

电脑防护不用愁，“非常实用”解您忧



完全外行 也能打赢 电脑攻防战

136个 本书同步高清视频
150个 电脑常见故障诊断与排除赠送视频
154个 电脑系统安装、重装与故障排除赠送视频



非常实用！ 零基础学黑客攻防 从新手到高手

(第2版)
九天科技 编著



详尽的操作步骤+精美的配图+超大容量视频讲解=助您快速掌握关键技术

全面讲解DOS/Windows下攻防技术

功能导向+实用范例：详尽步骤搭配图文解说，一步一图指导读者进行操作

内容丰富+视频教学：直观效果搭配视听教学，让你一学就会，一看就懂

新手问答+高手实操：指导新手搭配技巧点拨，让你查漏补缺，做好防护工作



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

非常实用!

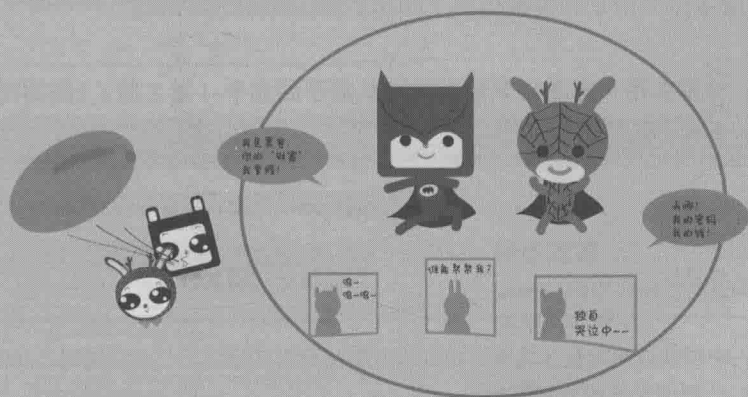
图解
视频版>

零基础学黑客攻防

(第2版)

九天科技 编著

完全外行 也能打赢 电脑攻防战



内 容 简 介

本书是指导初学者学习黑客攻防知识的入门书籍,不仅详细、全面地介绍了黑客经常使用的入侵手段和工具,还详细讲解了防御黑客攻击所必须掌握的各种方法、工具和技巧。主要内容包括:神秘黑客大曝光,黑客信息搜集、扫描与嗅探,Windows 系统漏洞攻防技术,系统安全策略设置,黑客密码攻防技术,远程控制攻防技术,黑客木马攻防技术,黑客病毒攻防技术,黑客 QQ 攻防技术,网页恶意指码攻防技术,黑客电子邮件攻防技术,黑客 U 盘病毒攻防技术,手持设备病毒攻防技术,以及网络支付工具安全防御等。

本书针对学习黑客攻防技术的初学者,适合对黑客知识有兴趣的人员进行学习和参考,同时也可作为网络操作以及网络管理等职场人员的参考用书。

图书在版编目(CIP)数据

非常实用!零基础学黑客攻防从新手到高手:图解
视频版 / 九天科技编著. — 2 版. — 北京:中国铁道
出版社, 2016. 7

ISBN 978-7-113-14233-9

I. ①非… II. ①九… III. ①计算机网络—安全技术
—图解 IV. ①TP393.08-64

中国版本图书馆 CIP 数据核字 (2016) 第 107148 号

书 名: 非常实用!零基础学黑客攻防从新手到高手(第2版)(图解视频版)
作 者: 九天科技 编著

策 划: 武文斌

读者热线电话: 010-63560056

责任编辑: 苏 茜

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(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: 2016年7月第2版

2016年7月第1次印刷

开 本: 720mm×1000mm 1/16 印张: 18.25 字数: 335千

书 号: ISBN 978-7-113-14233-9

定 价: 49.00 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

本书模块：索引、操作步骤和操作技巧



索引

指明本节操作所应用的素材、效果和视频的位置

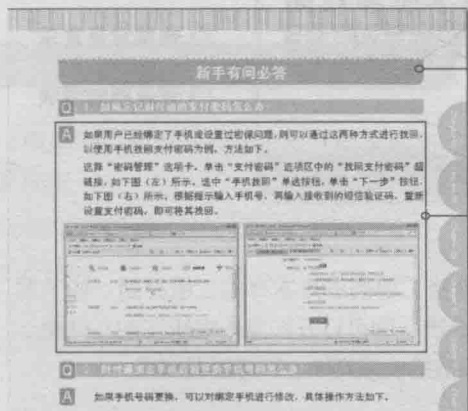
操作步骤

指明本节内容具体的操作步骤

操作技巧

指明本节操作技巧

本书提供新手有问必答，为你解答疑点难点



新手问答

指明初学者在学习过程中遇到的问题

回答

指明初学者在学习过程中遇到问题的解决方法



扫码！看视频

视频使用说明



多媒体视频的内容

本书配套的多媒体教学内容对应书中各章节的内容安排，为各章节内容的重点知识，播放时间长达500分钟。读者可以先阅读图书再浏览视频，也可以直接通过视频学习黑客攻防的相关知识。

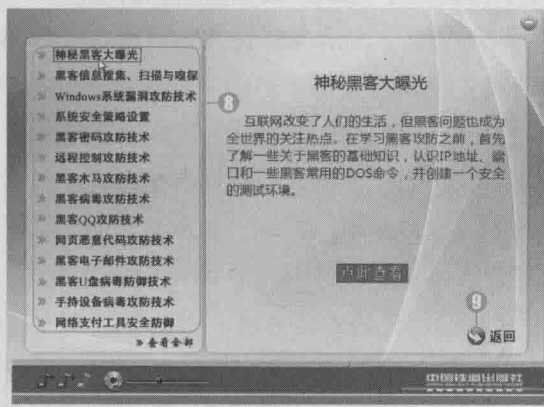
多媒体教学视频的界面

扫描二维码；或者打开链接地址 <http://upload.crphdm.com/2016/0603/1464913740732.rar>，下载压缩包文件。打开解压缩文件夹，双击 play 进入教学视频主界面。



- ① 使用帮助
- ② 视频教学
- ③ 超值赠送
- ④ 退出光盘
- ⑤ 选择背景音乐
- ⑥ 音量控制滑块

② 教学视频主界面中显示各章的链接，单击进入本章的二级界面，如下图（上）所示。单击“点此查看”超链接，即可打开视频教程所在的文件夹，如下图（下）所示。双击选择需要播放的视频文件，即可观看视频。



8 小節目录

9 返回主界面



10 双击观看视频



超值附赠视频

◎ 《电脑常见故障诊断与排除从新手到高手》视频

◎ 《电脑系统安装、重装与故障排除从新手到高手》视频

现在，黑客攻击已经成为威胁网络安全的最大隐患。黑客的攻击手段越来越“高明”，而防御黑客攻击的方法也在不断地衍变，如果你对黑客攻击和防御还比较陌生，还不了解黑客常用工具的使用方法，不会修补系统漏洞和应对漏洞攻击，对木马程序和远程监控一无所知，并且常常受到计算机病毒和木马的侵袭……那么就请静下心来阅读本书，它将引领你进入变化莫测的黑客世界。

内容导读

本书旨在帮助读者清晰地了解黑客入侵的攻击方式，进而制订出完善的防御方案，同时从另一个完全不同的角度全面解读黑客攻防，深入洞察防御的死角，组织更为严密防御体系，以应对层出不穷的入侵挑战。

本书共分为14章，其中包括：神秘黑客大曝光，黑客信息搜集、扫描与嗅探，Windows系统漏洞攻防技术，系统安全策略设置，黑客密码攻防技术，远程控制攻防技术，黑客木马攻防技术，黑客病毒攻防技术，黑客QQ攻防技术，网页恶意代码攻防技术，黑客电子邮件攻防技术，黑客U盘病毒攻防技术，手持设备病毒攻防技术，以及网络支付工具安全防御等。

主要特色

本书由业内资深信息安全专家精心策划与编写，其主要特色如下：

◎ 零基础、入门级的讲解

无论你是否从事电脑行业，无论你是否接触过网络，无论你以前是否了解黑客攻防技术，都能从本书中找到最佳起点，开始黑客攻防的学习历程。

◎ 重实战、案例化的体例

本书侧重实战技能，抛弃晦涩难懂的技术理论，基于实际案例的分析和操作指导，让读者学习起来更加轻松，操作起来有章可循。

◎ 传授实操经验精华

在本书中穿插了大量黑客攻防提示与技巧，在每章最后均设有“新手有问必答”和“高手实操技巧”两大版块，真正帮助读者解决在学习和工作中遇到的各种难题。

FOREWORD

◎ 清新的阅读环境

本书不像传统图书那样枯燥死板，而是深入考虑读者需求，版式设计清新、典雅，内容全面、实用，就像一位贴心的老师一样在你面前将各种黑客攻防知识娓娓道来。

◎ 视听光盘辅助学习

为了增加读者的学习渠道，增强读者的学习兴趣，本书配有超大容量多媒体视听教学视频，读者可以跟着提供的语音视频进行实战演练，并能快速应用于实际工作中。

教学视频说明

本书随书配有交互式、500分钟超长播放的多媒体视听教学视频，它是与图书完美结合的视听课堂，让你像看电视一样轻松、直观地进行学习。

教学视频中超值赠送本社出版的《电脑常见故障诊断与排除从新手到高手》和《电脑系统安装、重装与故障排除从新手到高手》的视频教程，超大容量，物超所值。

教学视频下载地址：<http://upload.crphdm.com/2016/0603/1464913740732.rar>

适用读者

本书针对有意学习黑客攻防技术的初学者，适合各行各业对黑客知识有兴趣的人员进行学习和参考，同时也可作为网络操作以及网络管理等职场人员的参考用书。

售后服务

如果读者在使用本书的过程中遇到问题或者有好的意见或建议，可以通过发送电子邮件（E-mail: jtbooks@126.com）或者在线QQ: 843688388联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

特别提醒

根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术攻击他人电脑，否则后果自负，特此声明！

目录

CONTENTS

第1章 神秘黑客大曝光 1

- 1.1 认识神秘的黑客 2
- 1.2 黑客定位依据——IP地址 3
 - 1.2.1 IP地址的表示方法 3
 - 1.2.2 IP地址的分类 3
- 1.3 黑客的专用通道——端口 5
 - 1.3.1 端口的分类 5
 - 1.3.2 查看系统的开放端口 7
 - 1.3.3 关闭不必要的端口 8
 - 1.3.4 限制访问指定的端口 9
- 1.4 黑客藏匿的首选地——系统进程 13
 - 1.4.1 认识系统进程 13
 - 1.4.2 关闭和新建系统进程 13
- 1.5 黑客常用的DOS命令 15
 - 1.5.1 ping命令 15
 - 1.5.2 net命令 17
 - 1.5.3 netstat命令 21
 - 1.5.4 ftp命令 22
 - 1.5.5 telnet命令 24
 - 1.5.6 ipconfig命令 24
- 1.6 安装与使用虚拟机 25
 - 1.6.1 认识虚拟机 25
 - 1.6.2 安装虚拟机 25
 - 1.6.3 创建虚拟机 27
 - 1.6.4 在虚拟机中安装操作系统 30

新手有问必答

- 1. 如何使用DOS命令快速查看磁盘内容? 33
- 2. 为什么任务管理器只显示系统进程, 标题栏、菜单栏和选项卡都不显示? 34

高手实操技巧

- 1. 查看ping命令的更多用法 34
- 2. net share命令无效的解决办法 34
- 3. 不知道局域网内对方的计算机名时查看共享资源的办法 34

第2章 黑客信息搜集、扫描与嗅探 35

- 2.1 搜集目标的重要信息 36
 - 2.1.1 确定目标的IP地址 36
 - 2.1.2 查看目标所属地区 36
- 2.2 认识扫描器 37
 - 2.2.1 扫描器的工作原理 37
 - 2.2.2 扫描器的作用 37
- 2.3 端口扫描器的应用 38
 - 2.3.1 Nmap扫描器 38
 - 2.3.2 SuperScan扫描器 41
- 2.4 多功能扫描器的应用 44
 - 2.4.1 流光扫描器 44
 - 2.4.2 SSS扫描器 48
 - 2.4.3 X-Scan扫描器 53



2.5 网络嗅探工具的应用	54	2.5.2 嗅探利器SmartSniff.....	55
2.5.1 认识嗅探的原理	54	2.5.3 网络数据包嗅探专家	56
		2.5.4 影音神探	57

新手 有问 必答

1. 如何查看网站的备案信息?	58
2. 嗅探可以做什么? 为什么需要嗅探?	59

高手 实操 技巧

1. Nmap扫描技巧	59
2. SSS扫描器提供的扫描方式	59
3. 使用nslookup命令查询IP地址	59

第3章 Windows系统漏洞攻防技术

60

3.1 认识系统漏洞	61	3.4 系统漏洞的监测与修复	69
3.1.1 系统漏洞是什么	61	3.4.1 利用Windows自动更新 软件.....	69
3.1.2 系统漏洞产生的原因	61	3.4.2 使用360安全卫士	70
3.2 Windows XP系统存在的 系统漏洞	62	3.4.3 使用瑞星安全助手	72
3.3 Windows 7系统存在的 系统漏洞	68	3.4.4 使用金山卫士	72

新手 有问 必答

1. 在Windows XP系统下如何设置自动更新?	73
2. 系统漏洞补丁为什么安装不上?	74

高手 实操 技巧

1. 微软停止Windows XP支持和服务后对用户使用的影	74
2. Windows XP系统下不自动更新漏洞	74
3. 手动更新系统漏洞	74

第4章 系统安全策略设置

75

4.1 设置本地安全策略	76	4.1.2 不显示上次登录时的 用户名.....	77
4.1.1 禁止在登录前关机	76		



CONTENTS

4.1.3 限制格式化和弹出 可移动媒体.....77	4.2.6 禁止访问控制面板.....88
4.1.4 对备份和还原权限进行 审计.....78	4.2.7 禁止更改“开始”菜单.....88
4.1.5 禁止在下次更改密码时存 储LAN管理器哈希值.....78	4.2.8 禁止更改桌面设置.....89
4.1.6 设置本地账户共享与 安全模式.....79	4.2.9 禁止访问指定的磁盘 驱动器.....90
4.1.7 不允许SAM账户和共享 的匿名枚举.....79	4.2.10 禁用部分应用程序.....90
4.1.8 将Everyone权限应用于 匿名用户.....80	
4.1.9 定义IP安全策略.....81	
4.2 设置本地组策略.....84	4.3 设置计算机管理策略.....92
4.2.1 设置账户锁定策略.....84	4.3.1 事件查看器的使用.....92
4.2.2 设置密码策略.....85	4.3.2 共享资源的管理.....93
4.2.3 设置用户权限.....85	4.3.3 管理系统中的服务程序.....94
4.2.4 更改系统默认的管理员 账户.....87	4.4 注册表编辑器安全设置.....95
4.2.5 不允许SAM账户的匿名 枚举.....87	4.4.1 禁止访问和编辑注册表.....95
	4.4.2 禁止远程修改注册表.....98
	4.4.3 禁止运行应用程序.....98
	4.4.4 禁止更改系统登录密码.....99
	4.4.5 隐藏控制面板中的图标.....100
	4.4.6 禁止IE浏览器查看本地 磁盘.....101
	4.4.7 关闭默认共享.....101

新手 有问 必答

1. 在安装软件时为什么提示“系统管理员设置了系统策略，禁止进行此项安装”？.....102
2. 注册表被修改后如何恢复之前的参数？.....103

高手 实操 技巧

1. 恢复显示控制面板中的图标.....103
2. 高级共享设置.....103
3. 恢复禁用的注册表编辑器.....103

第5章 黑客密码攻防技术.....104

5.1 为系统加密.....105	5.2.1 为Word文档加密.....107
5.1.1 设置CMOS开机密码.....105	5.2.2 为Excel表格加密.....108
5.1.2 设置系统启动密码.....106	5.2.3 为WPS Office文档加密.....108
5.2 为文件加密.....107	5.2.4 为电子邮件加密.....109
	5.2.5 为压缩文件加密.....110



5.3 使用加密软件加密 111

- 5.3.1 文本文件专用加密器 111
- 5.3.2 文件夹加密精灵 113
- 5.3.3 终极程序加密器 114
- 5.3.4 万能加密器 115

管理员账户 119

- 5.4.1 使用Administrator账户登录 119
- 5.4.2 强制清除管理员密码 120
- 5.4.3 创建密码重设盘 121
- 5.4.4 使用密码恢复软件 122

5.4 破解Windows XP系统

新手 有问 必答

- 1. Administrator账户名称太长, 如何对其进行重命名操作? 123
- 2. 如何破解常用办公软件的密码? 123
- 3. 如何破解ADSL密码? 124

高手 实操 技巧

- 1. 强制解除COMS密码 124
- 2. 使用密码重设盘找回密码 124
- 3. net user命令使用限制 124

第 6 章 远程控制攻防技术 125

6.1 基于认证入侵 126

- 6.1.1 IPC\$入侵与防范 126
- 6.1.2 Telnet入侵 132

6.2 通过注册表入侵 135

- 6.2.1 开启远程注册表服务 135
- 6.2.2 修改注册表实现远程监控 136

6.3 远程桌面控制 137

- 6.3.1 Windows 7远程协助 137
- 6.3.2 Windows 7远程关机 138

6.4 使用网络执法官 140

- 6.4.1 网络执法官的功能 140
- 6.4.2 认识网络执法官操作界面 141
- 6.4.3 网络执法官的应用 142

6.5 使用远程控制软件 144

- 6.5.1 网络人 (Netman) 的功能 144
- 6.5.2 网络人 (Netman) 的使用 144

新手 有问 必答

- 1. 在建立和断开IPC\$连接时, 输入的命令代表什么意思? 146
- 2. 如何快速打开“网络和共享中心”窗口? 146



CONTENTS

高手 实操 技巧

1. 远程控制和远程唤醒的区别 147
2. 关闭Windows XP默认共享 147
3. 修改远程计算机上的注册表项 147

第7章 黑客木马攻防技术 148

7.1 木马基础知识 149

- 7.1.1 认识木马及其结构 149
- 7.1.2 木马的分类 150
- 7.1.3 木马的特点 152
- 7.1.4 木马的入侵和启动 153
- 7.1.5 木马的伪装手段 155

7.2 木马的制作 157

- 7.2.1 使用“EXE捆绑机”
捆绑木马 157
- 7.2.2 自解压木马 158
- 7.2.3 CHM电子书木马 160

7.3 木马的清除与防范 163

- 7.3.1 木马清道夫清除木马 163
- 7.3.2 木马克星Iparmor清除
木马 167

7.3.3 金山贝壳木马专杀清除 木马 168

7.3.4 手动查杀系统中的 隐藏木马 168

7.3.5 常见木马防范措施 169

7.4 “广外女生”木马的使用 与清除 172

7.4.1 “广外女生”木马的 使用 172

7.4.2 “广外女生”木马的 清除 173

7.5 “新鬼影”木马的清除 174

7.5.1 认识“新鬼影”木马 174

7.5.2 清除“新鬼影”木马 174

7.6 “支付大盗”木马的攻击 手法 176

新手 有问 必答

1. 使用捆绑机捆绑文件后，再次运行文件有什么区别？ 177
2. 如何轻松识别木马程序？ 177

高手 实操 技巧

1. 防止CHM木马在本地运行 177
2. 在制作CHM电子书木马编写网页代码时更改木马运行时间 177
3. 设置“冰河”木马随着被攻击计算机系统一起启动 177



第8章 黑客病毒攻防技术 178

8.1 认识计算机病毒 179

8.1.1 计算机病毒的特征 179

8.1.2 计算机病毒常见的传播途径 180

8.1.3 计算机中毒后的常见症状 180

8.2 学会制作简单病毒 181

8.3 预防和查杀计算机病毒 185

8.3.1 掌握防范病毒的常用措施 185

8.3.2 使用杀毒软件查杀病毒 186

新手有问必答

1. 当计算机经常死机时，是否表示计算机一定中了病毒？ 193
2. 如何设置卡巴斯基在计算机启动时是自动运行？ 193

高手实操技巧

1. 使用Norton AntiVirus对计算机进行网络防护 194
2. 使用卡巴斯基进行系统优化 194

第9章 黑客QQ攻防技术 195

9.1 黑客攻击QQ常用的方式 196

9.1.1 向指定QQ发送炸弹 196

9.1.2 破解本地QQ的密码 197

9.2 盗取QQ密码——阿拉QQ密码潜伏者 198

9.3 黑客远程攻击——QQ细胞发送器 199

9.4 查看聊天记录——暗夜QQ聊天记录查看器 200

9.5 对自己的QQ进行保护 202

9.5.1 设置QQ密码保护 202

9.5.2 防范IP地址被探测 203

9.5.3 加密聊天记录 204

新手有问必答

1. 如何防止不认识的人加自己为好友？ 205
2. 如何设置QQ一登录就自动为“隐身”状态？ 206

高手 实操 技巧

1. QQ密保卡使用限制 206
2. 设置多个代理服务器 206
3. 使用QQ进行截图 206

第10章 网页恶意代码攻防技术 207

- 10.1 认识恶意代码 208
 - 10.1.1 恶意代码概述 208
 - 10.1.2 认识WSH 208
 - 10.1.3 恶意代码的特征 209
 - 10.1.4 非过滤性病毒 209
 - 10.1.5 恶意代码的传播方式 210
- 10.2 防范恶意代码 210
 - 10.2.1 恶意代码的预防 210
 - 10.2.2 恶意代码的清除 211
- 10.3 常见恶意代码攻防 212
 - 10.3.1 修改起始页和默认主页 212
 - 10.3.2 强行修改IE标题栏 212
 - 10.3.3 强行修改右键菜单 213
 - 10.3.4 禁用注册表 214
- 10.4 IE浏览器防护 215
 - 10.4.1 IE浏览器安全设置 215
 - 10.4.2 更新系统漏洞补丁 218
 - 10.4.3 使用“瑞星安全助手” 219

新手 有问 必答

1. 如何判断自己的计算机是否遭到了恶意网站的攻击? 224
2. 如何使用360安全卫士修复浏览器? 225

高手 实操 技巧

1. 手动选择删除浏览器临时文件 225
2. 常用的浏览器防御方法 225
3. 重装IE浏览器 225

第11章 黑客电子邮件攻防技术 227

- 11.1 认识电子邮件病毒 228
 - 11.1.1 认识电子邮件炸弹 229
 - 11.1.1.1 电子邮件炸弹的定义和危害 229
 - 11.1.2 电子邮件炸弹的制作 230
- 11.2 认识电子邮件炸弹 229
 - 11.2.1 电子邮件炸弹的定义和危害 229
- 11.3 防御电子邮件攻击 231
 - 11.3.1 重要邮箱的保护措施 231
 - 11.3.2 找回邮箱密码 232
 - 11.3.3 防止炸弹攻击 233



 11.4 防范电子邮件病毒.....	235
11.4.1 设置邮件的显示格式.....	235
11.4.2 设置Outlook Express	236

新手 有问 必答

1. 如何开通手机邮箱?	238
2. 如何添加关联邮箱?	238

高手 实操 技巧

1. 为邮箱设置安全密码的技巧.....	239
2. 发现邮箱被探测的处理方法.....	239
3. 学会使用邮件炸弹的克星.....	239

第12章 黑客U盘病毒防御技术.....240

12.1 认识U盘病毒.....	241	12.2.2 手动删除U盘病毒.....	244
12.1.1 U盘病毒的原理和特点... 241		12.2.3 U盘病毒专杀工具	
12.1.2 常见U盘病毒.....241		——USBCleaner	244
 12.2 U盘病毒的查杀.....	243	12.2.4 U盘病毒专杀工具	
12.2.1 利用WinRAR查杀U盘		——USBKiller	245
病毒.....243			

新手 有问 必答

1. 在弹出U盘时弹出提示信息框, 提示弹出时出现问题怎么办?	247
2. 计算机被U盘病毒感染时有哪些症状表现?	247
3. U盘感染病毒时有哪些症状表现?	247

高手 实操 技巧

1. 最简单判断U盘是否带有病毒的方法.....	248
2. 截断病毒的小技巧.....	248
3. 目前常用的U盘病毒专杀工具	248



CONTENTS

第13章 手持设备病毒攻防技术 249

13.1 平板电脑的病毒攻防技术 250

- 13.1.1 黑客攻击平板电脑的手法 250
- 13.1.2 iPad防黑技术 250

- 13.2.1 黑客攻击手机的手法 253
- 13.2.2 手机的防护策略 253
- 13.2.3 常见手机病毒 254
- 13.2.4 手机的防黑技术 256

13.2 手机的病毒攻防技术 253



13.3 使用360手机卫士 257

新手有问必答

- 1. 如何设置对骚扰电话或垃圾短信进行拦截? 259
- 2. 在手机上如何快速卸载安装的软件? 259

高手实操技巧

- 1. 固件强制升级 260
- 2. iPad平板电脑【开/关机】键和【Home】键的妙用 260
- 3. iPad快速静音方法 260

第14章 网络支付工具安全防御 261



14.1 防御黑客入侵支付宝 262

- 14.1.1 保障支付宝账户的安全 262
- 14.1.2 保障支付宝资金的安全 265



14.2 防御黑客入侵财付通 268

- 14.2.1 保障财付通账户的安全 268
- 14.2.2 保障财付通资金的安全 271

新手有问必答

- 1. 如果忘记财付通的支付密码怎么办? 273
- 2. 财付通绑定手机后若更换手机号码怎么办? 273

高手实操技巧

- 1. 快速进入财付通页面的方法 274
- 2. 在公共场合使用财付通后删除数字证书的方法 274