

新阅文化 李阳 田其壮 张明真 编著

黑客攻防

从入门到精通



超值赠送

Windows系统常用快捷键大全 / Windows文件管理手册
Windows硬件管理手册 / Windows系统安全与维护手册

 扫码看视频（扫描目录最后一页的二维码）



中国工信出版集团



人民邮电出版社
POSTS & TELECOM PRESS

ATTACK

网络安全(一) 网络攻防入门

本书是“网络安全(一) 网络攻防入门”系列丛书中的一本，旨在帮助读者了解网络攻防的基本概念、原理和方法。本书内容全面、重点突出、图文并茂、通俗易懂，可作为网络安全专业及相关专业的教材，也可供从事网络安全工作的工程技术人员参考。

新闻文化 李阳 田其壮 张明真 编著

黑客攻防

从入门到精通



本书是“网络安全(一) 网络攻防入门”系列丛书中的一本，旨在帮助读者了解网络攻防的基本概念、原理和方法。本书内容全面、重点突出、图文并茂、通俗易懂，可作为网络安全专业及相关专业的教材，也可供从事网络安全工作的工程技术人员参考。

人民邮电出版社

北京

DEFENSE

图书在版编目(CIP)数据

黑客攻防从入门到精通 / 李阳, 田其壮, 张明真
编著. — 北京: 人民邮电出版社, 2018. 5
ISBN 978-7-115-47956-3

I. ①黑… II. ①李… ②田… ③张… III. ①黑客—
网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2018)第051458号

内 容 提 要

本书主要介绍和分析与黑客攻防相关的基础知识。全书由浅入深地讲解了包括黑客攻防前的准备工作、扫描与嗅探攻防、系统漏洞攻防、密码攻防、病毒攻防和木马攻防等内容。通过对本书的学习,读者在了解黑客入侵攻击的原理和工具后,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。

本书实例丰富,可作为广大初、中级用户自学计算机黑客知识的参考用书。另外,本书知识全面,内容安排合理,也可作为高等院校相关专业的教材使用。

-
- ◆ 编 著 新闻文化 李 阳 田其壮 张明真
责任编辑 李永涛
责任印制 马振武
 - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
三河市君旺印务有限公司印刷
 - ◆ 开本: 787×1092 1/16
印张: 20.5
字数: 406千字
印数: 1—4000册
- 2018年5月第1版
2018年5月河北第1次印刷

定价: 49.80元

读者服务热线: (010)81055410 印装质量热线: (010)81055316
反盗版热线: (010)81055315
广告经营许可证: 京东工商广登字 20170147号



第 1 章 揭开黑客的神秘面纱 13

1.1 认识黑客.....	14	1.2.3 设置本机 IP 地址.....	19
1.1.1 黑客的过去、现在与未来.....	14	1.3 进程与端口基础.....	21
1.1.2 黑客基础术语.....	15	1.3.1 认识进程.....	21
1.1.3 常见的黑客攻击目标.....	18	1.3.2 进程基础操作.....	21
1.2 IP 地址.....	18	1.3.3 端口概述.....	23
1.2.1 IP 地址概述.....	19	1.3.4 查看端口.....	23
1.2.2 IP 地址分类.....	19		

第 2 章 黑客常用的命令 24

2.1 Windows 命令行常用操作.....	25	2.2.3 net 命令.....	30
2.1.1 启动 Windows 系统命令.....	25	2.2.4 telnet 命令.....	31
2.1.2 复制与粘贴命令行.....	25	2.2.5 ftp 命令.....	32
2.1.3 窗口基础设置.....	25	2.3 其他命令.....	32
2.2 常用网络命令.....	26	2.3.1 arp 命令.....	32
2.2.1 ping 命令.....	27	2.3.2 traceroute 命令.....	33
2.2.2 netstat 命令.....	29	2.3.3 route 命令.....	34



第3章 扫描与嗅探工具 36

3.1 黑客“踩点”	37	3.2.2 nmap 扫描器	40
3.1.1 黑客“踩点”概述	37	3.2.3 N-Stalker 扫描工具	42
3.1.2 黑客“踩点”的方式	37	3.3 常见的嗅探工具	45
3.1.3 whois 域名查询	37	3.3.1 嗅探概述	45
3.1.4 DNS 查询	38	3.3.2 SRSSniffer 嗅探工具	46
3.2 常见的扫描工具	39	3.3.3 影音嗅探器	47
3.2.1 扫描概述	39	3.3.4 嗅探防范	49

第4章 远程控制技术..... 50

4.1 认识远程控制技术.....	51	优缺点	56
4.1.1 何为远程控制技术	51	4.3 TeamViewer 的配置与使用	56
4.1.2 远程控制的技术原理	51	4.3.1 了解 TeamViewer	56
4.1.3 远程控制与远程协助的区别	51	4.3.2 TeamViewer 的配置	56
4.1.4 远程控制技术应用领域	52	4.3.3 TeamViewer 的使用	57
4.2 Windows 系统的远程桌面连接	53	4.3.4 多模式远程使用	59
4.2.1 远程桌面前的准备	53	4.3.5 TeamViewer 的“利器”——	
4.2.2 远程桌面系统的启动及配置	53	视频会议	63
4.2.3 Windows 远程桌面连接的			

第5章 密码安全防护..... 65

5.1 信息的加密与解密.....	66	5.3 文档、文件的加密.....	74
5.1.1 认识加密与解密	66	5.3.1 Word 文档加密	74
5.1.2 破解密码的常见方法	66	5.3.2 Excel 文档加密	75
5.1.3 设置高安全系数的密码	67	5.3.3 WinRAR 加密文件	76
5.2 系统密码攻防.....	68	5.4 常用的加密、解密工具	77
5.2.1 设置 Windows 账户密码	68	5.4.1 BitLocker 加密磁盘	77
5.2.2 设置屏幕保护密码	69	5.4.2 “加密精灵”工具	79
5.2.3 设置 BIOS 密码	71	5.4.3 AORP 文档破解工具	81
5.2.4 设定 Windows 密码重置盘	72	5.4.4 ARCHPR RAR 破解工具	82

第 6 章 系统漏洞防护与注册表防护 84

- 6.1 认识系统漏洞 85
 - 6.1.1 系统漏洞的概念 85
 - 6.1.2 系统漏洞的类型 86
- 6.2 系统漏洞防范策略 88
 - 6.2.1 Windows Update 更新系统 88
 - 6.2.2 启用 Windows 防火墙 90
 - 6.2.3 EFS 加密文件系统 91
 - 6.2.4 软件更新漏洞 91
- 6.3 注册表防范策略 93
 - 6.3.1 注册表的作用 93
 - 6.3.2 禁止使用注册表编辑器 94
 - 6.3.3 使用计算机安全软件禁止修改注册表 96
 - 6.3.4 关闭 Windows 远程注册表服务 99
 - 6.3.5 清理注册表垃圾 100

第 7 章 木马攻防 103

- 7.1 走近木马 104
 - 7.1.1 木马概述 104
 - 7.1.2 木马的特性 104
 - 7.1.3 木马分类 105
 - 7.1.4 木马的伪装手段 107
- 7.2 木马相关技术 109
 - 7.2.1 木马捆绑技术 109
 - 7.2.2 自解压捆绑木马 111
 - 7.2.3 木马加壳 112
- 7.3 木马的清理与防御 114
 - 7.3.1 利用沙盘运行程序 114
 - 7.3.2 PEiD 木马查壳 116
 - 7.3.3 运用木马清除大师查杀木马 116
 - 7.3.4 运用 360 查杀木马 118
 - 7.3.5 手动清除木马 120

第 8 章 防范计算机病毒 121

- 8.1 走近计算机病毒 122
 - 8.1.1 计算机病毒概述 122
 - 8.1.2 计算机病毒的特点 122
 - 8.1.3 计算机病毒的分类 123
 - 8.1.4 计算机病毒的危害 125
 - 8.1.5 制作类计算机病毒 126
- 8.2 清理与防御计算机病毒 128
 - 8.2.1 个人防范计算机病毒的措施 128
 - 8.2.2 运用杀毒软件查杀病毒 130
 - 8.2.3 开启病毒防火墙 132
- 8.3 防御新型攻击——勒索病毒 133
 - 8.3.1 走近勒索病毒 133
 - 8.3.2 破解勒索文件 134
 - 8.3.3 申请反勒索服务 138



第 9 章 浏览器安全防护 140

9.1 防范网页恶意代码..... 141	9.2.3 运用软件屏蔽广告..... 147
9.1.1 认识网页恶意代码..... 141	9.3 浏览器安全设置 148
9.1.2 修改被篡改内容..... 143	9.3.1 设置 Internet 安全级别 148
9.1.3 检测网页恶意代码..... 144	9.3.2 屏蔽网络自动完成功能..... 149
9.2 清理页面广告..... 145	9.3.3 添加受限站点..... 150
9.2.1 设置弹出窗口阻止程序..... 145	9.3.4 清除上网痕迹..... 151
9.2.2 删除网页广告..... 146	

第 10 章 局域网安全防护 153

10.1 局域网安全基础 154	10.2.2 隐藏共享文件夹..... 159
10.1.1 局域网简介..... 154	10.2.3 设置虚假描述 IP 160
10.1.2 局域网原理..... 154	10.3 局域网的防护与监控 161
10.1.3 局域网的安全隐患..... 155	10.3.1 LanSee 工具..... 161
10.2 局域网安全共享 157	10.3.2 网络特工..... 162
10.2.1 设置共享文件夹账户与 密码..... 157	10.3.3 局域网防护..... 166

第 11 章 入侵痕迹清理..... 168

11.1 系统日志..... 169	11.2.1 创建日志站点..... 173
11.1.1 系统日志概述..... 169	11.2.2 生成日志报表..... 177
11.1.2 事件查看器查看日志..... 170	11.3 清除服务器日志 179
11.1.3 注册表查看日志..... 172	11.3.1 手动删除日志..... 180
11.2 WebTrends 日志分析 173	11.3.2 批处理清除日志..... 181

第 12 章 网络代理与追踪技术..... 184

12.1 走进网络代理..... 185	12.1.1 网络代理概述..... 185
----------------------	------------------------

12.1.2 代理服务器的主要功能.....185	12.2.3 VPN 代理.....192
12.1.3 代理分类.....186	12.3 网络追踪.....192
12.2 代理操作.....187	12.3.1 网络路由追踪器.....193
12.2.1 HTTP 代理浏览器.....187	12.3.2 其他常用追踪.....193
12.2.2 SocksCap64 代理工具.....189	

第 13 章 影子系统与系统重装.....195

13.1 影子系统的使用.....196	13.2 系统重装.....198
13.1.1 影子系统概述.....196	13.2.1 OneKey Ghost 重装系统.....198
13.1.2 影子系统安装.....196	13.2.2 制作 U 盘启动盘.....199
13.1.3 影子系统模式设置.....196	13.2.3 一键重装系统.....202
13.1.4 目录迁移.....198	

第 14 章 数据的备份与恢复.....203

14.1 常见的数据备份方法.....204	系统.....212
14.1.1 数据备份概述.....204	14.2.2 使用 GHOST 备份与还原
14.1.2 Windows 系统盘备份.....204	系统.....215
14.1.3 云盘备份.....209	14.3 常用的数据恢复工具.....219
14.1.4 备份浏览器收藏夹.....210	14.3.1 利用“Recuva”恢复数据.....219
14.2 还原与备份操作系统.....212	14.3.2 运用 360 安全卫士恢复
14.2.1 使用还原点备份与还原	文件.....221

第 15 章 间谍、流氓软件的清除及系统清理.....223

15.1 间谍软件的防护与清理.....224	15.2 流氓软件的防护与清理.....229
15.1.1 间谍软件概述.....224	15.2.1 流氓软件概述.....230
15.1.2 Windows Defender 检测与 清除间谍软件.....224	15.2.2 设置禁止自动安装.....230
15.1.3 Spy Emergency 清除间谍 软件.....227	15.2.3 Combofix 清除流氓软件.....231
	15.2.4 其他应对流氓软件的措施.....232
	15.3 清理系统垃圾.....234



15.3.1 磁盘清理.....	234	15.3.3 手动删除.....	237
15.3.2 批处理脚本清理垃圾.....	235	15.3.4 专用软件清除垃圾.....	238

第 16 章 WiFi 安全防护..... 239

16.1 走近 WiFi.....	240	16.2.2 无线路由器账号管理.....	245
16.1.1 WiFi 的工作原理.....	240	16.2.3 扫描路由器安全隐患.....	246
16.1.2 WiFi 的应用领域.....	240	16.3 手机 WiFi 使用安全.....	247
16.1.3 WiFi 安全问题.....	241	16.3.1 手机 WiFi 安全防范建议.....	247
16.1.4 查询 WiFi 信息.....	242	16.3.2 “Wifi Protector”防护 WiFi 网络.....	248
16.2 无线路由器安全设置.....	243	16.3.3 手机热点安全设置.....	249
16.2.1 无线路由器的基本设置.....	243		

第 17 章 Android 操作系统与安全防护..... 251

17.1 走近 Android 操作系统.....	252	17.3.1 Android 系统安全性问题.....	261
17.1.1 Android 系统简介.....	252	17.3.2 Android 常用安全策略.....	262
17.1.2 Android 的系统特性.....	254	17.3.3 Android 数据备份.....	263
17.2 Android 刷机与 Root.....	255	17.3.4 Android 系统的加密方法.....	265
17.2.1 Android 系统刷机概述.....	255	17.4 常用的 Android 系统防御类软件....	266
17.2.2 Android 刷机操作.....	256	17.4.1 LBE 安全大师.....	267
17.2.3 Root 的原理.....	259	17.4.2 360 手机卫士.....	269
17.2.4 Root 操作.....	260	17.4.3 腾讯手机管家.....	270
17.3 Android 操作系统的安防策略.....	261		

第 18 章 iOS 操作系统与安全防护..... 271

18.1 iOS 操作系统概述.....	272	数据.....	273
18.1.1 系统架构.....	272	18.2.2 使用 iTunes 备份和恢复用户 数据.....	275
18.1.2 iOS 的系统特性.....	272	18.2.3 使用 iTunes 备份和恢复用户 数据.....	276
18.2 iOS 数据备份.....	273		
18.2.1 使用 iCloud 备份和恢复用户			

18.3 iOS 系统越狱.....	279	18.4.2 确保 Apple ID 安全.....	283
18.3.1 iOS 系统越狱概述.....	279	18.4.3 开启 Apple ID 的双重	
18.3.2 越狱的优点和缺点.....	280	认证.....	285
18.4 iOS 操作系统安全防护.....	282	18.4.4 iOS 操作系统的其他安全	
18.4.1 iOS 系统安全性问题.....	282	措施.....	288

第 19 章 社交账号与移动支付防护..... 294

19.1 QQ 安全攻防.....	295	19.2.2 冻结与解封账号.....	299
19.1.1 密保工具设定.....	295	19.2.3 丢失密码找回.....	301
19.1.2 独立密码设定.....	297	19.2.4 “腾讯手机管家”防护微信.....	302
19.1.3 QQ 安全中心软件防护.....	298	19.3 移动支付防护.....	303
19.2 微信安全防护.....	299	19.3.1 移动支付概述.....	303
19.2.1 微信安全概述.....	299	19.3.2 “支付保镖”防护.....	304

第 20 章 网络安全与社会工程学..... 306

20.1 走进社会工程学.....	307	20.2.2 组织与企业防范社工攻击	
20.1.1 社会工程学定义.....	307	策略.....	313
20.1.2 社会工程学的攻击手段.....	307	20.2.3 防范人肉搜索.....	313
20.1.3 社工库常用操作.....	309	20.2.4 识破心理骗局——	
20.2 防范社会工程学攻击.....	312	网络谣言.....	315
20.2.1 个人防范社工攻击策略.....	312		

第 21 章 远离电信诈骗..... 318

21.1 走进电信诈骗.....	319	21.2.1 个人防范电信诈骗策略.....	323
21.1.1 电信诈骗的定义.....	319	21.2.2 电信诈骗鉴定.....	324
21.1.2 电信诈骗的特点.....	319	21.2.3 欺诈拦截.....	325
21.1.3 常见的电信诈骗手段.....	320	21.2.4 举报电信诈骗.....	327
21.2 防范电信诈骗.....	323		

第1版 (2010) 第1次印刷

新闻文化 李阳 田其壮 张明真 编著

黑客攻防

从入门到精通

人民邮电出版社

北京

图书在版编目(CIP)数据

黑客攻防从入门到精通 / 李阳, 田其壮, 张明真
编著. — 北京: 人民邮电出版社, 2018.5
ISBN 978-7-115-47956-3

I. ①黑… II. ①李… ②田… ③张… III. ①黑客—
网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2018)第051458号

内 容 提 要

本书主要介绍和分析与黑客攻防相关的基础知识。全书由浅入深地讲解了包括黑客攻防前的准备工作、扫描与嗅探攻防、系统漏洞攻防、密码攻防、病毒攻防和木马攻防等内容。通过对本书的学习,读者在了解黑客入侵攻击的原理和工具后,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。

本书实例丰富,可作为广大初、中级用户自学计算机黑客知识的参考用书。另外,本书知识全面,内容安排合理,也可作为高等院校相关专业的教材使用。

-
- ◆ 编 著 新闻文化 李 阳 田其壮 张明真
责任编辑 李永涛
责任印制 马振武
 - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
三河市君旺印务有限公司印刷
 - ◆ 开本: 787×1092 1/16
印张: 20.5
字数: 406千字
印数: 1-4000册
- 2018年5月第1版
2018年5月河北第1次印刷
-

定价: 49.80元

读者服务热线: (010) 81055410 印装质量热线: (010) 81055316
反盗版热线: (010) 81055315
广告经营许可证: 京东工商广登字 20170147号



随着网络技术的飞速发展，网络已经成为个人生活与工作中获取信息的重要途径，但是随着网络带给人们生活便捷的同时，木马病毒肆虐、电信诈骗猖獗等网络安全问题也给我们个人信息及财产安全带来严重威胁。于是，构建一个良好的网络环境，对于病毒和系统漏洞做好安全防范，及时查杀病毒和修复漏洞就显得尤为重要。为了避免计算机网络遭遇恶意软件、病毒和黑客的攻击，就必须做好计算机网络安全维护和防范。

◆ 本书内容

本书主要介绍和分析与黑客攻防相关的基础知识。全书由浅入深地分析了黑客攻防有关的原理和防御手段，一共可分为四部分：第一部分主要讲述黑客入门基础与相关网络知识，第二部分主要讲述 PC 端系统及应用的安全攻防，第三部分主要讲述时下智能手机移动端的安全攻防，第四部分主要介绍社会工程学知识。

本书内容新颖，涵盖了时下热门的勒索病毒、WiFi 安全、网络谣言和电信诈骗等问题的应对方法。此外，本书还从黑客入侵防护应用角度给出了相对独立的论述，使读者可对如何建构一个实用的入侵防范体系有一个基本概念和思路。

◆ 本书特色

每章都以实例出发，讲解全面，轻松入门，快速打通初学者学习的重要关卡。真正以图来解释每一步操作过程，通俗易懂，阅读轻松。学习目的性、指向性强，黑客新技术盘点，让读者实现“先下手为强”。



◆ 读者对象

本书作为一本面向广大网络安全人员的速查手册，适合以下读者学习使用：

- (1) 网络安全及黑客技术初学者、爱好者；
- (2) 需要获取数据保护的日常办公人员；
- (3) 网吧工作人员、企业网络管理人员；
- (4) 喜欢研究黑客技术的网友；
- (5) 相关专业的学生；
- (6) 培训班学员。

本书由李阳、田其壮和张明真等人编著，书中若有疏漏和不足之处敬请广大读者批评指正，也期待读者能从本书中得到有价值的收获！

最后，提醒广大读者：根据国家有关法律法规，任何利用黑客技术攻击他人的行为都属于违法行为，广大读者在阅读本书后不要使用书中介绍的黑客技术试图对网络进行攻击，否则后果自负，切记勿忘。

编者

2018年1月



第 1 章 揭开黑客的神秘面纱 13

1.1 认识黑客..... 14	1.2.3 设置本机 IP 地址 19
1.1.1 黑客的过去、现在与未来..... 14	1.3 进程与端口基础 21
1.1.2 黑客基础术语 15	1.3.1 认识进程 21
1.1.3 常见的黑客攻击目标 18	1.3.2 进程基础操作 21
1.2 IP 地址 18	1.3.3 端口概述 23
1.2.1 IP 地址概述 19	1.3.4 查看端口 23
1.2.2 IP 地址分类 19	

第 2 章 黑客常用的命令 24

2.1 Windows 命令行常用操作 25	2.2.3 net 命令 30
2.1.1 启动 Windows 系统命令 25	2.2.4 telnet 命令 31
2.1.2 复制与粘贴命令行 25	2.2.5 ftp 命令 32
2.1.3 窗口基础设置 25	2.3 其他命令 32
2.2 常用网络命令 26	2.3.1 arp 命令 32
2.2.1 ping 命令 27	2.3.2 traceroute 命令 33
2.2.2 netstat 命令 29	2.3.3 route 命令 34



第 3 章 扫描与嗅探工具 36

3.1 黑客“踩点”.....37	3.2.2 nmap 扫描器.....40
3.1.1 黑客“踩点”概述.....37	3.2.3 N-Stalker 扫描工具.....42
3.1.2 黑客“踩点”的方式.....37	3.3 常见的嗅探工具.....45
3.1.3 whois 域名查询.....37	3.3.1 嗅探概述.....45
3.1.4 DNS 查询.....38	3.3.2 SRSniffer 嗅探工具.....46
3.2 常见的扫描工具.....39	3.3.3 影音嗅探器.....47
3.2.1 扫描概述.....39	3.3.4 嗅探防范.....49

第 4 章 远程控制技术..... 50

4.1 认识远程控制技术.....51	优缺点.....56
4.1.1 何为远程控制技术.....51	4.3 TeamViewer 的配置与使用.....56
4.1.2 远程控制的技术原理.....51	4.3.1 了解 TeamViewer.....56
4.1.3 远程控制与远程协助的区别...51	4.3.2 TeamViewer 的配置.....56
4.1.4 远程控制技术应用领域.....52	4.3.3 TeamViewer 的使用.....57
4.2 Windows 系统的远程桌面连接.....53	4.3.4 多模式远程使用.....59
4.2.1 远程桌面前的准备.....53	4.3.5 TeamViewer 的“利器”——
4.2.2 远程桌面系统的启动及配置..53	视频会议.....63
4.2.3 Windows 远程桌面连接的	

第 5 章 密码安全防护..... 65

5.1 信息的加密与解密.....66	5.3 文档、文件的加密.....74
5.1.1 认识加密与解密.....66	5.3.1 Word 文档加密.....74
5.1.2 破解密码的常见方法.....66	5.3.2 Excel 文档加密.....75
5.1.3 设置高安全系数的密码.....67	5.3.3 WinRAR 加密文件.....76
5.2 系统密码攻防.....68	5.4 常用的加密、解密工具.....77
5.2.1 设置 Windows 账户密码.....68	5.4.1 BitLocker 加密磁盘.....77
5.2.2 设置屏幕保护密码.....69	5.4.2 “加密精灵”工具.....79
5.2.3 设置 BIOS 密码.....71	5.4.3 AORP 文档破解工具.....81
5.2.4 设定 Windows 密码重置盘.....72	5.4.4 ARCHPR RAR 破解工具.....82

第 6 章 系统漏洞防护与注册表防护 84

- | | |
|-----------------------------------|----------------------------------|
| 6.1 认识系统漏洞..... 85 | 6.3 注册表防范策略..... 93 |
| 6.1.1 系统漏洞的概念..... 85 | 6.3.1 注册表的作用..... 93 |
| 6.1.2 系统漏洞的类型..... 86 | 6.3.2 禁止使用注册表编辑器..... 94 |
| 6.2 系统漏洞防范策略..... 88 | 6.3.3 使用计算机安全软件禁止修改注册表..... 96 |
| 6.2.1 Windows Update 更新系统..... 88 | 6.3.4 关闭 Windows 远程注册表服务..... 99 |
| 6.2.2 启用 Windows 防火墙..... 90 | 6.3.5 清理注册表垃圾..... 100 |
| 6.2.3 EFS 加密文件系统..... 91 | |
| 6.2.4 软件更新漏洞..... 91 | |

第 7 章 木马攻防 103

- | | |
|------------------------|-----------------------------|
| 7.1 走近木马..... 104 | 7.2.3 木马加壳..... 112 |
| 7.1.1 木马概述..... 104 | 7.3 木马的清理与防御..... 114 |
| 7.1.2 木马的特性..... 104 | 7.3.1 利用沙盘运行程序..... 114 |
| 7.1.3 木马分类..... 105 | 7.3.2 PEiD 木马查壳..... 116 |
| 7.1.4 木马的伪装手段..... 107 | 7.3.3 运用木马清除大师查杀木马..... 116 |
| 7.2 木马相关技术..... 109 | 7.3.4 运用 360 查杀木马..... 118 |
| 7.2.1 木马捆绑技术..... 109 | 7.3.5 手动清除木马..... 120 |
| 7.2.2 自解压捆绑木马..... 111 | |

第 8 章 防范计算机病毒 121

- | | |
|-------------------------|---------------------------|
| 8.1 走近计算机病毒..... 122 | 措施..... 128 |
| 8.1.1 计算机病毒概述..... 122 | 8.2.2 运用杀毒软件查杀病毒..... 130 |
| 8.1.2 计算机病毒的特点..... 122 | 8.2.3 开启病毒防火墙..... 132 |
| 8.1.3 计算机病毒的分类..... 123 | 8.3 防御新型攻击——勒索病毒..... 133 |
| 8.1.4 计算机病毒的危害..... 125 | 8.3.1 走近勒索病毒..... 133 |
| 8.1.5 制作类计算机病毒..... 126 | 8.3.2 破解勒索文件..... 134 |
| 8.2 清理与防御计算机病毒..... 128 | 8.3.3 申请反勒索服务..... 138 |
| 8.2.1 个人防范计算机病毒的 | |