



学电脑从入门到精通



THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER

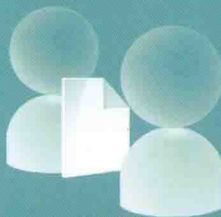


PC与智能手机黑客攻防实战

黑客攻防 大全

王叶 编著

- 从零起步，通俗易懂，由浅入深，快速掌握黑客攻防技巧与工具使用
- 实用性强，理论与案例结合，图文并茂，快速融会贯通
- 大量技巧与小窍门，帮读者解惑答疑、快速上手



黑客攻防 大全

王叶 编著



机械工业出版社
China Machine Press

图书在版编目(CIP)数据

黑客攻防大全 / 王叶编著. —北京: 机械工业出版社, 2015.8

ISBN 978-7-111-51017-8

I. 黑… II. 王… III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2015) 第 199994 号

本书由易到难、循序渐进地介绍了黑客攻防的基础技术, 主要包括黑客基础知识、Windows 系统中的命令行基础、黑客常用的 Windows 网络命令、常见的黑客攻击方式、扫描与嗅探攻防、病毒攻防技术、木马攻防技术、Windows 系统漏洞攻防、手机黑客攻防、WiFi 攻防、Windows 系统编程基础、局域网攻防、后门技术攻防、远程控制技术、密码攻防、网游与网吧攻防、网站脚本入侵与防范、QQ 账号及电子邮件攻防、黑客入侵检测技术、网络代理与追踪技术、入侵痕迹清除技术、网络支付工具安全防护、系统和数据的备份与恢复、计算机安全防护等内容。本书重点在于让读者在了解黑客入侵的基础上, 学会采取有效的防范措施来防御黑客入侵自己的计算机。每章都介绍了入侵和防御的相关内容。

本书适用于计算机初学者, 也适用于计算机维护人员、IT 从业人员以及对黑客攻防与网络安全维护感兴趣的计算机中级用户, 计算机培训机构也可以将本书用作辅导书。



黑客攻防大全

出版发行: 机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码: 100037)

责任编辑: 李华君

责任校对: 董纪丽

印 刷: 北京瑞德印刷有限公司

版 次: 2015 年 9 月第 1 版第 1 次印刷

开 本: 185mm×260mm 1/16

印 张: 35.5

书 号: ISBN 978-7-111-51017-8

定 价: 79.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88379426 88361066

投稿热线: (010) 88379604

购书热线: (010) 68326294 88379649 68995259

读者信箱: hzit@hzbook.com

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光 / 邹晓东



前言

如今已经进入信息化时代，随着网络技术的飞速发展，上网已经成为个人生活与工作中获取信息的重要手段，网上消费也随之不断增多。但是随着网络带给人们生活便捷的同时，各种网络病毒、木马也纷纷出现，给我们的个人信息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以及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，就必须要做好计算机网络安全维护和防范。

本书介绍黑客攻防基础知识，由浅入深地讲述黑客攻击的原理、常用手段，让读者在了解黑客攻击的同时学到拒敌于千里之外的方法。

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，对各个知识点进行了详细介绍，并介绍了相关代表性产品和工具的使用方法，使得读者可对网络安全主动防护及黑客入侵主动防御等关键技术有一个全面认识。

本书特色

- 从零起步，逐步深入，通俗易懂，由浅入深，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，节省摸索时间。
- 重点突出，操作简练，内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在计算机上操作，做到即学即用、即用即得，快速掌握这些操作。

本书适合人群

本书紧紧围绕“攻”和“防”两个不同的角度，讲解黑客技术与反黑工具的使用方法。作为一本面向广大网络爱好者的速查手册，本书适合以下读者学习使用：

- 没有多少计算机操作基础的广大读者。
- 需要获得数据保护的日常办公人员。
- 喜欢看图学习的广大读者。
- 相关网络管理人员、网吧工作人员等。
- 明确学习目的、喜欢钻研黑客技术但编程基础薄弱的读者。
- 网络管理员及广大网友。

目 录

前 言

第1章 黑客基础知识 / 1

- 1.1 认识黑客 / 1
 - 1.1.1 白帽、灰帽以及黑帽黑客 / 1
 - 1.1.2 黑客、红客、蓝客以及骇客 / 1
 - 1.1.3 黑客通常掌握的知识 / 2
 - 1.1.4 黑客常用术语 / 3
- 1.2 认识进程与端口 / 4
 - 1.2.1 系统进程 / 4
 - 1.2.2 关闭和新建系统进程 / 5
 - 1.2.3 端口的分类 / 6
 - 1.2.4 查看端口 / 8
 - 1.2.5 开启和关闭端口 / 9
 - 1.2.6 端口的限制 / 11
- 1.3 常见的网络协议 / 17
 - 1.3.1 TCP/IP 协议簇 / 17
 - 1.3.2 IP 协议 / 17
 - 1.3.3 ARP 协议 / 18
 - 1.3.4 ICMP 协议 / 19
- 1.4 在计算机中创建虚拟测试环境 / 20
 - 1.4.1 安装 VMware 虚拟机 / 20
 - 1.4.2 配置 VMware 虚拟机 / 22
 - 1.4.3 安装虚拟操作系统 / 24
 - 1.4.4 安装 VMware Tools / 25

第2章 Windows系统中的命令行基础 / 27

- 2.1 Windows 系统中的命令行 / 27
 - 2.1.1 命令行概述 / 27
 - 2.1.2 命令行操作 / 31
 - 2.1.3 启动命令行 / 31

2.2 在 Windows 系统中执行 DOS

命令 / 32

2.2.1 用菜单的形式进入 DOS

窗口 / 33

2.2.2 通过 IE 浏览器访问 DOS

窗口 / 33

2.2.3 复制、粘贴命令行 / 34

2.2.4 设置窗口风格 / 35

2.2.5 Windows 系统命令行常用

命令 / 38

2.3 全面认识 DOS 系统 / 39

2.3.1 DOS 系统的功能 / 39

2.3.2 文件与目录 / 39

2.3.3 文件类型与属性 / 40

2.3.4 目录与磁盘 / 42

2.3.5 DOS 命令格式 / 43

第3章

黑客常用的Windows网络命令 / 45

3.1 黑客常用的网络命令 / 45

3.1.1 测试物理网络的 ping 命令 / 45

3.1.2 查看网络连接的 netstat

命令 / 47

3.1.3 工作组和域的 net 命令 / 49

3.1.4 telnet 命令 / 54

3.1.5 传输协议 ftp 命令 / 54

3.1.6 查看网络配置的 ipconfig

命令 / 55

3.2 其他的网络命令 / 55

3.2.1 tracert 命令 / 56

3.2.2 route 命令 / 57

3.2.3 netsh 命令 / 58

3.2.4 arp 命令 / 60

第4章

常见的黑客攻击方式 / 62

4.1 网络欺骗攻击曝光 / 62

4.1.1 5 种常见的网络欺骗方式 / 62

4.1.2 网络钓鱼攻击概念 / 65

4.1.3 网络钓鱼攻击的常用手段 / 65

4.1.4 网络钓鱼攻击的预防 / 66

4.2 口令猜解攻击曝光 / 67

4.2.1 实现口令猜解攻击的 3 种方法 / 67

4.2.2 使用 LC6 破解计算机密码 / 68

4.2.3 使用 SAMInside 破解

计算机密码 / 71

4.3 缓冲区溢出攻击曝光 / 74

4.3.1 缓冲区溢出介绍 / 74

4.3.2 缓冲区溢出攻击方式 / 75

4.3.3 缓冲区溢出攻击防御 / 76

第5章 扫描与嗅探攻防 / 78

- 5.1 确定扫描目标 / 78
 - 5.1.1 确定目标主机 IP 地址 / 78
 - 5.1.2 了解网站备案信息 / 81
 - 5.1.3 确定可能开放的端口和服务 / 82
- 5.2 扫描的实施与防范 / 84
 - 5.2.1 扫描服务与端口 / 85
 - 5.2.2 用 X-Scan 扫描器查本机隐患 / 87
 - 5.2.3 用 SSS 扫描器扫描系统漏洞 / 92
 - 5.2.4 常见扫描工具 / 95
 - 5.2.5 用 ProtectX 实现扫描的反击与追踪 / 96
 - 5.2.6 极速端口扫描器 / 99
 - 5.2.7 S-GUI Ver 扫描器 / 101
- 5.3 嗅探的实现与防范 / 103
 - 5.3.1 什么是嗅探器 / 103
 - 5.3.2 经典嗅探器 Iris / 104
 - 5.3.3 使用影音神探嗅探在线视频地址 / 106
 - 5.3.4 捕获网页内容的艾菲网页侦探 / 110
- 5.4 运用工具实现网络监控 / 112
 - 5.4.1 运用 Real Spy Monitor 监控网络 / 112
 - 5.4.2 运用网络执法官实现网络监控 / 117

第6章 病毒攻防技术 / 121

- 6.1 病毒知识入门 / 121
 - 6.1.1 计算机病毒的特点 / 121
 - 6.1.2 病毒的基本结构 / 121
 - 6.1.3 病毒的工作流程 / 122
- 6.2 两种简单病毒的生成与防范 / 123
 - 6.2.1 U 盘病毒的生成与防范 / 123
 - 6.2.2 Restart 病毒形成过程 / 125
- 6.3 了解脚本病毒及其安全防范 / 128
 - 6.3.1 VBS 脚本病毒的特点 / 129
 - 6.3.2 VBS 脚本病毒通过网络传播的几种方式 / 129
 - 6.3.3 VBS 脚本病毒生成机 / 130
 - 6.3.4 刷 QQ 聊天屏的 VBS 脚本病毒 / 132
 - 6.3.5 如何防范 VBS 脚本病毒 / 133
- 6.4 全面防范网络蠕虫 / 133
 - 6.4.1 网络蠕虫病毒实例分析 / 133
 - 6.4.2 网络蠕虫病毒的全面防范 / 134
- 6.5 杀毒软件的使用 / 136
 - 6.5.1 使用免费的防火墙 Zone Alarm / 136
 - 6.5.2 用 NOD32 查杀病毒 / 137

第7章

木马攻防技术 / 139

7.1 认识木马 / 139

7.1.1 木马的发展历程 / 139

7.1.2 木马的组成 / 139

7.1.3 木马的分类 / 140

7.2 木马的伪装与生成 / 141

7.2.1 木马的伪装手段 / 141

7.2.2 木马捆绑技术 / 142

7.2.3 自解压捆绑木马 / 145

7.2.4 CHM 木马 / 146

7.3 木马的加壳与脱壳 / 149

7.3.1 使用 ASPack 加壳 / 150

7.3.2 使用“北斗程序压缩”

进行多次加壳 / 151

7.3.3 使用 PE-Scan 检测木马

是否加过壳 / 152

7.3.4 使用 UnAspack 进行

脱壳 / 153

7.4 木马清除软件的使用 / 154

7.4.1 用“木马清除专家”清除
木马 / 1557.4.2 用“木马清道夫”清除
木马 / 1587.4.3 在“Windows 进程管理器”
中管理进程 / 161

第8章

系统漏洞攻防 / 163

8.1 系统漏洞基础知识 / 163

8.1.1 系统漏洞概述 / 163

8.1.2 Windows 系统常见漏洞 / 163

8.2 Windows 服务器系统入侵曝光 / 166

8.2.1 入侵 Windows 服务器的
流程 / 166

8.2.2 NetBIOS 漏洞攻防 / 168

8.3 DcomRpc 漏洞入侵曝光 / 172

8.3.1 DcomRpc 漏洞描述 / 172

8.3.2 DcomRpc 入侵实战 / 174

8.3.3 DcomRpc 防范方法 / 175

8.4 用 MBSA 检测系统漏洞 / 177

8.4.1 检测单台计算机 / 177

8.4.2 检测多台计算机 / 178

8.5 使用 Windows Update 修复系统
漏洞 / 179

第9章

手机黑客攻防 / 181

- 9.1 初识手机黑客 / 181
 - 9.1.1 智能手机操作系统 / 181
 - 9.1.2 常见的手机攻击类型 / 182
- 9.2 手机黑客基础知识 / 183
 - 9.2.1 获取 Android Root 权限 / 183
 - 9.2.2 Android 手机备份功能 / 185
 - 9.2.3 安卓系统刷机 / 187
 - 9.2.4 苹果手机“越狱” / 189
- 9.3 手机病毒与木马攻防 / 191
 - 9.3.1 手机病毒与木马带来的危害 / 191
 - 9.3.2 手机病毒防范 / 192
- 9.4 手机蓝牙攻击曝光 / 194
 - 9.4.1 蓝牙的工作原理 / 194
 - 9.4.2 蓝劫攻击与防范 / 195
- 9.5 手机拒绝服务攻击曝光 / 196
 - 9.5.1 常见的手机拒绝服务攻击 / 196
 - 9.5.2 手机拒绝服务攻击防范 / 196
- 9.6 手机电子邮件攻击曝光 / 197
 - 9.6.1 认识邮件在网络上的传播方式 / 197
 - 9.6.2 手机上常用的邮件系统 / 197
 - 9.6.3 手机电子邮件攻击与防范 / 198
- 9.7 手机加密技术 / 198
 - 9.7.1 手机开机密码设置与解密 / 198
 - 9.7.2 手机短信与照片加密 / 202
- 9.8 手机支付安全防范 / 208
 - 9.8.1 手机支付的3种方式 / 208
 - 9.8.2 常见的5种手机支付软件 / 209
 - 9.8.3 手机支付安全问题 / 211
- 9.9 手机优化及安全性能的提升 / 211
 - 9.9.1 360手机卫士 / 211
 - 9.9.2 腾讯手机管家 / 212
 - 9.9.3 金山手机卫士 / 213

第10章

WiFi攻防 / 215

- 10.1 无线路由器基本设置 / 215
 - 10.1.1 无线路由器外观 / 215
 - 10.1.2 无线路由器参数设置 / 216
 - 10.1.3 设置完成重启无线路由器 / 217
 - 10.1.4 搜索无线信号连接上网 / 218
- 10.2 傻瓜式破解 WiFi 密码曝光及防范 / 219
 - 10.2.1 “WiFi 万能钥匙”手机破解 WiFi 密码 / 219

- 10.2.2 “WiFi 万能钥匙” 计算机
破解 WiFi 密码 / 221
- 10.2.3 防范 “WiFi 万能钥匙”
破解密码 / 222
- 10.3 Linux 下利用抓包破解 WiFi 密码
曝光 / 224
 - 10.3.1 虚拟 Linux 系统 / 224
 - 10.3.2 破解 PIN 码 / 227
 - 10.3.3 破解 WPA 密码 / 228
- 10.3.4 破解 WPA2 密码 / 229
- 10.4 无线路由器安全设置 / 231
 - 10.4.1 修改 WiFi 连接密码 / 231
 - 10.4.2 禁用 DHCP 功能 / 231
 - 10.4.3 无线加密 / 232
 - 10.4.4 关闭 SSID 广播 / 233
 - 10.4.5 设置 IP 过滤和 MAC
地址列表 / 233
 - 10.4.6 主动更新 / 234

第11章

Windows系统编程基础 / 235

- 11.1 了解黑客与编程 / 235
 - 11.1.1 黑客常用的4种编程语言 / 235
 - 11.1.2 黑客与编程的关系 / 236
- 11.2 网络通信编程 / 237
 - 11.2.1 网络通信简介 / 237
 - 11.2.2 Winsock 编程基础 / 240
- 11.3 文件操作编程 / 244
 - 11.3.1 文件读写编程 / 245
 - 11.3.2 文件的复制、移动和
删除编程 / 248
- 11.4 注册表编程 / 248
- 11.5 进程和线程编程 / 252
 - 11.5.1 进程编程 / 252
 - 11.5.2 线程编程 / 257

第12章

局域网攻防 / 260

- 12.1 局域网安全概述 / 260
 - 12.1.1 局域网基础知识 / 260
 - 12.1.2 局域网安全隐患 / 261
- 12.2 ARP 欺骗与防御 / 262
 - 12.2.1 ARP 欺骗概述 / 262
 - 12.2.2 WinArpAttacker ARP 欺骗
攻击 / 262
 - 12.2.3 网络监听与 ARP
欺骗 / 265
 - 12.2.4 金山贝壳 ARP 防火墙的
使用 / 267
- 12.3 绑定 MAC 防御 IP 冲突攻击 / 268

- 12.3.1 查看本机的 MAC 地址 / 268
- 12.3.2 绑定 MAC 防御 IP 冲突
攻击 / 269
- 12.4 局域网助手攻击与防御 / 270
- 12.5 利用“网络守护神”实现网络
管理 / 272
- 12.6 局域网监控工具 / 276
 - 12.6.1 网络特工 / 276
 - 12.6.2 LanSee 工具 / 279
 - 12.6.3 长角牛网络监控机 / 281

第13章 后门技术攻防 / 286

- 13.1 认识后门 / 286
 - 13.1.1 后门的发展历史 / 286
 - 13.1.2 后门的分类 / 287
- 13.2 账号后门技术曝光 / 287
 - 13.2.1 使用软件克隆账号 / 288
 - 13.2.2 手动克隆账号 / 289
- 13.3 系统服务后门技术曝光 / 292
 - 13.3.1 使用 Instsrv 创建系统
服务后门 / 292
 - 13.3.2 使用 Srvinstw 创建系统
服务后门 / 293
- 13.4 检测系统中的后门程序 / 297

第14章 远程控制技术 / 299

- 14.1 认识远程控制 / 299
 - 14.1.1 远程控制的技术发展
经历 / 299
 - 14.1.2 远程控制的技术原理 / 299
 - 14.1.3 远程控制的应用 / 300
- 14.2 远程桌面连接与协助 / 300
 - 14.2.1 Windows 系统的远程
桌面连接 / 301
 - 14.2.2 Windows 系统远程关机 / 304
 - 14.2.3 远程桌面与远程协助的
区别 / 305
- 14.3 利用“远程控制任我行”软件
进行远程控制 / 306
 - 14.3.1 配置服务端 / 306
 - 14.3.2 通过服务端程序进行
远程控制 / 307
- 14.4 用 WinShell 实现远程控制 / 309
 - 14.4.1 配置 WinShell / 309
 - 14.4.2 实现远程控制 / 311
- 14.5 用 QuickIP 进行多点控制 / 312
 - 14.5.1 设置 QuickIP 服务
器端 / 312
 - 14.5.2 设置 QuickIP 客户端 / 313
 - 14.5.3 实现远程控制 / 314

第15章

密码攻防 / 315

15.1 加密与解密基础知识 / 315

15.1.1 认识加密与解密 / 315

15.1.2 加密的通信模型 / 315

15.2 7种常见的加密解密类型 / 315

15.2.1 RAR 压缩文件 / 315

15.2.2 多媒体文件 / 317

15.2.3 光盘 / 320

15.2.4 Word 文件 / 322

15.2.5 Excel 文件 / 326

15.2.6 宏加密解密技术 / 330

15.2.7 NTFS 文件系统加密数据 / 332

15.3 文件和文件夹密码攻防 / 336

15.3.1 对文件分割加密 / 336

15.3.2 对文件夹进行加密 / 342

15.3.3 WinGuard 加密应用程序 / 347

15.4 系统密码攻防 / 348

15.4.1 利用 Windows 7 PE 破解
系统登录密码 / 34815.4.2 利用密码重设盘破解
系统登录密码 / 35215.4.3 使用 SecureIt Pro 给系统
桌面加把超级锁 / 35515.4.4 系统全面加密大师
PC Security / 357

15.5 其他加密解密工具 / 361

15.5.1 “加密精灵”加密
工具 / 361

15.5.2 MD5 加密解密实例 / 362

15.5.3 用“私人磁盘”隐藏
大文件 / 364

第16章

网游与网吧攻防 / 368

16.1 网游盗号木马曝光 / 368

16.1.1 捆绑木马盗号 / 368

16.1.2 哪些网游账号容易
被盗 / 370

16.2 解读网站充值欺骗术 / 371

16.2.1 欺骗原理 / 371

16.2.2 常见的欺骗方式 / 371

16.2.3 提高防范意识 / 372

16.3 防范游戏账号破解 / 373

16.3.1 勿用“自动记住
密码” / 373

16.3.2 防范方法 / 376

16.4 警惕局域网监听 / 376

16.4.1 了解监听的原理 / 376

16.4.2 防范方法 / 377

16.5 美萍网管大师 / 380

第17章

网站脚本入侵与防范 / 383

- 17.1 Web 脚本入侵与防范 / 383
 - 17.1.1 Web 脚本攻击的特点 / 383
 - 17.1.2 Web 脚本攻击常见的方式 / 384
 - 17.1.3 脚本漏洞的根源与防范 / 385
- 17.2 SQL 注入攻击与防范 / 386
 - 17.2.1 设置“显示友好 HTTP 错误消息” / 386
 - 17.2.2 准备注入工具 / 387
 - 17.2.3 SQL 注入攻击的防范 / 388
- 17.3 啊 D 注入工具 / 390
 - 17.3.1 啊 D 注入工具的功能 / 391
 - 17.3.2 使用啊 D 批量注入 / 391
- 17.4 NBSI 注入工具 / 394
 - 17.4.1 NBSI 功能概述 / 394
 - 17.4.2 使用 NBSI 实现注入 / 395
- 17.5 Domain 旁注工具 / 397
 - 17.5.1 Domain 功能概述 / 397
 - 17.5.2 使用 Domain 实现注入 / 398
 - 17.5.3 使用 Domain 扫描管理后台 / 401
 - 17.5.4 使用 Domain 上传 WebShell / 402
- 17.6 PHP 注入工具 ZBSI / 402
 - 17.6.1 ZBSI 功能概述 / 402
 - 17.6.2 使用 ZBSI 实现注入 / 402

第18章

QQ账号及电子邮件攻防 / 405

- 18.1 三种盗取QQ号码的软件及其防范 / 405
 - 18.1.1 “QQ 简单盗”盗取 QQ 密码曝光与防范方法 / 405
 - 18.1.2 “好友号好好盗”盗取 QQ 号码曝光 / 407
 - 18.1.3 QQExplorer 在线破解 QQ 号码曝光与防范方法 / 408
- 18.2 用密码监听器揪出内鬼 / 409
 - 18.2.1 “密码监听器”盗号披露 / 409
 - 18.2.2 找出“卧底”拒绝监听 / 411
- 18.3 保护 QQ 密码和聊天记录 / 411
 - 18.3.1 定期修改 QQ 密码 / 411
 - 18.3.2 申请 QQ 密保 / 412
 - 18.3.3 加密聊天记录 / 414
- 18.4 防范电子邮箱账户欺骗 / 414
 - 18.4.1 伪造邮箱账户 / 414
 - 18.4.2 隐藏邮箱账户 / 415
 - 18.4.3 追踪伪造邮箱账户发件人 / 415
 - 18.4.4 防范垃圾邮件 / 416
 - 18.4.5 邮箱使用规则 / 418

第19章 黑客入侵检测技术 / 419

- 19.1 入侵检测概述 / 419
- 19.2 基于网络的入侵检测系统 / 419
 - 19.2.1 包嗅探器和网络监视器 / 420
 - 19.2.2 包嗅探器和混杂模式 / 420
 - 19.2.3 基于网络的入侵检测：包嗅探器的发展 / 420
- 19.3 基于主机的入侵检测系统 / 421
- 19.4 基于漏洞的入侵检测系统 / 422
 - 19.4.1 运用“流光”进行批量主机扫描 / 423
 - 19.4.2 运用“流光”进行指定漏洞扫描 / 425
- 19.5 萨客嘶入侵检测系统 / 426
- 19.6 Snort 入侵检测系统 / 430
 - 19.6.1 Snort 的系统组成 / 430
 - 19.6.2 Snort 命令介绍 / 430
 - 19.6.3 Snort 的工作模式 / 431

第20章 网络代理与追踪技术 / 433

- 20.1 代理服务器软件的使用 / 433
 - 20.1.1 利用“代理猎手”找代理 / 433
 - 20.1.2 用 SocksCap32 设置动态代理 / 438
 - 20.1.3 防范远程跳板代理攻击 / 441
- 20.2 常见的黑客追踪工具 / 443
 - 20.2.1 实战 IP 追踪技术 / 443
 - 20.2.2 NeroTrace Pro 追踪工具的使用 / 443

第21章 入侵痕迹清除技术 / 447

- 21.1 黑客留下的脚印 / 447
 - 21.1.1 日志产生的原因 / 447
 - 21.1.2 为什么要清理日志 / 450
- 21.2 日志分析工具 WebTrends / 451
 - 21.2.1 创建日志站点 / 451
 - 21.2.2 生成日志报表 / 455
- 21.3 清除服务器日志 / 457
 - 21.3.1 手工删除服务器日志 / 457
 - 21.3.2 使用批处理清除远程主机日志 / 459

21.4 Windows 日志清理工具 / 460

21.4.1 elseve 工具 / 460

21.4.2 ClearLogs 工具 / 461

21.5 清除历史痕迹 / 462

21.5.1 清除网络历史记录 / 462

21.5.2 使用“Windows 优化大师”进行清理 / 466

21.5.3 使用 CCleaner / 467

第22章

网络支付工具的安全防护 / 471

22.1 加强支付宝的安全防护 / 471

22.1.1 支付宝账户的安全防护 / 471

22.1.2 支付宝内资金的安全防护 / 475

22.2 加强财付通的安全防护 / 478

22.2.1 财付通账户的安全防护 / 478

22.2.2 财付通内资金的安全防护 / 481

22.3 加强网上银行的安全防护 / 483

22.3.1 定期修改登录密码 / 483

22.3.2 设置预留验证信息 / 485

22.3.3 安装防钓鱼安全控件 / 486

22.3.4 使用小 e 安全检测系统 / 488

22.3.5 使用工行 U 盾 / 489

22.3.6 使用电子银行口令卡 / 489

第23章

系统和数据的备份与恢复 / 490

23.1 备份与还原操作系统 / 490

23.1.1 使用还原点备份与还原系统 / 490

23.1.2 使用 GHOST 备份与还原系统 / 493

23.2 备份与还原用户数据 / 497

23.2.1 使用“驱动精灵”备份与还原驱动程序 / 497

23.2.2 备份与还原 IE 浏览器的收藏夹 / 499

23.2.3 备份与还原 QQ 聊天记录 / 502

23.2.4 备份与还原 QQ 自定义表情 / 504

23.3 使用恢复工具恢复误删除的数据 / 508

23.3.1 使用 Recuva 恢复数据 / 508

23.3.2 使用 FinalData 恢复数据 / 512

23.3.3 使用 FinalRecovery 恢复数据 / 517

- 24.1 间谍软件防护实战 / 520
 - 24.1.1 间谍软件防护概述 / 520
 - 24.1.2 使用 SpySweeper 清除间谍软件 / 521
 - 24.1.3 微软反间谍专家 Windows Defender 使用流程 / 523
 - 24.1.4 使用 360 安全卫士对计算机进行防护 / 525
- 24.2 流氓软件的清除 / 528
 - 24.2.1 清理浏览器插件 / 528
 - 24.2.2 使用“金山清理专家”清除恶意软件 / 530
 - 24.2.3 流氓软件的防范 / 531
- 24.3 常见的网络安全防护工具 / 535
 - 24.3.1 浏览器绑架克星 HijackThis / 535
 - 24.3.2 诺顿网络安全特警 / 539
 - 24.3.3 Ad-Aware 让间谍程序消失无踪 / 542
- 24.4 系统安全设置 / 545
 - 24.4.1 更改账户名 / 545
 - 24.4.2 禁用来宾账户 / 547
 - 24.4.3 设置离开时快速锁定桌面 / 548
 - 24.4.4 设置账户锁定策略 / 549