

# ATTACK

在攻与防的对立统一中  
寻求技术突破

# 黑客攻防 从入门到精通

黑客与反黑工具篇 · 全新升级版

明月工作室 栾铭斌◎编著

超值赠送

黑客攻防全能视频+计算机硬件管理超级手册+Windows文件管理高级手册+Linux命令应用大全

以下人群请勿翻阅本书：

1. 自以为很牛，对黑客不屑一顾的人
2. 心存侥幸，认为黑客离自己很远的人
3. 习惯黑客攻击，总是折腾他人的人
4. 号太多，习惯被盗号的人
5. 不差钱，不怕被盗刷的人
6. 我不是Boss，对交易安全漠不关心的人

# DEFENSE



北京大学出版社  
PEKING UNIVERSITY PRESS

# ATTACK

# 黑客攻防

## 从入门到精通

黑客与反黑工具篇·全新升级版

明月工作室 栾铭斌◎编著



北京大学出版社  
PEKING UNIVERSITY PRESS

# DEFENSE

## 内 容 提 要

本书由浅入深、图文并茂地介绍了黑客攻防领域黑客与反黑工具方面的相关知识。

本书主要内容有19章,分别为走进黑客的世界、扫描工具、嗅探工具、网络追踪与代理、密码设置、破解和保护、木马攻防、QQ攻防、揭秘入侵痕迹清除技术、远程控制技术、系统漏洞与溢出问题、针对电子邮件攻击与防御、恶意网页代码攻防、局域网攻防、黑客入侵行为检测技术、揭秘黑客常用的入侵方式、系统安全防护策略、系统安全防护工具、加强网络支付工具的安全、无线网络Wi-Fi攻防。

本书语言简洁、流畅,内容丰富全面,适用于计算机中级用户、计算机维护人员、IT从业人员及对黑客攻防与网络安全维护感兴趣的计算机中级用户,各类计算机培训班也可以将其作为辅导用书。

## 图书在版编目(CIP)数据

黑客攻防从入门到精通. 黑客与反黑工具篇: 全新升级版 / 栾铭斌编著. — 北京: 北京大学出版社, 2017.2

ISBN 978-7-301-27874-1

I. ①黑… II. ①栾… III. ①黑客 - 网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2016)第313912号

书 名: 黑客攻防从入门到精通(黑客与反黑工具篇·全新升级版)

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者: 明月工作室 栾铭斌 编著

责任编辑: 尹 毅

标准书号: ISBN 978-7-301-27874-1

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> 新浪微博: @北京大学出版社

电子信箱: [pup7@pup.cn](mailto:pup7@pup.cn)

电 话: 邮购部62752015 发行部62750672 编辑部62580653

印 刷 者: 三河市博文印刷有限公司

经 销 者: 新华书店

787毫米×1092毫米 16开本 25印张 544千字

2017年2月第1版 2017年2月第1次印刷

印 数: 1-3000册

定 价: 59.00元

未经许可, 不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有, 侵权必究

举报电话: 010-62752024 电子信箱: [fd@puppkuedu.cn](mailto:fd@puppkuedu.cn)

图书如有印装质量问题, 请与出版部联系, 电话: 010-62756370

# 前言

## INTRODUCTION

### · 全新升级版

从 2003 年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，如电子商务、网络游戏、视频网站、社交娱乐等。计算机技术及通信技术的进一步发展，持续推动中国互联网新一轮的高速增长，2008 年，互联网用户已经达到 2.53 亿人，首次超过美国，跃居世界首位。

2009 年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为民众重要的消费渠道。当前，“互联网+”的战略布局与工业 4.0 的深度发展，使得国家经济发展、民众工作生活，都与网络安全休戚相关，一个安全的网络环境是必不可少的。

当前最大的一个问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就给不法分子提供了大量的机会，借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产安全带来了非常大的威胁。

为提升广大用户对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护，我们编写了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）》分册。

## 丛书书目

黑客攻防从入门到精通（全新升级版）

黑客攻防从入门到精通（Web 技术实战篇）

黑客攻防从入门到精通（Web 脚本编程篇·全新升级版）

黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）

黑客攻防从入门到精通（加密与解密篇）

黑客攻防从入门到精通（手机安全篇·全新升级版）

黑客攻防从入门到精通（应用大全篇·全新升级版）

黑客攻防从入门到精通（命令实战篇·全新升级版）

黑客攻防从入门到精通（社会工程学篇）

## 本书特点

- 内容全面：本书从计算机黑客攻防入门，到专业级的 Web 技术安全知识，适合各个层面、不同基础的读者阅读。此外，对当前移动端应用较多的 Wi-Fi、移动支付等新知识进行重点介绍和剖析。
- 与时俱进：本书主要适用于 Windows 7 及更新版本的操作系统用户阅读。尽管本书中的许多工具、案例等可以在 Windows XP 等系统下运行或使用，但为了能够顺利学习本书全部的内容，强烈建议广大读者安装 Windows 7 及更高版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行介绍，加深读者对该知识点的理解和认知能力，力争彻底掌握该知识点。
- 适合阅读：本书摒弃了大量枯燥文字叙述的编写方式，而采用了图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步、步步深入、通俗易懂、由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高。

## 读者对象

- 计算机初、中级用户。
- 网店店主、网店管理及开发人员。
- 计算机爱好者、提高者。
- 各行各业需要网络防护的人员、中小企业的网络管理员。
- Web 前、后端的开发及管理人员。
- 无线网络相关行业的从业人员。
- 计算机及网络相关的培训机构。
- 大中专院校相关学生。

## 本书结构及内容

本书共 19 章，内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

第 1 章 走进黑客的世界

第 2 章 扫描工具

第 3 章 嗅探工具

第 4 章 网络追踪与代理

第 5 章 密码设置、破解与保护

第 6 章 木马攻防

- 第 7 章 QQ 攻防
- 第 8 章 揭秘入侵痕迹清除技术
- 第 9 章 远程控制技术
- 第 10 章 系统漏洞与溢出问题
- 第 11 章 针对电子邮件攻击与防御
- 第 12 章 恶意网页代码攻防
- 第 13 章 局域网攻防
- 第 14 章 黑客入侵行为检测技术
- 第 15 章 揭秘黑客常用的入侵方式
- 第 16 章 系统安全防护策略
- 第 17 章 系统安全防护工具
- 第 18 章 加强网络支付工具的安全
- 第 19 章 无线网络 Wi-Fi 攻防



## 超值赠送资源

### 1. 黑客攻防全能视频

为了读者能全面地了解黑客方面的知识从而有效地防御黑客的不法入侵行为，本书特赠送全能教学视频，视频内容包括社会工程学、黑客攻防入门、信息的扫描与嗅探、木马与病毒的防范、系统漏洞防范、远程控制术、加密与解密、数据备份与恢复、移动网络安全等内容。

### 2. 其他赠送资源

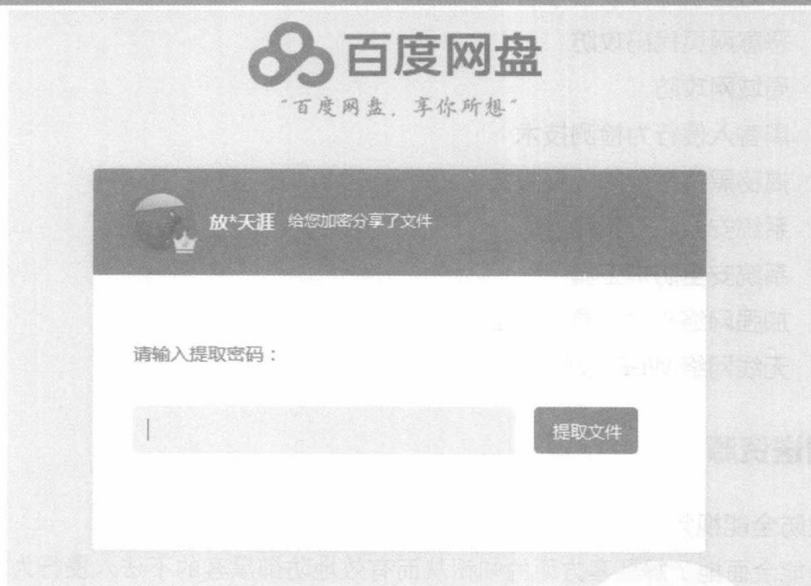
- Windows 系统安全与维护手册
- 计算机硬件管理超级手册
- Windows 文件管理高级手册
- ( 140 个 ) Windows 系统常用快捷键大全
- ( 157 个 ) Linux 基础命令手册
- ( 136 个 ) Linux 系统管理与维护命令手册
- ( 58 个 ) Linux 网络与服务器命令手册
- 黑客攻防命令手册

我们已将赠送内容上传百度网盘，在浏览器中输入下载链接，打开链接后，在如下图所示的文本框中输入提取码便可下载赠送资源。下载链接：<http://pan.baidu.com/s/1eSfvxDK>，提取码：ez6a。



### 提示

读者也可加入 QQ 群，在群文件中下载“资源下载地址列表”文档，直接复制链接和密码，下载多媒体视频。(注意：我们会在群文件中共享一些赠送资源，如百度网盘链接失效，请加入 QQ 群下载资源。)



## 后续服务

本书由栾铭斌编著，胡华、王栋、宗立波、马琳、赵玉萍、闫珊珊等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过 E-mail 或 QQ 群与我们联系。

投稿邮箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

## 郑重声明

本书对大量计算机及移动端的攻击行为进行曝光，是为了帮助广大用户，做好安全防范工作。

请广大读者注意：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都是违法的！



|                                |          |
|--------------------------------|----------|
| <b>第 1 章 走进黑客的世界.....</b>      | <b>1</b> |
| 1.1 初识黑客.....                  | 2        |
| 1.1.1 什么是黑客.....               | 2        |
| 1.1.2 什么是红客.....               | 2        |
| 1.1.3 黑客与红客的区别.....            | 2        |
| 1.2 有关 IP 地址的基础知识.....         | 2        |
| 1.2.1 认识 IP 地址.....            | 3        |
| 1.2.2 分类解析 IP 地址.....          | 4        |
| 1.3 了解端口.....                  | 5        |
| 1.3.1 各类端口详解.....              | 5        |
| 1.3.2 端口的查看.....               | 6        |
| 1.3.3 端口的开启与关闭.....            | 8        |
| 1.3.4 限制端口的步骤.....             | 10       |
| 1.4 常见的黑客术语与命令.....            | 15       |
| 1.4.1 常用的黑客术语.....             | 15       |
| 1.4.2 Ping 命令的使用.....          | 18       |
| 1.4.3 Netstat 命令的使用.....       | 20       |
| 1.4.4 Net 命令的使用.....           | 22       |
| 1.4.5 Telnet 命令.....           | 25       |
| 1.4.6 传输协议 FTP 命令.....         | 25       |
| 1.4.7 查看网络配置的 Ipconfig 命令..... | 26       |
| 1.4.8 CD 命令的使用.....            | 27       |
| 1.5 虚拟测试环境的创建.....             | 27       |
| 1.5.1 VMware 虚拟机的安装.....       | 28       |
| 1.5.2 VMware 虚拟机的配置.....       | 29       |



|                             |    |
|-----------------------------|----|
| 1.5.3 在虚拟机中安装操作系统 .....     | 31 |
| 1.5.4 安装 VMware Tools ..... | 32 |
| 技巧与问答 .....                 | 33 |

## 第2章 扫描工具..... 36

|                                     |    |
|-------------------------------------|----|
| 2.1 为什么要使用扫描工具 .....                | 37 |
| 2.2 小榕黑客字典 .....                    | 37 |
| 2.2.1 小榕黑客字典的简介 .....               | 37 |
| 2.2.2 小榕黑客字典的使用技巧 .....             | 37 |
| 2.3 弱口令扫描器 Tomcat .....             | 38 |
| 2.4 X-Scan 端口扫描器 .....              | 40 |
| 2.4.1 X-Scan 端口扫描器的简介 .....         | 40 |
| 2.4.2 X-Scan 端口扫描器的使用技巧 .....       | 40 |
| 2.5 SuperScan 扫描器 .....             | 45 |
| 2.5.1 SuperScan 扫描器的简介 .....        | 45 |
| 2.5.2 SuperScan 扫描器的使用技巧 .....      | 46 |
| 2.6 常见的扫描工具 .....                   | 48 |
| 2.6.1 Free Port Scanner 的使用技巧 ..... | 48 |
| 2.6.2 ScanPort 的使用技巧 .....          | 49 |
| 2.7 SSS 漏洞扫描器 .....                 | 50 |
| 2.7.1 SSS 漏洞扫描器的简介 .....            | 50 |
| 2.7.2 SSS 漏洞扫描器的使用技巧 .....          | 50 |
| 2.8 ProtectX .....                  | 53 |
| 2.8.1 ProtectX 的简介 .....            | 53 |
| 2.8.2 ProtecX 组件简述 .....            | 53 |
| 2.8.3 ProtectX 初始界面 .....           | 54 |
| 2.9 极速端口扫描器 .....                   | 57 |
| 2.10 S-GUI Ver 扫描器 .....            | 58 |
| 2.10.1 S-GUI Ver 扫描器的简介 .....       | 58 |
| 2.10.2 S-GUI Ver 扫描器的使用技巧 .....     | 58 |

|                                       |    |
|---------------------------------------|----|
| 2.11 网络监控的实现 .....                    | 59 |
| 2.11.1 利用“网络执法官”监控局域网 .....           | 59 |
| 2.11.2 Real Spy Monitor 监控网络的应用 ..... | 64 |
| 技巧与问答 .....                           | 69 |

### 第3章 嗅探工具.....71

|                                  |    |
|----------------------------------|----|
| 3.1 什么是嗅探器 .....                 | 72 |
| 3.2 经典嗅探器 Wireshark 的使用 .....    | 72 |
| 3.2.1 Wireshark 的使用技巧 .....      | 72 |
| 3.2.2 Wireshark 窗口介绍 .....       | 73 |
| 3.2.3 Wireshark 过滤器的使用技巧 .....   | 74 |
| 3.2.4 捕获过滤器的使用 .....             | 74 |
| 3.3 WinArpAttacker 的使用 .....     | 75 |
| 3.3.1 WinArpAttacker 的简介 .....   | 75 |
| 3.3.2 WinArpAttacker 的使用技巧 ..... | 75 |
| 3.4 影音神探嗅探在线视频地址的使用 .....        | 78 |
| 3.4.1 影音神探的简介 .....              | 78 |
| 3.4.2 影音神探的使用技巧 .....            | 78 |
| 3.5 WebSiteSniffer 的认识与使用 .....  | 82 |
| 3.5.1 WebSiteSniffer 的简介 .....   | 82 |
| 3.5.2 WebSiteSniffer 的使用技巧 ..... | 82 |
| 技巧与问答 .....                      | 84 |

### 第4章 网络追踪与代理.....86

|                                  |    |
|----------------------------------|----|
| 4.1 代理服务器——共享网络 .....            | 87 |
| 4.1.1 通过“代理猎手”寻找可用代理 .....       | 87 |
| 4.1.2 SocksCap32 设置动态代理的步骤 ..... | 92 |
| 4.1.3 防范远程跳板代理攻击的步骤 .....        | 94 |
| 4.2 黑客追踪工具——精确定位 .....           | 96 |
| 4.2.1 IP 追踪技术的应用 .....           | 96 |

|                                   |     |
|-----------------------------------|-----|
| 4.2.2 NeroTrace Pro 追踪工具的应用 ..... | 96  |
| 4.3 其他代理工具.....                   | 98  |
| 4.3.1 WaysOnline 代理工具 .....       | 98  |
| 4.3.2 遥志代理服务器.....                | 101 |
| 技巧与问答.....                        | 103 |

## 第5章 密码设置、破解与保护 ..... 105

|                          |     |
|--------------------------|-----|
| 5.1 为操作系统加密 .....        | 106 |
| 5.1.1 设置 CMOS 开机密码 ..... | 106 |
| 5.1.2 设置系统启动密码.....      | 106 |
| 5.1.3 设置屏幕保护密码.....      | 107 |
| 5.2 对文件进行加密 .....        | 108 |
| 5.2.1 为 Word 文档加密.....   | 108 |
| 5.2.2 为 Excel 表格加密 ..... | 109 |
| 5.2.3 为压缩文件加密.....       | 109 |
| 5.3 使用加密软件加密 .....       | 110 |
| 5.3.1 文本文件专用加密器.....     | 110 |
| 5.3.2 文件夹加密精灵.....       | 112 |
| 5.3.3 终极程序加密器.....       | 113 |
| 技巧与问答.....               | 115 |

## 第6章 木马攻防..... 116

|                       |     |
|-----------------------|-----|
| 6.1 初识木马.....         | 117 |
| 6.1.1 木马的起源与发展.....   | 117 |
| 6.1.2 木马的机体构造.....    | 117 |
| 6.1.3 木马的种类.....      | 118 |
| 6.2 揭秘木马的伪装与生成 .....  | 119 |
| 6.2.1 揭秘木马的伪装手段 ..... | 119 |
| 6.2.2 揭秘木马捆绑技术.....   | 121 |
| 6.2.3 揭秘自解压捆绑木马.....  | 123 |

|                                       |     |
|---------------------------------------|-----|
| 6.2.4 揭秘 CHM 木马 .....                 | 125 |
| 6.3 揭秘木马的加壳与脱壳工具 .....                | 128 |
| 6.3.1 揭秘 ASPack 加壳 .....              | 128 |
| 6.3.2 利用“北斗压缩”对木马服务端进行多次加壳 .....      | 129 |
| 6.3.3 使用 PE-Scan 检测木马是否加过壳 .....      | 130 |
| 6.3.4 使用 UnASPack 进行脱壳 .....          | 131 |
| 6.4 木马清除工具 .....                      | 132 |
| 6.4.1 利用木马清除专家清除木马 .....              | 132 |
| 6.4.2 利用“Windows 进程管理器”来管理计算机进程 ..... | 135 |
| 技巧与问答 .....                           | 137 |

## 第 7 章 QQ 攻防 ..... 140

|                            |     |
|----------------------------|-----|
| 7.1 揭秘攻击 QQ .....          | 141 |
| 7.1.1 揭秘 QQ 消息“炸弹”攻击 ..... | 141 |
| 7.1.2 本地 QQ 密码是怎样破解的 ..... | 142 |
| 7.1.3 获取用户 IP 地址 .....     | 142 |
| 7.1.4 查询本地聊天记录 .....       | 143 |
| 7.2 QQ 安全防御 .....          | 144 |
| 7.2.1 保护 QQ 密码 .....       | 144 |
| 7.2.2 防范 IP 地址探测 .....     | 145 |
| 技巧与问答 .....                | 146 |

## 第 8 章 揭秘入侵痕迹清除技术 ..... 148

|                            |     |
|----------------------------|-----|
| 8.1 黑客留下的脚印 .....          | 149 |
| 8.1.1 日志产生的原因 .....        | 149 |
| 8.1.2 为什么要清理日志 .....       | 152 |
| 8.2 日志分析工具 WebTrends ..... | 152 |
| 8.2.1 创建日志站点 .....         | 153 |
| 8.2.2 生成日志报表 .....         | 157 |
| 8.3 清除服务器日志 .....          | 158 |

|       |                           |     |
|-------|---------------------------|-----|
| 8.3.1 | 手工删除服务器日志 .....           | 158 |
| 8.3.2 | 使用批处理清除远程主机日志 .....       | 160 |
| 8.4   | 清除历史痕迹 .....              | 161 |
| 8.4.1 | 清除网络历史记录 .....            | 161 |
| 8.4.2 | 使用 Windows 优化大师进行清理 ..... | 164 |
| 8.4.3 | 使用 CCleaner .....         | 165 |
|       | 技巧与问答 .....               | 168 |

## 第 9 章 远程控制技术 ..... 170

|       |                          |     |
|-------|--------------------------|-----|
| 9.1   | 远程控制概述 .....             | 171 |
| 9.1.1 | 远程控制的技术原理 .....          | 171 |
| 9.1.2 | 基于两种协议的远程控制 .....        | 172 |
| 9.1.3 | 远程控制的应用 .....            | 172 |
| 9.2   | 利用任我行软件进行远程控制 .....      | 173 |
| 9.2.1 | 配置服务端 .....              | 174 |
| 9.2.2 | 通过服务端程序进行远程控制 .....      | 175 |
| 9.3   | 使用 QuickIP 进行多点控制 .....  | 176 |
| 9.3.1 | 安装 QuickIP .....         | 176 |
| 9.3.2 | 设置 QuickIP 服务器端 .....    | 177 |
| 9.3.3 | 设置 QuickIP 客户端 .....     | 178 |
| 9.3.4 | 实现远程控制 .....             | 179 |
| 9.4   | 使用 WinShell 实现远程控制 ..... | 179 |
| 9.4.1 | 配置 WinShell .....        | 180 |
| 9.4.2 | 实现远程控制 .....             | 182 |
| 9.5   | 远程桌面连接与协助 .....          | 183 |
| 9.5.1 | Windows 系统的远程桌面连接 .....  | 183 |
| 9.5.2 | Windows 系统远程关机 .....     | 187 |
| 9.5.3 | 区别远程桌面与远程协助 .....        | 188 |
|       | 技巧与问答 .....              | 189 |

|                               |                |
|-------------------------------|----------------|
| <b>第 10 章 系统漏洞与溢出问题</b>       | <b>191</b>     |
| 10.1 什么是溢出                    | 192            |
| 10.2 溢出分类                     | 192            |
| 10.2.1 缓冲区溢出                  | 192            |
| 10.2.2 内存溢出                   | 193            |
| 10.2.3 数据溢出                   | 193            |
| 10.3 DcomRpc 溢出工具             | 193            |
| 10.3.1 认识 DcomRpc 漏洞          | 193            |
| 10.3.2 DcomRpc 入侵原理揭秘         | 195            |
| 10.3.3 怎样防御 DcomRpc 入侵        | 196            |
| 10.4 如何使用系统漏洞检测修复工具           | 198            |
| 10.4.1 如何使用 MBSA 检测系统漏洞       | 198            |
| 10.4.2 如何使用 360 安全卫士修复漏洞      | 201            |
| 技巧与问答                         | 202            |
| <br><b>第 11 章 针对电子邮件攻击与防御</b> | <br><b>204</b> |
| 11.1 揭秘电子邮件病毒                 | 205            |
| 11.1.1 认识“邮件病毒”               | 205            |
| 11.1.2 “邮件病毒”的识别技巧            | 205            |
| 11.2 揭秘制作电子邮件炸弹的运行过程          | 206            |
| 11.3 电子邮件密码是怎样被破解的            | 206            |
| 11.3.1 揭秘怎样使用“流光”破解密码         | 206            |
| 11.3.2 揭秘怎样使用“黑雨”破解密码         | 207            |
| 11.3.3 揭秘怎样使用“流影”破解密码         | 208            |
| 11.4 电子邮件安全防御                 | 210            |
| 11.4.1 电子邮件安全防范措施             | 210            |
| 11.4.2 找回邮件密码                 | 210            |
| 11.4.3 防止炸弹攻击                 | 212            |
| 11.5 “溯雪”邮箱窃密的原理曝光            | 213            |
| 技巧与问答                         | 216            |



## 第 12 章 恶意网页代码攻防 ..... 218

|                                |     |
|--------------------------------|-----|
| 12.1 认识恶意网页代码 .....            | 219 |
| 12.2 恶意网页代码的防范和清除 .....        | 219 |
| 12.2.1 恶意网页代码的防范 .....         | 219 |
| 12.2.2 恶意网页代码的清除 .....         | 220 |
| 12.3 常见恶意网页代码攻击与防御方法 .....     | 221 |
| 12.3.1 启动时自动弹出对话框和网页 .....     | 221 |
| 12.3.2 修改起始页和默认主页 .....        | 222 |
| 12.3.3 强行修改 IE 标题栏 .....       | 223 |
| 12.4 IE 浏览器的安全设置 .....         | 224 |
| 12.4.1 清除 IE 各项内容 .....        | 224 |
| 12.4.2 限制他人访问不良站点 .....        | 225 |
| 12.4.3 设置安全级别和隐私设置 .....       | 226 |
| 12.4.4 IE 的 ActiveX 控件设置 ..... | 227 |
| 技巧与问答 .....                    | 228 |

## 第 13 章 局域网攻防 ..... 232

|                                            |     |
|--------------------------------------------|-----|
| 13.1 局域网安全介绍 .....                         | 233 |
| 13.1.1 局域网基础知识 .....                       | 233 |
| 13.1.2 局域网安全隐患 .....                       | 233 |
| 13.2 揭秘局域网攻击工具 .....                       | 234 |
| 13.2.1 网络剪刀手 NetCut .....                  | 235 |
| 13.2.2 揭秘局域网 ARP 攻击工具 WinArpAttacker ..... | 238 |
| 13.2.3 利用网络特工监视数据 .....                    | 241 |
| 13.3 局域网监控工具 .....                         | 244 |
| 13.3.1 如何使用 LanSee 工具 .....                | 244 |
| 13.3.2 如何使用“长角牛网络监控机” .....                | 246 |
| 技巧与问答 .....                                | 252 |

|                                                   |                |
|---------------------------------------------------|----------------|
| <b>第 14 章 黑客入侵行为检测技术 .....</b>                    | <b>255</b>     |
| 14.1 认识入侵检测 .....                                 | 256            |
| 14.2 基于漏洞的入侵检测系统 .....                            | 256            |
| 14.2.1 如何使用“流光”进行批量主机扫描 .....                     | 256            |
| 14.2.2 如何使用“流光”进行指定漏洞扫描 .....                     | 258            |
| 14.3 Snort 入侵检测系统 .....                           | 260            |
| 14.3.1 Snort 的系统组成 .....                          | 260            |
| 14.3.2 Snort 命令介绍 .....                           | 260            |
| 14.3.3 Snort 的工作模式 .....                          | 262            |
| 14.4 NetBrute 的扫描与防御 .....                        | 263            |
| 14.4.1 对共享资源进行扫描 .....                            | 264            |
| 14.4.2 对端口进行扫描 .....                              | 265            |
| 14.5 利用 WAS 检测网站 .....                            | 267            |
| 14.5.1 Web Application Stress Tool (WAS) 简介 ..... | 267            |
| 14.5.2 如何检测网站的承受压力 .....                          | 267            |
| 14.5.3 如何进行数据分析 .....                             | 271            |
| 14.6 自动防御入侵 .....                                 | 272            |
| 14.6.1 入侵检测方法的分类 .....                            | 273            |
| 14.6.2 入侵检测系统的功能和结构 .....                         | 274            |
| 14.6.3 操作系统的审计跟踪管理 .....                          | 274            |
| 14.6.4 入侵检测技术的发展现状 .....                          | 274            |
| 技巧与问答 .....                                       | 275            |
| <br><b>第 15 章 揭秘黑客常用的入侵方式 .....</b>               | <br><b>277</b> |
| 15.1 揭秘网络欺骗入侵 .....                               | 278            |
| 15.1.1 网络欺骗的主要技术 .....                            | 278            |
| 15.1.2 常见的网络欺骗方式 .....                            | 279            |
| 15.1.3 经典案例解析——网络钓鱼 .....                         | 283            |
| 15.2 揭秘缓冲区溢出入侵 .....                              | 286            |
| 15.2.1 认识缓冲区溢出 .....                              | 286            |
| 15.2.2 缓冲区溢出攻击的基本流程 .....                         | 287            |

|        |                            |     |
|--------|----------------------------|-----|
| 15.2.3 | 了解缓冲区溢出的入侵方法 .....         | 288 |
| 15.2.4 | 缓冲区溢出常用的防范措施 .....         | 289 |
| 15.2.5 | 缓冲区溢出常用的防范措施 .....         | 290 |
| 15.3   | 揭秘口令猜解入侵 .....             | 291 |
| 15.3.1 | 黑客常用的口令猜解攻击方法 .....        | 291 |
| 15.3.2 | 揭秘口令猜解攻击 .....             | 292 |
| 15.3.3 | 揭秘口令攻击类型 .....             | 292 |
| 15.3.4 | 使用 SAMInside 破解计算机密码 ..... | 293 |
| 15.3.5 | 使用 LC6 破解计算机密码 .....       | 296 |
|        | 技巧与问答 .....                | 299 |

## 第 16 章 系统安全防护策略 ..... 300

|        |                           |     |
|--------|---------------------------|-----|
| 16.1   | 设置计算机管理 .....             | 301 |
| 16.1.1 | 使用事件查看器 .....             | 301 |
| 16.1.2 | 管理共享资源 .....              | 302 |
| 16.1.3 | 管理系统服务程序 .....            | 303 |
| 16.2   | 设置系统安全 .....              | 305 |
| 16.2.1 | 超过登录时间后强制用户注销 .....       | 305 |
| 16.2.2 | 不显示上次登录时的用户名 .....        | 306 |
| 16.2.3 | 限制格式化和弹出可移动媒体 .....       | 306 |
| 16.2.4 | 对备份和还原权限进行审核 .....        | 307 |
| 16.2.5 | 禁止在下次更改密码时存储 Hash 值 ..... | 308 |
| 16.2.6 | 设置本地账户共享与安全模式 .....       | 308 |
| 16.3   | 设置系统组策略 .....             | 309 |
| 16.3.1 | 设置账户锁定策略 .....            | 309 |
| 16.3.2 | 设置密码策略 .....              | 310 |
| 16.3.3 | 设置用户权限 .....              | 311 |
| 16.3.4 | 更改系统默认管理员账户 .....         | 312 |
| 16.3.5 | 不允许 SAM 账户匿名枚举 .....      | 313 |
| 16.3.6 | 禁止更改“开始菜单” .....          | 314 |
| 16.4   | 设置注册表 .....               | 314 |
| 16.4.1 | 禁止访问和编辑注册表 .....          | 314 |