

天河文化 编著

最新 黑客攻防 从入门到精通

The Newest Hacker Attack and Defense:
from Novice to Master



CD-ROM

内容全面，与时俱进：

介绍手机黑客攻防、木马攻防等内容，帮助读者快速打通学习的重要关卡，轻松入门。

任务驱动，自主学习：

“理论 + 实战 + 图文 + 视频”的学习模式，让读者快速精通黑客攻防技术。

实例为主，易于上手：

模拟真实的工作环境，解决各种疑难问题。



机械工业出版社
CHINA MACHINE PRESS

网络安全技术丛书

最新黑客攻防从入门到精通

天河文化 编著



机械工业出版社

本书共 19 章, 结合案例, 由浅入深、系统全面地介绍了黑客攻防技术, 内容涵盖: 从零开始认识黑客、信息的扫描与嗅探、系统漏洞攻防、病毒攻防、木马攻防、手机黑客攻防、网游与网吧攻防、密码攻防、黑客入侵检测技术、网络代理与追踪技术、后门技术、入侵痕迹清除技术、远程控制技术、局域网攻防、QQ 账号攻防、网站攻防、系统和数据的备份与恢复、保障网络支付工具的安全、间谍软件的清除和系统清理。

本书内容丰富全面、图文并茂、从易到难, 面向广大计算机初学者和黑客攻防技术爱好者, 也适用于需要保障数据安全的日常办公人员、网络安全从业人员及网络管理人员参考阅读。

图书在版编目 (CIP) 数据

最新黑客攻防从入门到精通 / 天河文化编著. —北京: 机械工业出版社, 2015.3

(网络安全技术丛书)

ISBN 978-7-111-49787-5

I. ①最… II. ①天… 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 (2015) 第 061306 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策划编辑: 王海霞

责任编辑: 王海霞 责任校对: 张艳霞

责任印制: 乔宇

保定市 中画美凯印刷有限公司印刷

2015 年 5 月第 1 版 · 第 1 次印刷

184mm×260mm · 26 印张 · 643 千字

0001-4000 册

标准书号: ISBN 978-7-111-49787-5

ISBN 978-7-89405-745-7 (光盘)

定价: 69.80 元 (含 1CD)

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换
电话服务 网络服务

服务咨询热线: (010) 88361066 机工官网: www.cmpbook.com

读者购书热线: (010) 68326294 机工官博: weibo.com/cmp1952

(010) 88379203 教育服务网: www.cmpedu.com

封面 无防伪标均为盗版

金书网: www.golden-book.com

随着互联网的普及，人们越发地依赖利用互联网进行购物和投资等，互联网的发展同时方便了黑客工具的传播，有的黑客会对一些疏于防范的计算机做出攻击，进行识别偷窃、窃取信用卡账号、勒索银行等行为。因此，提高防范意识，学习黑客的入侵手段以及防御黑客的技术和方法极为重要。

本书内容

本书紧紧围绕“攻”和“防”两个不同的角度，先揭露黑客攻击手段，再介绍相应的防范方法。知己知彼，方能更好地防御黑客攻击。

本书内容共 19 章。

第 1 章：从零开始认识黑客。主要介绍黑客基础知识，包括黑客常用术语、进程、端口、常见的网络协议、黑客常用命令以及在计算机中创建虚拟测试环境等内容。

第 2 章：信息的扫描与嗅探。主要介绍扫描、嗅探的实施与防范以及网络监控等内容。

第 3 章：系统漏洞攻防。主要介绍系统漏洞基础知识、Windows 服务器系统入侵曝光、DcomRpc 漏洞入侵曝光以及用 MBSA 检测系统漏洞等内容。

第 4 章：病毒攻防。主要介绍病毒基础知识、两种简单病毒的生成与防范、脚本病毒的生成与防范、宏病毒与邮件病毒的防范、网络蠕虫的防范以及杀毒软件的使用等内容。

第 5 章：木马攻防。主要介绍木马基础知识、木马的伪装与生成、木马的加壳与脱壳以及木马清除软件的使用等内容。

第 6 章：手机黑客攻防。主要介绍智能手机操作系统、获取 Android Root 权限、Android 手机备份功能、安卓系统刷机、苹果手机越狱、手机蓝牙攻击曝光、手机拒绝服务攻击曝光、手机电子邮件攻击曝光、手机病毒与木马攻防、手机加密技术、手机支付安全防范、手机优化及安全性能的提升等内容。

第 7 章：网游与网吧攻防。主要介绍网游盗号木马、网站充值欺骗术、防范游戏账号破解、警惕局域网监听及美萍网管大师等内容。

第 8 章：密码攻防。主要介绍加密与解密基础知识、七种常见的加密解密类型、文件和文件夹密码攻防、系统密码攻防及其他加密解密工具等内容。

第9章：黑客入侵检测技术。主要介绍基于网络的入侵检测系统、基于主机的入侵检测系统、基于漏洞的入侵检测系统、萨客嘶入侵检测系统、Snort入侵检测系统等内容。

第10章：网络代理与追踪技术。主要介绍网络代理工具“代理猎手”和SocksCap32、常见的黑客追踪工具NeroTrace Pro等内容。

第11章：后门技术。主要介绍后门的分类、账号后门技术曝光、系统服务后门技术曝光、检测系统中的后门程序等内容。

第12章：入侵痕迹清除技术。主要介绍黑客留下的脚印、清除服务器日志、Windows日志清理工具、清除历史痕迹等内容。

第13章：远程控制技术。主要介绍认识远程控制、远程桌面连接与协助、用WinShell实现远程控制、用QuickIP进行多点控制等内容。

第14章：局域网攻防。主要介绍局域网安全、局域网攻击曝光、局域网监控工具等内容。

第15章：QQ账号攻防。主要介绍三种盗取QQ号码软件防范、用密码监听器揪出“内鬼”、保护QQ密码和聊天记录等内容。

第16章：网站攻防。主要介绍SQL注入攻击曝光、ZBSI检测注入点曝光、Cookie注入攻击曝光、跨站脚本攻击曝光等内容。

第17章：系统和数据的备份与恢复。主要介绍备份与还原操作系统、备份与还原用户数据、使用恢复工具来恢复误删除的数据等内容。

第18章：保障网络支付工具的安全。主要介绍加强支付宝的安全防护和加强财付通的安全防护等内容。

第19章：间谍软件的清除和系统清理。主要介绍流氓软件的清除、间谍软件防护实战和常见的网络安全防护工具等内容。

本书特色

本书循序渐进地讲解了黑客攻防的具体方法和技巧，通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 任务驱动，自主学习，“理论+实战+图文”学习模式让读者快速入门。
- 内容全面，轻松入门，快速打通初学者学习的重要关卡。
- 实例为主，易于上手，模拟真实工作环境，解决各种疑难问题。

本书以图文并茂、按图索骥的方式揭露黑客的攻击手法，并详细讲解相应的网络安全管理防御技术，详细分析每一个操作案例，力求让读者尽快掌握黑客编程技术，理解和掌握类似场合的应对思路。

本书适合人群

本书适合以下读者学习使用：

- 计算机初学者；
- 需要保障数据安全的日常办公人员；
- 网络管理人员、网吧工作人员；
- 喜欢钻研黑客攻防技术但编程基础薄弱的读者；
- 相关计算机培训机构的师生。

本书作者

本书由天河文化编著，参与本书编写的人员有郑奎国、王叶、候琴琴、郅朝怡、施亚、宫晨伟、朱伟伟、李季、郑林、张阮阮、丁建飞、方开庆、陈红、陈伟、赵雨、王越、赵根昌、竹简、苗玉珍和余东航。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人计算机及相关设备的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术侵害别人权益，否则后果自负。

编者

前言

第 1 章 从零开始认识黑客 / 1

1.1 认识黑客 / 2

- 1.1.1 黑客、红客、蓝客及骇客 / 2
- 1.1.2 白帽黑客、灰帽黑客及黑帽黑客 / 2
- 1.1.3 成为黑客必须掌握的知识 / 2
- 1.1.4 黑客常用术语 / 3

1.2 认识进程与端口 / 5

- 1.2.1 认识系统进程 / 5
- 1.2.2 关闭和新建系统进程 / 6
- 1.2.3 端口的分类 / 7
- 1.2.4 查看端口 / 9
- 1.2.5 开启和关闭端口 / 10
- 1.2.6 端口的限制 / 12

1.3 常见的网络协议 / 18

- 1.3.1 TCP/IP 协议簇 / 18

- 1.3.2 IP 协议 / 18

- 1.3.3 ARP 协议 / 19

- 1.3.4 ICMP 协议 / 20

1.4 黑客常用命令 / 21

- 1.4.1 测试物理网络的 ping 命令 / 21

- 1.4.2 查看网络连接的 netstat 命令 / 23

- 1.4.3 工作组和域的 net 命令 / 24

- 1.4.4 23 端口登录的 telnet 命令 / 27

- 1.4.5 传输协议 ftp 命令 / 27

- 1.4.6 查看网络配置的 ipconfig 命令 / 27

1.5 在计算机中创建虚拟测试环境 / 28

- 1.5.1 安装 VMware 虚拟机 / 28

- 1.5.2 配置 VMware 虚拟机 / 30

- 1.5.3 安装虚拟操作系统 / 31

- 1.5.4 VMware Tools 安装 / 32

2.1 确定扫描目标 / 35

- 2.1.1 确定目标主机 IP 地址 / 35
- 2.1.2 了解网站备案信息 / 38
- 2.1.3 确定可能开放的端口和服务 / 39

2.2 扫描的实施与防范 / 40

- 2.2.1 扫描服务与端口 / 41
- 2.2.2 Free Port Scanner 与 ScanPort 等常见扫描工具 / 43
- 2.2.3 扫描器 X-Scan 查本机隐患 / 44
- 2.2.4 用 SSS 扫描器扫描系统漏洞 / 49

- 2.2.5 用 ProtectX 实现扫描的反击与追踪 / 52

2.3 嗅探的实现与防范 / 54

- 2.3.1 什么是嗅探器 / 54
- 2.3.2 经典嗅探器 Iris / 54
- 2.3.3 捕获网页内容的艾菲网页侦探 / 57
- 2.3.4 使用影音神探嗅探在线视频地址 / 59

2.4 运用工具实现网络监控 / 63

3.1 系统漏洞基础知识 / 69

- 3.1.1 系统漏洞概述 / 69
- 3.1.2 Windows 操作系统常见漏洞 / 69

3.2 Windows 服务器系统入侵曝光 / 72

- 3.2.1 入侵 Windows 服务器的流程曝光 / 72
- 3.2.2 NetBIOS 漏洞攻防 / 73

3.3 DcomRpc 漏洞入侵曝光 / 78

- 3.3.1 DcomRpc 漏洞描述 / 78
- 3.3.2 DcomRpc 入侵实战 / 79
- 3.3.3 DcomRpc 防范方法 / 80

3.4 用 MBSA 检测系统漏洞 / 82

- 3.4.1 检测单台计算机 / 82
- 3.4.2 检测多台计算机 / 83

3.5 使用 Windows Update 修复系统漏洞 / 84

第4章 病毒攻防 / 86

4.1 病毒知识入门 / 87

- 4.1.1 计算机病毒的特点 / 87
- 4.1.2 病毒的三个基本结构 / 87
- 4.1.3 病毒的工作流程 / 88

4.2 两种简单病毒的生成与防范 / 88

- 4.2.1 U 盘病毒的生成与防范 / 89
- 4.2.2 Restart 病毒形成过程曝光 / 91

4.3 脚本病毒的生成与防范 / 94

- 4.3.1 VBS 脚本病毒的特点 / 94
- 4.3.2 VBS 脚本病毒通过网络传播的几种方式 / 95
- 4.3.3 VBS 脚本病毒生成机 / 95
- 4.3.4 刷屏的 VBS 脚本病毒

曝光 / 98

- 4.3.5 如何防范 VBS 脚本病毒 / 99

4.4 宏病毒与邮件病毒的防范 / 99

- 4.4.1 宏病毒的判断方法 / 99
- 4.4.2 防范与清除宏病毒 / 100
- 4.4.3 全面防御邮件病毒 / 101

4.5 网络蠕虫的防范 / 101

- 4.5.1 网络蠕虫病毒实例分析 / 101
- 4.5.2 网络蠕虫病毒的全面防范 / 102

4.6 杀毒软件的使用 / 103

- 4.6.1 用 NOD32 查杀病毒 / 103
- 4.6.2 瑞星杀毒软件 / 105
- 4.6.3 免费的个人防火墙 Zone Alarm / 107

第5章 木马攻防 / 109

5.1 认识木马 / 110

- 5.1.1 木马的发展历程 / 110
- 5.1.2 木马的组成 / 110
- 5.1.3 木马的分类 / 111

5.2 木马的伪装与生成 / 111

- 5.2.1 木马的伪装手段曝光 / 112
- 5.2.2 木马捆绑技术曝光 / 113
- 5.2.3 自解压捆绑木马曝光 / 115
- 5.2.4 CHM 木马曝光 / 117

5.3 木马的加壳与脱壳 / 120

- 5.3.1 使用 ASPack 加壳曝光 / 120

- 5.3.2 使用“北斗程序压缩”进行多次加壳 / 121

- 5.3.3 使用 PE-Scan 检测木马是否加过壳 / 122

- 5.3.4 使用 UnASPack 进行脱壳 / 123

5.4 木马清除软件的使用 / 124

- 5.4.1 用木马清除专家清除木马 / 124
- 5.4.2 用木马清道夫清除木马 / 127
- 5.4.3 在“Windows 进程管理器”中管理进程 / 128

第6章 手机黑客攻防 / 130

- 6.1 初识手机黑客 / 131
 - 6.1.1 智能手机操作系统 / 131
 - 6.1.2 常见的手机攻击类型 / 132
- 6.2 手机黑客基础知识 / 132
 - 6.2.1 获取 Android Root 权限 / 132
 - 6.2.2 Android 手机备份功能 / 134
 - 6.2.3 安卓系统刷机 / 135
 - 6.2.4 苹果手机越狱 / 137
- 6.3 手机蓝牙攻击曝光 / 139
 - 6.3.1 蓝牙的工作原理 / 139
 - 6.3.2 蓝劫攻击与防范 / 140
- 6.4 手机拒绝服务攻击曝光 / 140
 - 6.4.1 常见的手机拒绝服务攻击曝光 / 141
 - 6.4.2 手机拒绝服务攻击防范 / 141
- 6.5 手机电子邮件攻击曝光 / 141
 - 6.5.1 认识邮件在网络上的传播方式 / 142
 - 6.5.2 手机上常用的邮件系统 / 142
 - 6.5.3 手机电子邮件攻击与防范 / 142
- 6.6 手机病毒与木马攻防 / 143
 - 6.6.1 手机病毒与木马带来的危害 / 143
 - 6.6.2 手机病毒防范 / 144
- 6.7 手机加密技术 / 145
 - 6.7.1 手机开机密码设置与解密 / 145
 - 6.7.2 手机短信与照片加密 / 149
- 6.8 手机支付安全防范 / 154
 - 6.8.1 常见的5种手机支付 / 154
 - 6.8.2 手机支付安全问题 / 156
- 6.9 手机优化及安全性能的提升 / 157
 - 6.9.1 360手机卫士 / 157
 - 6.9.2 腾讯手机管家 / 157
 - 6.9.3 金山手机卫士 / 158

第7章 网游与网吧攻防 / 159

- 7.1 网游盗号木马曝光 / 160
 - 7.1.1 捆绑盗号木马过程曝光 / 160
 - 7.1.2 哪些网游账号被盗的风险高 / 161
- 7.2 解读网站充值欺骗术 / 162
 - 7.2.1 欺骗原理 / 162
 - 7.2.2 常见的欺骗方式 / 162
 - 7.2.3 提高防范意识 / 163
- 7.3 防范游戏账号破解 / 164
 - 7.3.1 勿用“自动记住密码” / 165
 - 7.3.2 防范方法 / 167
- 7.4 警惕局域网监听 / 167
 - 7.4.1 了解监听的原理 / 167
 - 7.4.2 防范方法 / 168
- 7.5 美萍网管大师 / 170

第8章 密码攻防 / 173

- 8.1 加密与解密的基础知识 / 174
 - 8.1.1 认识加密与解密 / 174
 - 8.1.2 加密的通信模型 / 174
- 8.2 七种常见的加密解密类型 / 174
 - 8.2.1 RAR 压缩文件 / 174
 - 8.2.2 多媒体文件 / 176
 - 8.2.3 光盘 / 179
 - 8.2.4 Word 文件 / 181
 - 8.2.5 Excel 文件 / 185
 - 8.2.6 宏加密解密技术 / 189
 - 8.2.7 NTFS 文件系统加密数据 / 191
- 8.3 文件和文件夹密码攻防 / 194
 - 8.3.1 文件分割巧加密 / 194
 - 8.3.2 对文件夹进行加密 / 199
 - 8.3.3 WinGuard 加密应用程序 / 202
- 8.4 系统密码攻防 / 204
 - 8.4.1 利用 Windows 7 PE 破解系统登录密码 / 204
 - 8.4.2 利用密码重置盘破解系统登录密码 / 207
 - 8.4.3 使用 SecureIt Pro 给系统桌面加把超级锁 / 210
 - 8.4.4 系统全面加密大师 PC Security / 212
- 8.5 其他加密解密工具 / 215
 - 8.5.1 “加密精灵”加密工具 / 215
 - 8.5.2 MD5 加密解密实例 / 216
 - 8.5.3 用“私人磁盘”隐藏大文件 / 217

第9章 黑客入侵检测技术 / 220

- 9.1 入侵检测概述 / 221
- 9.2 基于网络的入侵检测系统 / 221
 - 9.2.1 包嗅探器和网络监视器 / 222
 - 9.2.2 包嗅探器和混杂模式 / 222
 - 9.2.3 基于网络的入侵检测：包嗅探器的发展 / 222
- 9.3 基于主机的入侵检测系统 / 222
- 9.4 基于漏洞的入侵检测系统 / 224
 - 9.4.1 运用流光进行批量主机扫描 / 224
 - 9.4.2 运用流光进行指定漏洞扫描 / 226
- 9.5 萨客嘶入侵检测系统 / 227
- 9.6 Snort 入侵检测系统 / 230
 - 9.6.1 Snort 的系统组成 / 231
 - 9.6.2 Snort 命令介绍 / 231
 - 9.6.3 Snort 的工作模式 / 233

第10章 网络代理与追踪技术 / 234

- 10.1 代理服务器软件的使用 / 235
 - 10.1.1 利用“代理猎手”找代理曝光 / 235
 - 10.1.2 用 SocksCap32 设置动态代理曝光 / 239
 - 10.1.3 防范远程跳板代理攻击 / 242
- 10.2 常见的黑客追踪工具 / 243
 - 10.2.1 实战 IP 追踪技术 / 243
 - 10.2.2 NeroTrace Pro 追踪工具的使用 / 244

第11章 后门技术 / 247

- 11.1 认识后门 / 248
 - 11.1.1 后门的发展历史 / 248
 - 11.1.2 后门的分类 / 248
- 11.2 账号后门技术曝光 / 249
 - 11.2.1 使用软件克隆账号曝光 / 249
 - 11.2.2 手动克隆账号曝光 / 251
- 11.3 系统服务后门技术曝光 / 254
 - 11.3.1 使用 Instsrv 创建系统服务后门曝光 / 254
 - 11.3.2 使用 Srvinstw 创建系统服务后门曝光 / 255
- 11.4 检测系统中的后门程序 / 259

第12章 入侵痕迹清除技术 / 261

- 12.1 黑客留下的脚印 / 262
 - 12.1.1 日志产生的原因 / 262
 - 12.1.2 为什么要清理日志 / 265
- 12.2 清除服务器日志 / 265
 - 12.2.1 手工删除服务器日志 / 265
 - 12.2.2 使用批处理清除远程主机日志 / 267
- 12.3 Windows 日志清理工具 / 268
 - 12.3.1 elsave 工具 / 268
 - 12.3.2 ClearLogs 工具 / 269
- 12.4 清除历史痕迹 / 270
 - 12.4.1 清除网络历史记录 / 270
 - 12.4.2 使用 Windows 优化大师进行清理 / 274

第13章 远程控制技术 / 275

13.1 认识远程控制 / 276

- 13.1.1 远程控制的技术发展经历 / 276
- 13.1.2 远程控制的技术原理 / 276
- 13.1.3 远程控制的应用 / 276

13.2 远程桌面连接与协助 / 277

- 13.2.1 Windows 系统的远程桌面连接 / 277
- 13.2.2 Windows 系统远程关机 / 280

13.2.3 区别远程桌面与远程协助 / 281

13.3 用 WinShell 实现远程控制 / 282

- 13.3.1 配置 WinShell / 282
- 13.3.2 实现远程控制 / 284

13.4 用 QuickIP 进行多点控制 / 285

- 13.4.1 设置 QuickIP 服务器端 / 285
- 13.4.2 设置 QuickIP 客户端 / 286
- 13.4.3 实现远程控制 / 287

第14章 局域网攻防 / 288

14.1 局域网安全介绍 / 289

- 14.1.1 局域网基础知识 / 289
- 14.1.2 局域网安全隐患 / 289

14.2 局域网攻击曝光 / 290

- 14.2.1 网络剪刀手 Netcut 切断网络连接曝光 / 290

14.2.2 局域网 ARP 攻击工具 WinArp Attacker 曝光 / 292

14.2.3 网络特工监视数据曝光 / 294

14.3 局域网监控工具 / 297

- 14.3.1 LanSee 工具 / 297
- 14.3.2 长角牛网络监控机 / 299

第15章 QQ 账号攻防 / 305

15.1 QQ 号码盗取防范 / 306

- 15.1.1 “QQ 简单盗”盗取 QQ 密码曝光与防范方法 / 306
- 15.1.2 “好友号好好盗”盗取 QQ 号码曝光 / 307
- 15.1.3 “QQExplorer”在线破解 QQ

号码曝光与防范方法 / 309

15.2 保护 QQ 密码和聊天记录 / 310

- 15.2.1 定期修改 QQ 密码 / 310
- 15.2.2 申请 QQ 密保 / 311
- 15.2.3 加密聊天记录 / 312

第16章 网站攻防 / 313

16.1 SQL 注入攻击曝光 / 314

- 16.1.1 Domain(明小子)注入曝光 / 314
- 16.1.2 啊 D 注入曝光 / 317
- 16.1.3 对 SQL 注入漏洞的防范 / 321

16.2 ZBSI 检测注入点曝光 / 322

16.3 Cookie 注入攻击曝光 / 323

16.3.1 IECookiesView 搜寻 Cookie 文件数据曝光 / 324

16.3.2 Cookie 注入曝光 / 325

16.4 跨站脚本攻击曝光 / 326

16.4.1 简单留言本的跨站漏洞 / 326

16.4.2 跨站漏洞的利用 / 329

16.4.3 对跨站漏洞的预防措施 / 334

第17章 系统和数据的备份与恢复 / 336

17.1 备份与还原操作系统 / 337

17.1.1 使用还原点备份与还原系统 / 337

17.1.2 使用 GHOST 备份与还原系统 / 339

17.2 备份与还原用户数据 / 344

17.2.1 使用驱动精灵备份与还原驱动程序 / 344

17.2.2 备份与还原 IE 浏览器的收藏夹 / 345

17.2.3 备份和还原 QQ 聊天记录 / 348

17.2.4 备份和还原 QQ 自定义表情 / 350

17.3 使用恢复工具来恢复误删除的数据 / 354

17.3.1 使用 Recuva 来恢复数据 / 354

17.3.2 使用 FinalData 来恢复数据 / 358

17.3.3 使用 FinalRecovery 恢复数据 / 362

第18章 保障网络支付工具的安全 / 365

18.1 加强支付宝的安全防护 / 366

18.1.1 加强支付宝账户的安全防护 / 366

18.1.2 加强支付宝内资金的安全防护 / 369

18.2 加强财付通的安全防护 / 373

18.2.1 加强财付通账户的安全防护 / 373

18.2.2 加强财付通内资金的安全防护 / 376

第19章 间谍软件的清除和系统清理 / 379

19.1 流氓软件的清除 / 380

19.1.1 清理浏览器插件 / 380

19.1.2 流氓软件的防范 / 382

19.1.3 金山清理专家清除恶意软件 / 385

19.2 间谍软件防护实战 / 387

19.2.1 间谍软件防护概述 / 387

19.2.2 用 Spy Sweeper 清除间谍

软件 / 387

19.2.3 微软反间谍专家 Windows Defender / 389

19.3 常见的网络安全防护工具 / 391

19.3.1 浏览器绑架克星 HijackThis / 391

19.3.2 诺盾网络安全特警 / 394

第1章

从零开始认识黑客

要学习黑客知识，就得了解进程、端口、IP 地址以及黑客常见的术语和命令。由于初学者对这方面知识了解不多，本章专门针对上述内容进行讲解，从而帮助读者为后面的学习打好基础。

要点提示

- 黑客常用术语
- 进程和端口
- 常见的网络协议
- 黑客常用命令
- 创建虚拟测试环境