

丛书畅销

50万册

精品图书+  
多媒体互动演示+  
超值赠品=  
您的最佳选择!



入门→提高→精通→实战，助您  
从新手变成高手!



软件知识一应俱全，行业应用典  
型实用，情景再现职场案例!



内文版式温馨、典雅，阅读时倍  
感舒适、亲切!



赠送超长多媒体教学视频，便于  
教学和自学!

超值DVD

- 专为本书开发的15小时多媒体教学视频
- 模拟上机练习的互动操作系统
- 特别收录的本书学习所需的素材及源文件
- 盘中免费赠送：
  - ▶ 15小时《黑客攻防》多媒体教学演示

学电脑从入门到精通

九州书源 丛威 范晶晶 编著

新编  
黑客攻防

从入门到精通



清华大学出版社

学电脑从入门到精通

# 新编黑客攻防从入门到精通

九州书源

丛威 范晶晶 编著

清华大学出版社

北 京

## 内 容 简 介

本书以常见的黑客软件及黑客编程为主,由浅入深地讲解了使用黑客技术对电脑进行相应信息的嗅探、扫描、攻击和记录等相关知识。本书分为4篇,从黑客的定义、黑客攻击的途径开始,一步步讲解了搭建黑客测试环境、使用黑客常用工具、QQ攻击与安全指南、电子邮件攻击与防范、常见的加密与解密方式、网络攻击与防御、浏览器的攻击与防御、开启电脑后门并清除攻击痕迹、黑客编程基础知识、网络威胁的清除和防御、U盘攻击与防御、重要信息的备份和恢复、建立电脑安全防护体系等知识。本书实例丰富,包含了使用软件实现黑客攻击和编写程序获取用户信息所涉及的方方面面,可帮助读者快速上手,并将其应用到实际电脑的安全防护领域。

本书案例丰富、实用,且简单明了,可作为广大初、中级用户自学电脑黑客知识的参考用书。同时,本书知识全面,安排合理,也可作为大、中专院校相关专业的教材使用。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

### 图书在版编目(CIP)数据

新编黑客攻防从入门到精通/九州书源编著. —北京:清华大学出版社,2014  
(学电脑从入门到精通)

ISBN 978-7-302-33429-3

I. ①新… II. ①九… 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182083号



责任编辑:朱英彪 贾小红

封面设计:刘超

版式设计:文森时代

责任校对:王云

责任印制:杨艳

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质 量 反 馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 刷 者:北京鑫丰华彩印有限公司

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:190mm×260mm 印 张:24 插 页:1 字 数:584千字  
(附DVD光盘1张)

版 次:2014年1月第1版

印 次:2014年1月第1次印刷

印 数:1~5200

定 价:49.80元

产品编号:049520-01

# 多媒体光盘使用说明



→ 素材和效果文件区

**4. 调用素材或效果文件。**在演示界面中单击“素材”按钮，进入素材界面，其中提供了部分章的素材和效果文件，单击后面的“点击打开”链接，即可找到所需的文件，如图4所示。

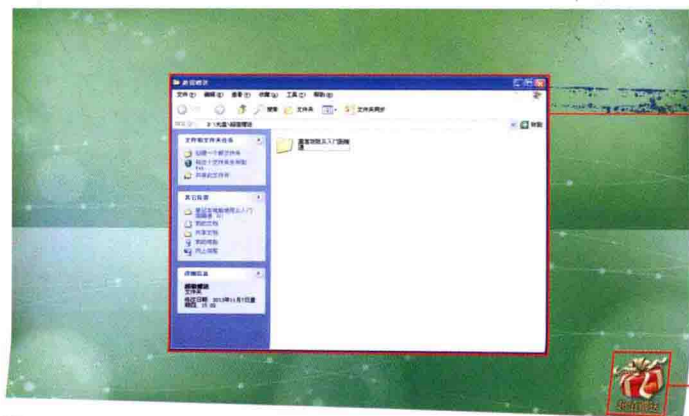
图4 素材界面



光盘使用帮助 ←

**5. 获得帮助。**单击主界面中的“帮助”按钮，将进入帮助界面。拖动右侧的滚动条，可以浏览光盘的详细使用说明，如图5所示。

图5 帮助界面



→ 打开的赠送内容界面

**6. 赠送的学习资料。**单击主界面上的“超值赠送”图标，打开超值赠送内容的界面，即可进入相应的文件夹中学习使用，如图6所示。

→ 超值赠送图标，单击此图标，进入超级赠送界面

图6 超值赠送界面

# 多媒体光盘使用说明

本书所配光盘是专业、大容量、高品质的交互式多媒体学习光盘，讲解流畅，配音标准，画面清晰，界面美观大方。本光盘操作简单，即使没有任何电脑使用经验的人也都可以轻松掌握。



光盘的主要模块按钮，可逐一单击，进入对应界面

图1 光盘主界面

**1. 运行光盘，进入光盘主界面。**将光盘放入光驱，光盘会自动运行。若不能自动运行，可在“我的电脑”窗口中双击光盘盘符，或在光盘根目录下双击Autorun.exe文件即可运行。程序运行后进入光盘主界面，如图1所示。

**2. 进入多媒体教学演示界面。**在光盘主界面中单击“目录”按钮，在出现的界面中选择相应的章节内容，即可进入多媒体教学演示界面，按照多媒体讲解进行学习，并可方便地控制整个演示流程，如图2所示。

目录菜单

功能按钮、进度条、  
调音按钮、解说字幕

教学演示界面

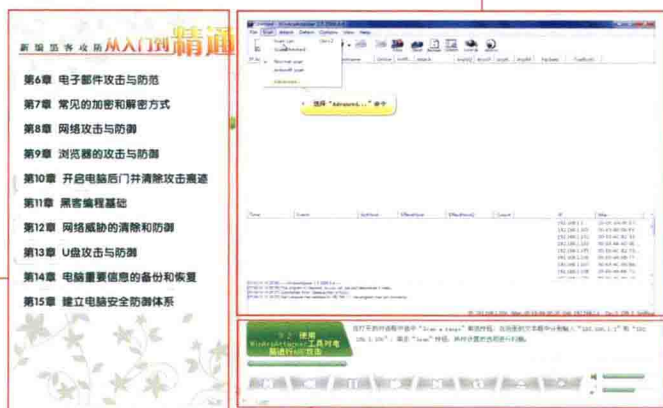


图2 多媒体教学演示界面

交互模式标志  
需操作的项目  
操作提示语言

**3. 进入交互模式界面。**在演示界面中单击“交互”按钮，进入交互模式界面。该模式提供了一个模拟操作环境，读者可按照界面上的操作提示亲自操作，可迅速提高实际动手能力，如图3所示。

图3 交互模式界面



# 前言

## PREFACE

### 本套书的故事和特点 >>>>>>>>

“学电脑从入门到精通”系列图书从2008年第1版问世，到2010年改版，共两批30余种图书，涵盖了电脑软、硬件各个领域，由于其知识丰富，讲解清晰，被广大读者口口相传，成为大家首选的电脑入门与提高类图书，并得到了广大读者的一致好评。

为了使更多的读者受益，成为这个信息化社会中的一员，为自己的工作和生活带来方便，我们对“学电脑从入门到精通”系列图书进行了第3次改版。改版后的图书将继承前两版图书的优势，并将不足的地方进行改进，将软件的版本进行更新，使其以一种全新的面貌呈现在大家面前。总体来说，新版的“学电脑从入门到精通”系列图书有如下特点：

#### ◆ 结构科学，自学、教学两不误

本套书均采用分篇的方式写作，全书分为入门篇、提高篇、精通篇和实战篇，每一篇的结构和要求均有所不同。其中入门篇和提高篇重在知识的讲解，精通篇重在技巧的学习和灵活运用，实战篇主要讲解该知识在实际工作和生活中的综合应用。除了实战篇外，每一章的最后都安排了实例和练习，以教会读者综合应用本章的知识制作实例并且进行自我练习，所以本书不管是用于自学，还是用于教学，都可以获得不错的效果。

#### ◆ 知识丰富，达到“精通”

本书的知识丰富、全面，将一个“高手”应掌握的知识有序地放在各篇中，在每一页的下方都添加了与本页相关的知识和技巧，与正文相呼应，对知识进行补充与提升。同时，除实战篇和精通篇以外的每一章最后都添加了“知识问答”和“知识关联”版块，将与本章相关的疑难点再次提问并解答，并将一些特殊的技巧教予大家，从而最大限度地提高本书的知识含量，让读者达到“精通”的程度。

#### ◆ 大量实例，更易上手

学习电脑的人都知道，多练习实例更利于学习和掌握。本书实例丰富，对于经常使用的操作我们均以实例的形式展示出来，并将实例以标题的形式列出，以方便读者快速查阅。

#### ◆ 专业分析，让您与现实工作更贴近

本书中大型综合实例除了讲解该实例的操作方法外，还讲解了与该实例相关的专业知识，如本书中15.4节讲解的实例——使用360杀毒软件实时防护，在“专业分析”中则讲解了常见杀毒软件所运用的主要技术，从而让读者真正了解这个实例“背后的故事”，增加知识面，缩小书本知识与实际工作的差距。



## 本书有哪些内容 >>>>>>>>

本书内容分为4篇、共17章，其主要内容介绍如下。

- ◆ **入门篇（第1~4章，黑客攻防的基础知识）**：主要讲解黑客的定义、黑客常用平台和命令、黑客的攻击途径、搭建黑客测试环境和使用黑客常用工具等知识。
- ◆ **提高篇（第5~10章，黑客攻防在重要领域的应用）**：主要讲解常见通信工具、重要资料、网络和IE浏览器等对象的攻击和防御知识。包括QQ攻击与安全指南、电子邮件攻击与防范、常见的加密和解密方式、网络攻击与防御、浏览器的攻击与防御、开启电脑后门并清除攻击痕迹等知识。
- ◆ **精通篇（第11~15章，使用编程进行黑客攻击和电脑的安全防护）**：主要讲解黑客编程的相关知识、重要资料的备份和防护以及电脑安全防范。包括黑客编程基础、网络威胁的清除和防御、U盘攻击与防御、电脑重要信息的备份和恢复以及建立电脑安全防护体系等知识。
- ◆ **实战篇（第16~17章，利用黑客工具以及使用电脑自带功能防御黑客攻击）**：主要讲解使用黑客工具获取电脑控制权和使用电脑自带功能防御黑客攻击等知识。

## 光盘有哪些内容 >>>>>>>>

本书配备的多媒体教学光盘，容量大，内容丰富，主要包含如下内容。

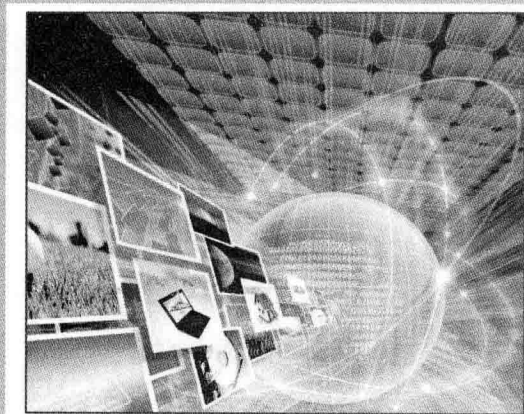
- ◆ **素材和效果文件**：光盘中包含了本书中所有实例使用的素材，以及进行操作后最后完成的效果文件，使读者可以轻松地制作出与书本相同的效果。
- ◆ **实例和练习的视频演示**：将本书所有实例和课后练习的内容以视频文件的形式显示并提供出来，这样可以使操作更加直观，学习更加有效率。

## 如何快速解决学习的疑惑 >>>>>>>>

本书由九州书源组织编写，为保证每个知识都能让读者学有所用，参与本书编写的人员在电脑书籍的编写方面都有较高的造诣。他们是丛威、范晶晶、杨学林、李星、常开忠、唐青、羊清忠、董娟娟、彭小霞、何晓琴、陈晓颖、赵云、张良瑜、张良军、宋玉霞、牟俊、李洪、贺丽娟、曾福全、汪科、宋晓均、张春梅、任亚炫、余洪、廖宵、杨明宇、刘可、李显进、付琦、刘成林、简超、林涛、张娟、程云飞、杨强、刘凡馨、向萍、杨颖、朱非、蒲涛、林科炯、阿木古堵。如果您在学习的过程中遇到什么困难或疑惑，可以联系我们，我们会尽快为您解答。联系方式是网址：<http://www.jzbooks.com>；QQ群：122144955、120241301。



# 入门篇



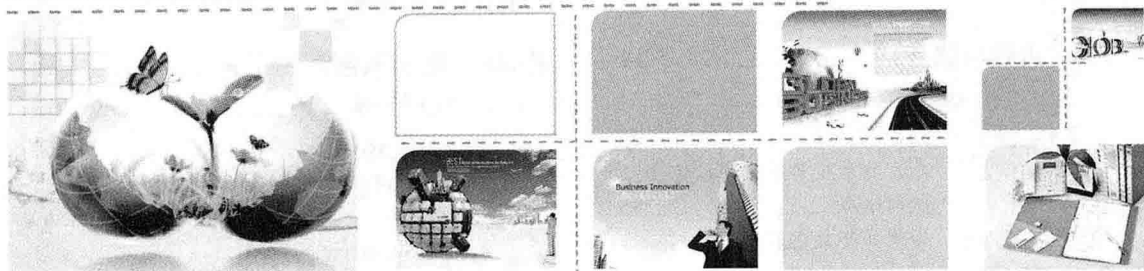
几乎每个用户都有电脑被病毒感染以及资料丢失的经历，也深深体会到了其所带来的困扰。本篇主要介绍造成这些现象的原因以及黑客的相关知识，包括认识黑客、黑客的攻击途径、搭建黑客的测试环境以及使用常见的黑客工具对电脑进行扫描等知识。



# 目录

## CONTENTS

### 入门篇



第1章 细说黑客 .....	2	实例1-4 使用tracert命令搜集百度网络的节点信息 .....	9
1.1 认识黑客 .....	3	1.3.6 ipconfig命令 .....	10
1.1.1 黑客与骇客 .....	3	实例1-5 使用ipconfig命令重新获取地址 .....	10
1.1.2 黑客攻击电脑的目的 .....	3	1.3.7 其他命令的使用 .....	11
1.1.3 黑客常用的攻击手段 .....	4	1.4 基础实例 .....	13
1.2 黑客常用平台——DOS .....	4	1.4.1 使用net start和net stop命令 .....	13
1.2.1 DOS的主要功能 .....	5	1.4.2 使用ipconfig命令 .....	15
1.2.2 DOS的组成部分 .....	5	1.5 基础练习 .....	16
1.2.3 进入DOS的操作界面 .....	6	1.5.1 使用net view命令查看用户信息 .....	16
实例1-1 通过运行命令提示符进入DOS界面 .....	6	1.5.2 使用ping命令获取新浪服务器地址 .....	17
1.3 常见黑客命令的使用 .....	6	1.6 知识问答 .....	18
1.3.1 ping命令 .....	6	第2章 黑客的攻击途径 .....	20
1.3.2 net命令 .....	7	2.1 无处不在——漏洞 .....	21
1.3.3 telnet命令 .....	8	2.1.1 认识漏洞 .....	21
实例1-2 在Windows 7中使用telnet命令 .....	8	2.1.2 常见操作系统的漏洞分析 .....	23
1.3.4 netstat命令 .....	9	2.2 权限之争——账户 .....	25
实例1-3 使用netstat命令查看电脑端口信息 .....	9	2.2.1 认识电脑账户 .....	25
1.3.5 tracert命令 .....	9		

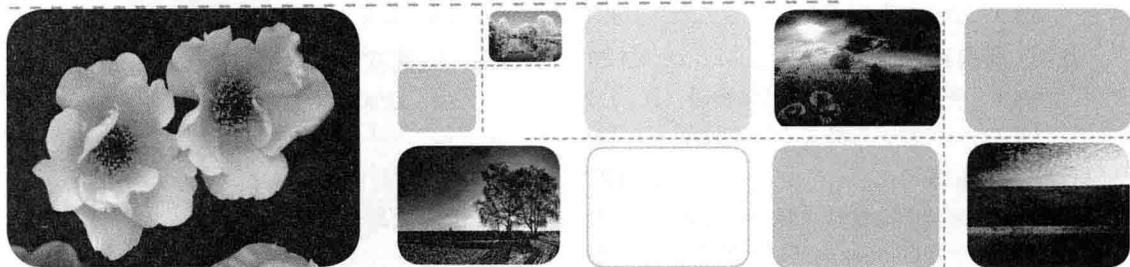


2.2.2 黑客攻击目标——管理员账户..... 25	实例3-4 将物理电脑的网络与虚拟机进行共享 ..... 54
🔍 实例2-1 将Administrator账户修改为“Tony” ..... 25	3.4 基础实例.....56
2.2.3 创建账户 ..... 26	3.4.1 配置虚拟机的硬件设置 ..... 56
🔍 实例2-2 创建账户并设置密码..... 26	3.4.2 在虚拟机中安装Windows XP..... 59
2.3 黑客通道——端口 ..... 28	3.5 基础练习.....64
2.3.1 认识端口 ..... 28	3.5.1 安装和配置VirtualBox ..... 64
2.3.2 端口的种类 ..... 29	3.5.2 在VirtualBox虚拟机中安装Windows XP ..... 65
2.3.3 关闭和限制端口 ..... 29	3.6 知识问答.....66
🔍 实例2-3 禁止其他电脑访问本地电脑的80端口 ..... 29	第4章 使用黑客常用工具.....68
2.4 进程与服务 ..... 34	4.1 使用扫描工具 ..... 69
2.4.1 认识服务和进程 ..... 34	4.1.1 X-Scan扫描器 ..... 69
2.4.2 服务和进程的操作 ..... 35	🔍 实例4-1 使用X-Scan扫描器扫描目标电脑的漏洞 ..... 69
🔍 实例2-4 开启打印服务并禁用U盘识别服务 ..... 35	4.1.2 Superscan扫描器 ..... 71
🔍 实例2-5 关闭并开启进程 ..... 37	🔍 实例4-2 使用Superscan扫描并解析目标电脑的IP地址 ..... 71
2.5 基础实例.....38	4.1.3 Nmap扫描器 ..... 72
2.5.1 创建标准账户..... 39	🔍 实例4-3 使用Nmap对局域网中的电脑进行扫描 ..... 73
2.5.2 关闭电脑打印和共享服务 ..... 41	4.2 使用注入工具 ..... 74
2.6 基础练习——创建拒绝访问端口445的IP安全规则.....43	4.2.1 Nbsi注入工具..... 74
2.7 知识问答..... 44	🔍 实例4-4 使用Nbsi检测网站漏洞和后台程序 ..... 74
第3章 搭建黑客测试环境..... 46	4.2.2 Domain注入工具..... 76
3.1 认识虚拟机 ..... 47	🔍 实例4-5 使用Domain工具扫描并修改网站后台程序 ..... 76
3.1.1 虚拟机的作用..... 47	4.3 使用嗅探工具 ..... 77
3.1.2 常见虚拟机的简介 ..... 47	4.3.1 网络嗅探器 ..... 77
3.2 准备创建虚拟系统 ..... 48	🔍 实例4-6 使用网络嗅探器嗅探网络信息 ..... 77
3.2.1 安装虚拟机软件..... 48	4.3.2 Iris嗅探器..... 79
🔍 实例3-1 安装VMware Workstation 9虚拟机..... 48	🔍 实例4-7 使用Iris嗅探器捕获网络信息 ..... 79
3.2.2 配置虚拟机 ..... 50	4.4 基础实例.....80
🔍 实例3-2 新建Windows 7虚拟机并对其进行配置 ..... 50	4.4.1 使用Nmap扫描器扫描 ..... 80
3.3 搭建Windows 7虚拟系统 ..... 52	4.4.2 使用网络嗅探器扫描文件并保存列表 ..... 83
3.3.1 安装Windows 7操作系统..... 52	
🔍 实例3-3 安装Windows 7和虚拟机工具..... 52	
3.3.2 共享网络 ..... 54	



4.5 基础练习.....	85	4.5.2 使用Domain扫描并修改后台管理项.....	86
4.5.1 使用Superscan扫描网络中的活动主机.....	86	4.6 知识问答.....	87

## 提高篇



第5章 QQ 攻击与安全指南.....	92	5.4.1 申请QQ密保.....	103
5.1 认识QQ漏洞.....	93	🔍 实例5-6 为QQ设置密保手机和密保问题.....	103
5.1.1 常见的漏洞类型.....	93	5.4.2 QQ密码的安全防护.....	104
5.1.2 修复QQ漏洞.....	93	5.4.3 使用QQ病毒查杀工具.....	105
5.2 窃取QQ密码.....	94	🔍 实例5-7 使用QQ病毒木马专杀工具.....	105
5.2.1 使用啊拉QQ大盗.....	94	5.5 提高实例.....	106
🔍 实例5-1 使用啊拉QQ大盗窃取QQ密码.....	94	5.5.1 使用广外幽灵记录程序密码.....	107
5.2.2 使用键盘记录王者窃取.....	95	5.5.2 使用QQ医生清理盗号木马.....	108
🔍 实例5-2 使用键盘记录王者窃取QQ密码.....	95	5.6 提高练习.....	109
5.2.3 使用广外幽灵窃取.....	96	5.6.1 使用键盘记录王者生成木马文件.....	110
🔍 实例5-3 使用广外幽灵窃取QQ密码.....	97	5.6.2 为QQ申请密码保护.....	110
5.3 攻击和控制QQ.....	98	5.7 知识问答.....	111
5.3.1 使用QQ狙击手获取IP地址.....	99	第6章 电子邮件攻击与防范.....	112
5.3.2 使用飘叶千夫指发送QQ信息炸弹.....	99	6.1 电子邮箱密码攻防.....	113
🔍 实例5-4 使用飘叶千夫指攻击QQ.....	99	6.1.1 使用工具窃取电子邮箱密码.....	113
5.3.3 使用微方聊天监控大师控制QQ.....	101	🔍 实例6-1 使用流光窃取新浪邮箱密码.....	113
🔍 实例5-5 使用微方聊天监控大师监控QQ聊天记录.....	101	6.1.2 找回电子邮箱密码.....	115
5.4 保护QQ安全.....	102	🔍 实例6-2 找回163免费邮箱的密码.....	115
		6.2 常见的邮箱炸弹.....	116





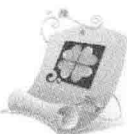
6.3 保护电子邮箱 .....	117	7.3.2 破解压缩文件密码 .....	142
6.3.1 防范电子邮件病毒 .....	117	🔍 实例7-8 使用 ARPR破解“图片” 压缩文件密码 .....	142
🔍 实例6-3 设置邮件格式和附件 防御病毒 .....	117	7.4 文件夹的加密和解密 .....	143
6.3.2 防御邮箱炸弹 .....	119	7.4.1 加密文件夹 .....	143
🔍 实例6-4 设置邮件收件规则防御 邮箱炸弹 .....	119	🔍 实例7-9 使用文件夹加密超级大师 加密“图片”文件夹 .....	143
6.3.3 防止邮件被探测 .....	121	7.4.2 解密文件夹 .....	144
6.4 提高实例 .....	121	7.5 提高实例 .....	145
6.4.1 使用流光窃取163邮箱密码 .....	122	7.5.1 破解“旅游宣传单”文档密码 .....	145
6.4.2 设置邮件以纯文本方式读取 .....	125	7.5.2 使用文件夹加密器加密“资料” 文件夹 .....	147
6.5 提高练习 .....	127	7.6 提高练习 .....	149
6.5.1 使用随机邮件炸弹攻击邮箱 .....	127	7.6.1 使用LCP破解系统SAM文件 .....	149
6.5.2 修改Outlook电子邮件的规则 .....	128	7.6.2 使用360压缩软件加密并 压缩“数据”文件夹 .....	150
6.6 知识问答 .....	128	7.7 知识问答 .....	151
第7章 常见的加密和解密方式 .....	130	第8章 网络攻击与防御 .....	152
7.1 常见办公软件的加密和解密 .....	131	8.1 局域网攻击 .....	153
7.1.1 Word文档的加密和解密 .....	131	8.1.1 局域网信息嗅探 .....	153
🔍 实例7-1 加密“市场调查报告.docx” 文档 .....	131	🔍 实例8-1 使用LanSee对所在 局域网的信息进行嗅探 .....	153
🔍 实例7-2 解密“市场调查报告.docx” 文档 .....	132	8.1.2 广播风暴 .....	154
7.1.2 Excel文档的加密和解密 .....	134	8.1.3 ARP欺骗攻击 .....	155
7.1.3 Access文档的加密和解密 .....	135	🔍 实例8-2 使用WinArpAttacker工具 对电脑进行ARP攻击 .....	155
🔍 实例7-3 加密“员工档案.accdb” 数据库文件 .....	135	8.1.4 IP地址冲突攻击 .....	156
7.2 操作系统的加密和解密 .....	136	8.2 局域网安全防御 .....	156
7.2.1 系统的常规加密 .....	137	8.2.1 广播风暴防御 .....	157
🔍 实例7-4 加密管理员账户 .....	137	8.2.2 ARP攻击防御 .....	157
7.2.2 使用U盘加密系统 .....	138	🔍 实例8-3 使用ARP防护墙 防御ARP欺骗攻击 .....	157
🔍 实例7-5 制作Windows操作系统 的U盘启动 .....	138	8.2.3 IP地址冲突防御 .....	159
7.2.3 破解系统密码 .....	139	🔍 实例8-4 修改IP地址并使用360杀毒 防御IP地址冲突 .....	159
🔍 实例7-6 使用LCP获取SAM文件中 的密码 .....	139	8.3 网络远程攻击 .....	161
7.3 压缩文件的加密和解密 .....	141	8.3.1 使用VNC实现远程攻击 .....	161
7.3.1 设置压缩文件密码 .....	141	🔍 实例8-5 安装VNC软件并 控制远程电脑 .....	161
🔍 实例7-7 压缩“图片”文件夹 并设置密码 .....	141		





8.3.2 使用Radmin实现远程攻击.....165	9.3.3 清除IE缓存.....186
🔍 实例8-6 配置Radmin软件 控制远程电脑 .....165	9.4 提高实例.....186
8.4 远程攻击防御 .....167	9.4.1 制作IE炸弹攻击浏览器 .....187
8.4.1 使用网络防火墙.....167	9.4.2 设置IE分级审查口令.....189
🔍 实例8-7 使用瑞星个人防火墙 防御远程攻击 .....167	9.5 提高练习.....190
8.4.2 关闭电脑远程功能.....168	9.5.1 使用360安全卫士修复IE 浏览器 .....191
🔍 实例8-8 关闭远程协助和 Telnet功能.....168	9.5.2 设置Internet选项保护IE 浏览器 .....191
8.5 提高实例——使用Windows 7 远程控制功能 .....169	9.6 知识问答.....192
8.5.1 操作思路 .....170	
8.5.2 操作步骤 .....170	
8.6 提高练习.....172	
8.6.1 使用WinArpAttacker扫描 局域网中的电脑信息 .....172	
8.6.2 使用Radmin进行远程控制.....173	
8.7 知识问答.....173	
第9章 浏览器的攻击与防御 .....174	
9.1 IE浏览器攻击.....175	
9.1.1 常见IE浏览器攻击方式 .....175	
9.1.2 编写网页代码攻击.....175	
9.1.3 使用万花谷病毒攻击.....176	
9.1.4 制作IE炸弹攻击.....178	
🔍 实例9-1 使用VBA病毒制造机 生成病毒 .....178	
9.2 IE程序攻防 .....180	
9.2.1 chm文件执行任意程序 .....180	
🔍 实例9-2 限制运行活动脚本.....180	
9.2.2 IE执行本地可执行文件的攻防.....181	
9.3 IE浏览器防御.....182	
9.3.1 使用安全工具维护IE浏览器.....182	
🔍 实例9-3 使用360安全卫士 修复IE浏览器.....182	
9.3.2 提升IE安全等级.....184	
🔍 实例9-4 在“Internet选项”对话框 中设置IE安全等级.....184	
	9.3.3 清除IE缓存.....186
	9.4 提高实例.....186
	9.4.1 制作IE炸弹攻击浏览器 .....187
	9.4.2 设置IE分级审查口令.....189
	9.5 提高练习.....190
	9.5.1 使用360安全卫士修复IE 浏览器 .....191
	9.5.2 设置Internet选项保护IE 浏览器 .....191
	9.6 知识问答.....192
	第10章 开启电脑后门并清除攻击 痕迹.....194
	10.1 远程开启系统后门 .....195
	10.1.1 使用WinEggDrop shell .....195
	🔍 实例10-1 使用WinEggDrop shell 开启系统后门 .....195
	10.1.2 使用Winshell .....197
	🔍 实例10-2 使用Winshell开启 系统后门 .....197
	10.2 远程开启账户后门 .....198
	🔍 实例10-3 在注册表中修改 来宾账户的权限 .....198
	10.3 远程开启服务后门 .....200
	🔍 实例10-4 使用instsrv.exe程序 创建系统服务后门 .....200
	10.4 清除攻击痕迹 .....202
	10.4.1 使用批处理文件清除痕迹 .....202
	🔍 实例10-5 使用批处理文件 清除系统日志 .....202
	10.4.2 登录远程电脑清除痕迹 .....203
	🔍 实例10-6 连接远程电脑清除 并阻止生成系统日志.....203
	🔍 实例10-7 使用DameWare清除 Event Log.....205
	10.5 提高实例.....206
	10.5.1 使用Winshell开启端口21 .....206
	10.5.2 使用clearlogs清理系统日志.....208
	10.6 提高练习.....209

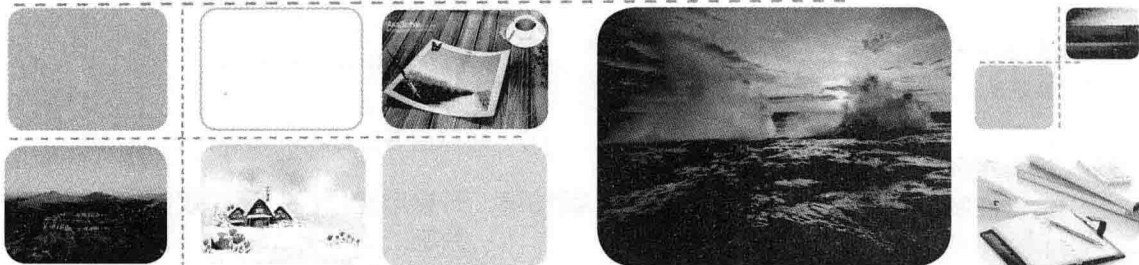




10.6.1 使用DameWare清理入侵痕迹 .....	210
-------------------------------	-----

10.6.2 清理本地电脑系统日志 .....	210
10.7 知识问答 .....	211

## 精通篇



## 第11章 黑客编程基础 .....

## 11.1 认识黑客编程 .....

11.1.1 认识编程语言 .....	215
11.1.2 使用程序攻击电脑的原理 .....	216

## 11.2 Visual C++编程简介 .....

11.2.1 认识Visual Studio编辑器 .....	217
11.2.2 Visual C++编辑器可创建的文件类型 .....	218
11.2.3 Visual C++常用名词 .....	219

## 11.3 Windows程序的结构和组成元素 .....

11.3.1 应用程序的主要内容——代码 .....	220
11.3.2 用户界面资源 .....	220
11.3.3 动态链接——库模块 .....	220
11.3.4 Windows程序源代码分析 .....	221

## 11.4 认识微软基础类库 (MFC) .....

11.4.1 MFC的分类和作用 .....	223
11.4.2 创建MFC应用程序的类 (Class) .....	227
11.4.3 创建非Document/View应用程序 .....	228

## 11.4.4 Document/View的基本原理 .....

11.4.5 创建Document/View应用程序 .....	232
----------------------------------	-----

## 11.5 常见控件的使用 .....

11.5.1 MFC常用控件 .....	237
11.5.2 控件的公共函数 .....	237
11.5.3 控件的使用 .....	238

## 11.6 定时器和通用对话框 .....

11.6.1 实现精确定时器 .....	242
11.6.2 通用对话框类——CFileDialog .....	246

## 11.7 常见的Visual C++编译错误 .....

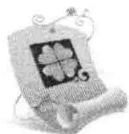
## 11.8 动态链接库——DLL .....

11.8.1 DLL的工作方式 .....	253
11.8.2 DLL的内容 .....	253
11.8.3 DLL变体 .....	254
11.8.4DllMain()函数 .....	255

## 11.9 精通实例——监视远程电脑屏幕 .....

11.9.1 专业分析 .....	256
11.9.2 操作思路 .....	256
11.9.3 操作步骤 .....	256





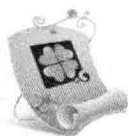
11.10 精通练习——将程序隐藏到任务栏.....	259
<b>第12章 网络威胁的清除和防御.....</b>	<b>262</b>
12.1 间谍软件的清除和防御.....	263
12.1.1 认识间谍软件.....	263
12.1.2 清除间谍软件.....	263
🔍 实例12-1 使用 SpyBot-Search & Destroy清除间谍软件.....	263
12.1.3 防御间谍软件.....	266
🔍 实例12-2 使用 Windows Defender 防御间谍软件.....	266
12.2 流氓软件的清除和防御.....	267
12.2.1 认识流氓软件.....	268
12.2.2 清除流氓软件.....	269
🔍 实例12-3 使用Windows清理助手清除流氓软件.....	269
12.2.3 防御流氓软件.....	271
🔍 实例12-4 使用Wopti防御并清除流氓软件.....	272
12.3 恶意广告的清除和防御.....	272
12.3.1 使用软件清除恶意广告.....	272
🔍 实例12-5 使用Ad Killer清除恶意广告.....	273
🔍 实例12-6 使用Anvi Ad Blocker 拦截恶意广告.....	274
12.3.2 使用浏览器拦截恶意广告.....	274
🔍 实例12-7 使用遨游浏览器拦截网页.....	274
12.4 使用HijackThis防御网络威胁.....	275
🔍 实例12-8 使用HijackThis 清除恶意程序.....	276
12.5 精通实例——使用Defendio 防御恶意软件.....	277
12.5.1 专业分析.....	278
12.5.2 操作思路.....	278
12.5.3 操作步骤.....	278
12.6 精通练习.....	281
12.6.1 使用Windows清理助手修复故障.....	281
12.6.2 使用HijackThis清除电脑中的恶意选项.....	282
<b>第13章 U盘攻击与防御.....</b>	<b>284</b>
13.1 认识U盘病毒.....	285
13.1.1 U盘病毒的工作原理和隐藏方式.....	285
13.1.2 U盘病毒的运行机制.....	286
13.1.3 U盘病毒的判断.....	287
13.2 制作U盘病毒.....	288
13.2.1 Autorun.inf文件的组成.....	288
13.2.2 AutoRun、AutoRun.Alpha和 DeviceInstall命令.....	289
13.2.3 制作Autorun.inf病毒.....	290
🔍 实例13-1 制作Autorun.inf 病毒程序.....	290
13.3 U盘病毒的防御.....	291
13.3.1 编写代码防御U盘病毒.....	291
🔍 实例13-2 编写清除和恢复 Autorun.inf的代码.....	292
13.3.2 使用软件防御U盘病毒.....	292
🔍 实例13-3 使用USBCleaner软件 对U盘进行杀毒.....	293
13.3.3 关闭系统自动播放功能.....	294
🔍 实例13-4 在组策略中关闭 自动播放功能.....	294
13.3.4 编写程序清除U盘病毒.....	295
🔍 实例13-5 编写“清理病毒” 批处理文件.....	295
13.4 U盘的维护.....	296
13.4.1 查杀U盘中的病毒.....	296
🔍 实例13-6 使用360杀毒软件 查杀U盘中的病毒.....	296
13.4.2 使用系统自带功能维护U盘.....	297
🔍 实例13-7 对U盘进行检查 和碎片整理.....	297





13.5 精通实例——使用U盘杀毒精灵 免疫U盘.....299	14.4.2 使用Ghost备份和还原.....319
13.5.1 专业分析.....299	☞ 实例14-8 使用MaxDOS软件 备份操作系统.....319
13.5.2 操作思路.....300	☞ 实例14-9 使用MaxDOS软件 还原操作系统.....321
13.5.3 操作步骤.....300	14.5 精通实例——使用魔方优化大师 保护注册表.....322
13.6 精通练习.....301	14.5.1 专业分析.....323
13.6.1 使用USBCleaner软件 扫描U盘.....302	14.5.2 操作思路.....323
13.6.2 开启360杀毒软件的U盘 防护功能.....302	14.5.3 操作步骤.....323
第14章 电脑重要信息的备份和 恢复.....304	14.6 精通练习.....325
14.1 数据的备份和恢复.....305	14.6.1 使用超级兔子备份驱动程序.....325
14.1.1 使用系统自带功能备份和还原.....305	14.6.2 使用最后一次正确配置功能.....326
☞ 实例14-1 备份“资料”文件夹.....305	第15章 建立电脑安全防御体系.....328
☞ 实例14-2 将备份在网络中的“资料” 文件夹恢复到E盘.....308	15.1 注册表和组策略安全设置.....329
14.1.2 使用FBackup备份和还原 数据.....309	15.1.1 注册表安全设置.....329
☞ 实例14-3 使用FBackup备份 “软件”文件夹.....309	☞ 实例15-1 禁止开机自动打开网页.....329
☞ 实例14-4 使用FBackup恢复 功能恢复文件.....311	☞ 实例15-2 通过注册表禁止 电脑远程修改注册表.....330
14.2 驱动程序的备份和恢复.....312	☞ 实例15-3 在注册表中删除“vmware- tray.exe”启动项.....331
14.2.1 备份驱动程序.....312	15.1.2 组策略安全设置.....331
☞ 实例14-5 使用驱动精灵备份 驱动程序.....313	☞ 实例15-4 通过组策略禁止 在电脑上使用U盘.....331
14.2.2 恢复驱动程序.....314	☞ 实例15-5 通过组策略禁止 桌面被修改.....333
☞ 实例14-6 使用驱动精灵恢复 驱动程序.....314	15.2 操作系统安全防御.....334
14.3 注册表的备份和恢复.....315	15.2.1 设置锁定电脑.....334
14.3.1 使用注册表自带功能进行 备份和恢复.....315	☞ 实例15-6 创建“锁定电脑” 快捷方式.....334
14.3.2 使用优化大师备份和恢复.....316	15.2.2 开启系统共享密码保护.....335
14.4 操作系统的备份和还原.....317	☞ 实例15-7 开启共享密码保护.....335
14.4.1 使用系统还原点.....317	15.3 使用安全防御软件.....336
☞ 实例14-7 在Windows 7中创建 并使用系统还原点.....317	15.3.1 使用杀毒软件查杀安全隐患.....336
	☞ 实例15-8 使用360杀毒软件 查杀病毒.....336
	15.3.2 使用防火墙维护系统安全.....337
	☞ 实例15-9 使用瑞星防火墙 防御电脑.....337

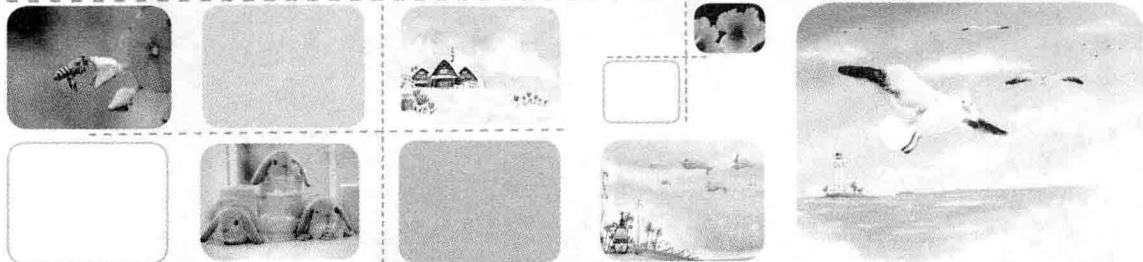




15.4 精通实例——使用360杀毒软件 实时防护.....	339
15.4.1 专业分析 .....	340
15.4.2 操作思路 .....	340

15.4.3 操作步骤 .....	341
15.5 精通练习.....	342
15.5.1 在组策略中禁用账户密码更改...342	
15.5.2 使用金山卫士防御电脑安全 .....	343

## 实战篇



第16章 利用黑客工具获取电脑 控制权 .....	346
16.1 实例说明.....	347
16.2 专业分析.....	347
16.3 操作思路.....	348
16.4 操作步骤.....	348
16.4.1 扫描网络中的主机信息 .....	348
16.4.2 生成病毒程序.....	349
16.4.3 将病毒发送到目标电脑 并运行 .....	350
16.4.4 控制目标电脑.....	351
16.5 拓展练习——利用X-Scan和VNC 扫描控制电脑 .....	354

第17章 使用电脑自带功能防御 黑客攻击 .....	356
17.1 实例说明.....	357
17.2 专业分析.....	357
17.3 操作思路.....	358
17.4 操作步骤.....	358
17.4.1 开启Windows防火墙.....	358
17.4.2 关闭远程协助功能.....	361
17.4.3 关闭共享功能.....	362
17.4.4 设置IP规则.....	364
17.5 拓展练习.....	367
17.5.1 创建“程序连接”入站规则 .....	368
17.5.2 创建“端口限制”安全策略 .....	369