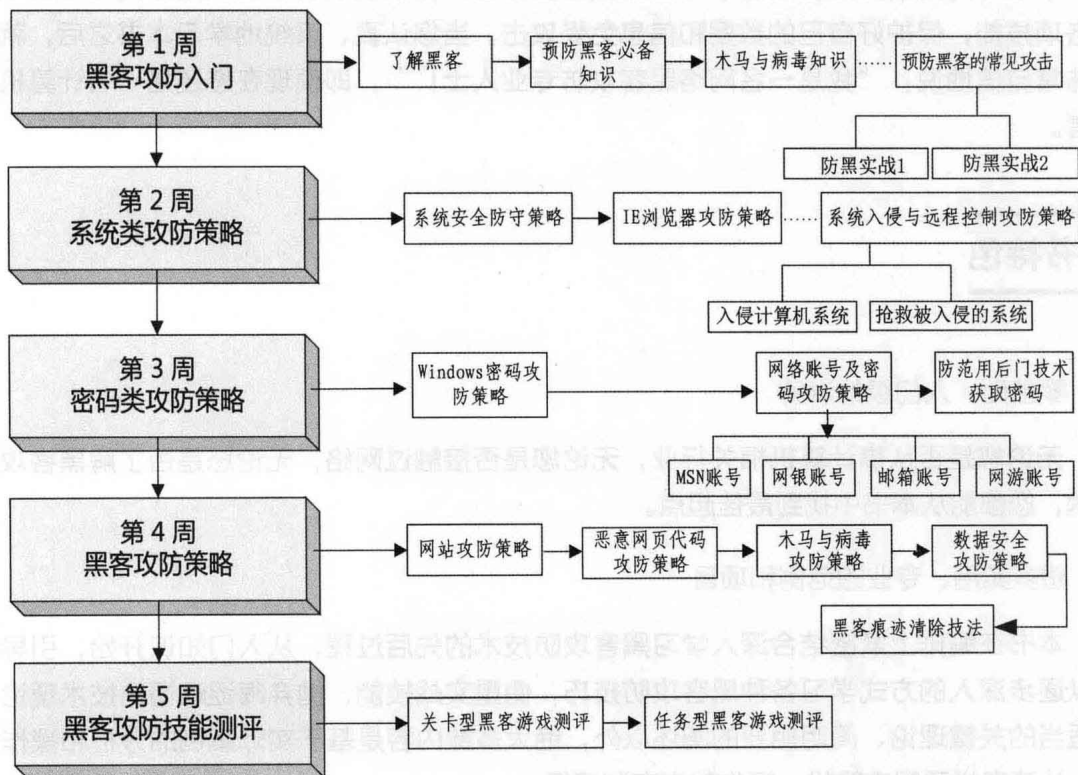
每章最后的“防黑实战”板块，均根据本章内容精选而成，读者可以随时检测自己的学习成果和实战能力，做到融会贯通。

► 细致入微、贴心提示

本书在讲解过程中，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，并轻松掌握各种操作技巧。

“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，从最初的黑客攻防入门、系统类攻防策略、密码类攻防策略、黑客攻防策略到最终的黑客攻防技能测评，同时在讲述中融入了很多攻防实战环节，以便进一步提高读者攻防的实战技能。



► 10 小时全书同步视频教学录像

视频教学录像以章节二级标题为纲领，全面完整地涵盖本书所有内容，详细完整地解析了每个技能点和行业案例，立体化教学，全方位指导。读者可以根据视频教学录像参照本书同步学习，有如一位老师在手把手教你，从而能更轻松地掌握书中所有的行业技能与操作技巧，使学习变得更轻松和从容。

► 超多、超值资源大放送

赠送20小时Office2003 电脑高效办公影音视频、电脑维护与故障排除技巧速查手册50招、摆脱黑客攻击的150招秘籍、“轻轻松松学会五笔打字”电子书、Excel办公常用函数速查手册177例、本书全部案例的素材与结果文件以及本书内容的教学PPT课件等超值资源。

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

本书由新奇e族编著，参加编写和资料搜集的人员有孙若淞、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。

在编写过程中，我们尽所能地将最好的讲解呈现给读者，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，可写信至信箱 elesite@163.com。

编 者

2013 年 11 月

目 录

21天精通黑客攻防策略

CONTENTS

第1周

黑客攻防入门

第1天 星期一
了解黑客

（7月22日 星期一）

2

- 1.1 黑客的定义 3
- 1.2 历史上著名的黑客事件 3
- 1.3 预防黑客必须掌握的网络知识 4

第2天 星期二
预防黑客必备知识

（7月23日 星期二）

6

- 2.1 进程、端口和服务 7
 - 2.1.1 进程概述 7
 - 2.1.2 端口概述 9
- 2.2 用于追踪黑客攻击的命令 11
 - 2.2.1 ping命令 11
 - 2.2.2 ipconfig命令 13
 - 2.2.3 NET命令 14
 - 2.2.4 netstat命令 15
 - 2.2.5 ftp命令 16
 - 2.2.6 telnet命令 18
 - 2.2.7 tracert命令 20
- 2.3 常见网络协议 20
 - 2.3.1 TCP/IP协议 21
 - 2.3.2 ARP协议 22
 - 2.3.3 ICMP协议 23
- 2.4 防黑实战1——利用“TCP/IP筛选”功能对服务器端口进行限制 24
- 2.5 防黑实战2——新建和关闭系统进程 25

- 3.1 认识木马..... 28
 - 3.1.1 什么是木马..... 28
 - 3.1.2 木马常用的入侵方法..... 29
 - 3.1.3 木马常用的伪装手段..... 30
 - 3.1.4 查询系统中的木马..... 35
- 3.2 认识病毒..... 38
 - 3.2.1 什么是病毒..... 38
 - 3.2.2 病毒的工作流程..... 39
- 3.3 常见的病毒..... 39
 - 3.3.1 操作系统病毒..... 40
 - 3.3.2 U盘病毒..... 43
 - 3.3.3 网络蠕虫病毒..... 45
 - 3.3.4 邮箱病毒..... 47
- 3.4 防黑实战1——将木马伪装成电子书..... 49
- 3.5 防黑实战2——在Word 2003中预防宏病毒..... 51

- 4.1 认识扫描目标的相关信息..... 54
 - 4.1.1 确定目标的IP地址..... 54
 - 4.1.2 查看目标所属地区..... 54
- 4.2 了解扫描器工具..... 55
 - 4.2.1 扫描器的工作原理..... 55
 - 4.2.2 扫描器的作用..... 55
- 4.3 常见端口扫描器工具..... 56
 - 4.3.1 Nmap扫描器..... 56
 - 4.3.2 SuperScan扫描器..... 57
- 4.4 常见多功能扫描器工具..... 60
 - 4.4.1 流光扫描器..... 60
 - 4.4.2 SSS扫描器..... 65
- 4.5 常用网络嗅探工具..... 69
 - 4.5.1 嗅探利器SmartSniff..... 69
 - 4.5.2 网络数据包嗅探专家..... 71
 - 4.5.3 影音神探..... 72
- 4.6 防黑实战1——注入点扫描工具..... 72
- 4.7 防黑实战2——交换型网络嗅探器WinArpSpoof..... 74

- 5.1 口令猜解攻击..... 77
 - 5.1.1 攻击原理..... 77

5.1.2 攻击实战	77	5.4 网络欺骗攻击	86
5.2 恶意代码攻击	82	5.4.1 攻击原理	86
5.2.1 攻击原理	82	5.4.2 攻击案例	87
5.2.2 攻击案例	83	5.5 防黑实战1——如何清除恶意 代码	88
5.3 缓冲区溢出攻击	83	5.6 防黑实战2——黑客是如何 破解压缩包密码的	89
5.3.1 攻击原理	84		
5.3.2 攻击案例	84		

第2周

系统类攻防策略

第**6**天 星期一
系统安全防守策略

 (7月 29 日 星期一)

94

6.1 本地安全策略	95	6.1.9 让“每个人”权限应用于 匿名用户	100
6.1.1 禁止在登录前关机	95	6.2 组安全策略	101
6.1.2 在超过登录时间后强制 用户注销	96	6.2.1 应用账户锁定策略	101
6.1.3 不显示上次登录时的 用户名	96	6.2.2 应用密码策略	102
6.1.4 限制格式化和弹出可移动 媒体	97	6.2.3 设置用户权限	104
6.1.5 对备份和还原权限进行 审计	98	6.2.4 不允许SAM账户的匿名 枚举	105
6.1.6 设置本地账户共享与安全 模式	98	6.2.5 禁止访问控制面板	105
6.1.7 禁止安装未签名的驱动 程序	99	6.2.6 禁止更改【开始】菜单与 任务栏	106
6.1.8 不允许SAM账户和共享的 匿名枚举	100	6.2.7 禁止更改桌面设置	106
		6.2.8 禁用部分应用程序	107
		6.3 计算机管理策略	108
		6.3.1 事件查看器的使用	108
		6.3.2 共享资源的管理	110

6.3.3	管理系统中的服务程序...	110
6.4	防黑实战1——自定义IP安全策略	111

6.5	防黑实战2——锁定电脑中的隐私磁盘	115
-----	-------------------------	-----

第7天 星期二

IE浏览器攻防策略

 (7月30日 星期二)

116

7.1	常见的IE浏览器攻击方式	117	7.1.7	篡改IE浏览器默认的搜索引擎	126
7.1.1	篡改IE浏览器首页	117	7.1.8	桌面上的IE浏览器图标“不见”了	126
7.1.2	恶意更改IE浏览器标题栏	119	7.2	通过权限设置保护IE浏览器	128
7.1.3	篡改IE浏览器的右键菜单	121	7.3	防黑实战1——在IE中设置隐私保护	129
7.1.4	禁用IE浏览器的【源文件】菜单项	122	7.4	防黑实战2——在IE浏览器窗口中屏蔽广告	131
7.1.5	网页广告信息炸弹	124			
7.1.6	IE浏览器默认的首页变成灰色且按钮不可用	125			

第8天 星期三

注册表编辑器攻防策略

 (7月31日 星期三)

132

8.1	常见注册表入侵方式	133	8.2.5	禁止更改系统登录密码 ...	139
8.1.1	连接远程注册表	133	8.2.6	隐藏控制面板中的图标 ...	140
8.1.2	利用网页改写注册表	134	8.2.7	禁止IE浏览器查看本地磁盘	140
8.2	注册表的防护	135	8.3	防黑实战1——关闭远程注册表管理服务	141
8.2.1	禁止访问和编辑注册表 ...	135	8.4	防黑实战2——只允许运行指定的程序	142
8.2.2	关闭默认共享保证系统安全	137			
8.2.3	禁止远程修改注册表	137			
8.2.4	禁止运行应用程序	138			

9.1 系统漏洞概述	145	9.4 系统漏洞防御	152
9.1.1 什么是系统漏洞	145	9.4.1 使用Windows Update为 系统打补丁	152
9.1.2 系统漏洞产生的原因	145	9.4.2 使用360安全卫士为系统 打补丁	154
9.2 黑客如何入侵系统漏洞	146	9.4.3 使用瑞星卡卡上网安全 助手	155
9.2.1 X-SCAN快速抓鸡	146	9.5 防黑实战1——WebDAV缓冲区 溢出漏洞攻击	155
9.2.2 啊D光速抓鸡	147	9.6 防黑实战2——WebDAV缓冲区 溢出攻击防御	157
9.3 经典系统漏洞实战	149		
9.3.1 IPC\$漏洞概述	149		
9.3.2 IPC\$漏洞入侵 “挂马”	150		
9.3.3 IPC\$漏洞的防御	151		

10.1 入侵计算机系统	160	10.4 利用远程控制工具进行远程 控制	171
10.1.1 通过建立隐藏账号入侵 系统	160	10.4.1 使用“魔法远程控制” 进行远程控制	171
10.1.2 通过开放的端口入侵 系统	163	10.4.2 使用“灰鸽子”实现远程 控制	173
10.2 抢救被入侵的系统	166	10.5 实时保护系统安全	177
10.2.1 揪出黑客创建的隐藏 账号	166	10.5.1 360安全卫士	177
10.2.2 关闭不必要的开放 端口	167	10.5.2 拒绝系统入侵的 防火墙	182
10.3 利用Windows系统自带的远程 协作实现远程控制	168	10.6 防黑实战1——确定可能开放的 端口服务	184
10.3.1 什么是远程控制	168	10.7 防黑实战2——使用MT工具 创建复制账号	185
10.3.2 通过Windows远程桌面 实现远程控制	169		

- 11.1 破解Windows各个账户的密码 189
 - 11.1.1 破解BIOS开机密码 189
 - 11.1.2 使用Administrator账户登录 190
 - 11.1.3 强制清除管理员密码 191
 - 11.1.4 使用软件窃取账户密码 192
 - 11.1.5 破解屏幕保护密码 193
- 11.2 加强Windows账户密码的管理... 193
 - 11.2.1 更改Administrator账户 194
 - 11.2.2 强健Windows系统管理员密码..... 195
 - 11.2.3 删除Guest账户..... 196
- 11.3 防黑实战1——判断Guest账户是否被利用..... 197
- 11.4 防黑实战2——创建密码恢复盘..... 198

- 12.1 Word文件的加密与解密..... 201
 - 12.1.1 利用Word自身功能加密 201
 - 12.1.2 Word密码查看器 202
- 12.2 Excel文件的加密与解密 203
 - 12.2.1 利用Excel自身功能加密 203
 - 12.2.2 Excel加密文档解密工具——Excel Key..... 205
- 12.3 PDF文件的加密与解密 206
 - 12.3.1 利用Adobe Acrobat professional创建并加密PDF文件 206
 - 12.3.2 使用PDF文件加密器.... 208
 - 12.3.3 PDF密码破解工具..... 210
- 12.4 文件或文件夹的加密与解密 212
 - 12.4.1 加密文件或文件夹 212
 - 12.4.2 解密文件或文件夹 213
- 12.5 防黑实战1——利用加密文件系统进行加密 214
- 12.6 防黑实战2——为WPS Office文档加密..... 215

- 13.1 忘了QQ密码怎么办..... 217
 - 13.1.1 通过QQ申诉找回密码... 217
 - 13.1.2 通过QQ密保找回
密码..... 219
- 13.2 黑客如何盗取QQ账号及密码... 220
 - 13.2.1 盗取QQ密码的方法..... 221
 - 13.2.2 使用“QQ简单盗”盗取
QQ账号与密码 221
 - 13.2.3 使用“QQ破密使者”
破解本地QQ密码 223
 - 13.2.4 使用“盗Q黑侠”盗取
QQ密码 224
- 13.3 QQ密码防护 225
 - 13.3.1 申请QQ密码保护 225
 - 13.3.2 QQ安全设置..... 228
 - 13.3.3 使用“金山密保”来
保护QQ号码..... 229
 - 13.3.4 使用“QQ令牌”来
保护QQ 230
- 13.4 QQ木马防范与清除..... 231
 - 13.4.1 防范QQ木马..... 231
 - 13.4.2 清除QQ木马..... 232
- 13.5 防黑实战1——利用QQ远程
协助 234
- 13.6 防黑实战2——在QQ群共享中
共享文件..... 236

- 14.1 MSN账号及密码攻防 238
 - 14.1.1 获取MSN账号密码..... 238
 - 14.1.2 防范MSN账号密码被
窃取..... 240
- 14.2 网银账号及密码攻防..... 242
 - 14.2.1 网银常见攻击手段 242
 - 14.2.2 网银攻击防范技巧 246
- 14.3 邮箱账号及密码攻防..... 249
 - 14.3.1 盗取邮箱密码的常用
方法..... 249
 - 14.3.2 使用“流光”盗取邮箱
密码..... 249
 - 14.3.3 重要邮箱的保护措施.... 251
 - 14.3.4 找回邮箱密码..... 251
- 14.4 网游账号及密码攻防..... 252
 - 14.4.1 用木马盗取账号的
攻防..... 253
 - 14.4.2 用远程控制方式盗取
账号的攻防 254
 - 14.4.3 利用系统漏洞盗取
账号的攻防 256
- 14.5 防黑实战1——将收到的“邮件
炸弹”标记为垃圾邮件..... 256
- 14.6 防黑实战2——个人账号为何在
网吧中容易被盗取 258

- 15.1 后门是什么..... 262
- 15.2 账号后门..... 262
 - 15.2.1 手动克隆账号..... 262
 - 15.2.2 在命令行方式下制作账号后门..... 266
 - 15.2.3 利用程序克隆账号..... 267
- 15.3 漏洞后门..... 269
 - 15.3.1 制造Unicode漏洞后门..... 269
 - 15.3.2 制造.idq后门..... 270
- 15.4 系统服务后门..... 271
 - 15.4.1 利用instsrv创建Telnet后门..... 271
 - 15.4.2 利用SRVINSTW创建系统服务后门..... 272
- 15.5 木马后门..... 275
 - 15.5.1 Wolf木马后门..... 275
 - 15.5.2 SQL后门..... 276
- 15.6 防黑实战1——利用系统漏洞自动加载后门..... 277
- 15.7 防黑实战2——删除各种脚本对象以禁止asp木马运行..... 279

第**4**周

黑客攻防策略

- 16.1 网站基础知识..... 283
 - 16.1.1 网站的维护与安全..... 283
 - 16.1.2 常见网站攻击方式..... 284
- 16.2 网站数据安全策略..... 285
 - 16.2.1 备份网站..... 286
 - 16.2.2 恢复被黑客攻击网站..... 287
- 16.3 网站数据库安全策略..... 288
 - 16.3.1 备份数据库 (Sql Server)..... 288
 - 16.3.2 恢复数据库 (Sql Server)..... 291
- 16.4 防黑实战1——查看网站的流量..... 293
- 16.5 防黑实战2——设置网站访问权限..... 295

- 17.1 恶意网页代码概述..... 297
 - 17.1.1 恶意代码概述..... 297
 - 17.1.2 恶意代码的特征 297
 - 17.1.3 恶意代码的传播方式 297
 - 17.1.4 网页恶意代码脚本 297
- 17.2 常见恶意网页代码攻击及解决方法 299
 - 17.2.1 启动时自动弹出对话框和网页 299
 - 17.2.2 禁用注册表 300
 - 17.2.3 网页广告信息炸弹 300
 - 17.2.4 IE部分设置被禁止 302
 - 17.2.5 定时弹出IE窗口 302
 - 17.2.6 禁止电脑功能..... 303
 - 17.2.7 格式化硬盘..... 303
 - 17.2.8 下载木马程序..... 303
- 17.3 恶意网页代码的预防和清除 303
 - 17.3.1 恶意网页代码的预防..... 303
 - 17.3.2 恶意网页代码的清除..... 304
- 17.4 防黑实战1——论坛被点歌网站攻击的原因..... 305
- 17.5 防黑实战2——论坛被恶意网站攻击的原因..... 307

- 18.1 常见木马攻击系统 310
 - 18.1.1 使用“网络公牛”木马攻击..... 310
 - 18.1.2 使用“网络精灵”木马攻击..... 312
- 18.2 清除系统中的木马 314
 - 18.2.1 使用木马清除大师清除木马..... 314
 - 18.2.2 使用“木马克星”清除木马..... 316
 - 18.2.3 用木马清除专家清除木马..... 317
- 18.3 病毒的防御 320
 - 18.3.1 U盘病毒的防御 321
 - 18.3.2 邮箱病毒的防御 323

18.3.3 未知病毒木马的 防御.....	325
---------------------------	-----

18.4 防黑实战——通过修改文件的 关联性预防病毒	327
-------------------------------------	-----

第19天 星期四

数据安全攻防策略

 (8月15日 星期四)

329

19.1 彻底销毁机密数据	330	19.2.4 使用Easy Recovery 恢复数据	336
19.1.1 暂时删除文件或 文件夹	330	19.3 网络数据安全策略	341
19.1.2 彻底删除文件或 文件夹	331	19.3.1 加密网络聊天数据	341
19.1.3 使用360安全卫士粉碎 机密数据	331	19.3.2 备份个人网络数据	342
19.2 恢复被误删除的数据	332	19.3.3 上传与下载网络数据	343
19.2.1 恢复删除的数据应 注意的事项	332	19.3.4 网络用户信息的安全 策略	345
19.2.2 从回收站中还原	333	19.4 防黑实战1——查看并备份QQ 聊天记录	347
19.2.3 清空回收站后的恢复	334	19.5 防黑实战2——防止本机数据库 文件被下载	347

第20天 星期五

黑客痕迹清除技法

 (8月16日 星期五)

350

20.1 黑客留下的足迹——日志	351	20.2.3 利用工具清除日志 文件	357
20.1.1 日志的详细定义	351	20.3 防黑实战1——清除WWW和 FTP日志	360
20.1.2 为什么要清除日志	352	20.4 防黑实战2——使用批处理清除 远程主机日志	362
20.2 清除日志文件	352		
20.2.1 分析入侵日志	352		
20.2.2 手工清除日志文件	356		



21.1 关卡型黑客游戏测评.....	365	21.2 任务型黑客游戏测评.....	366
21.1.1 黑客榜中榜.....	365	21.2.1 UPLINK	366
21.1.2 PCSEC' Game	365	21.2.2 Hack TheGame.....	368
21.1.3 Monyer (梦之光芒) ..	365		