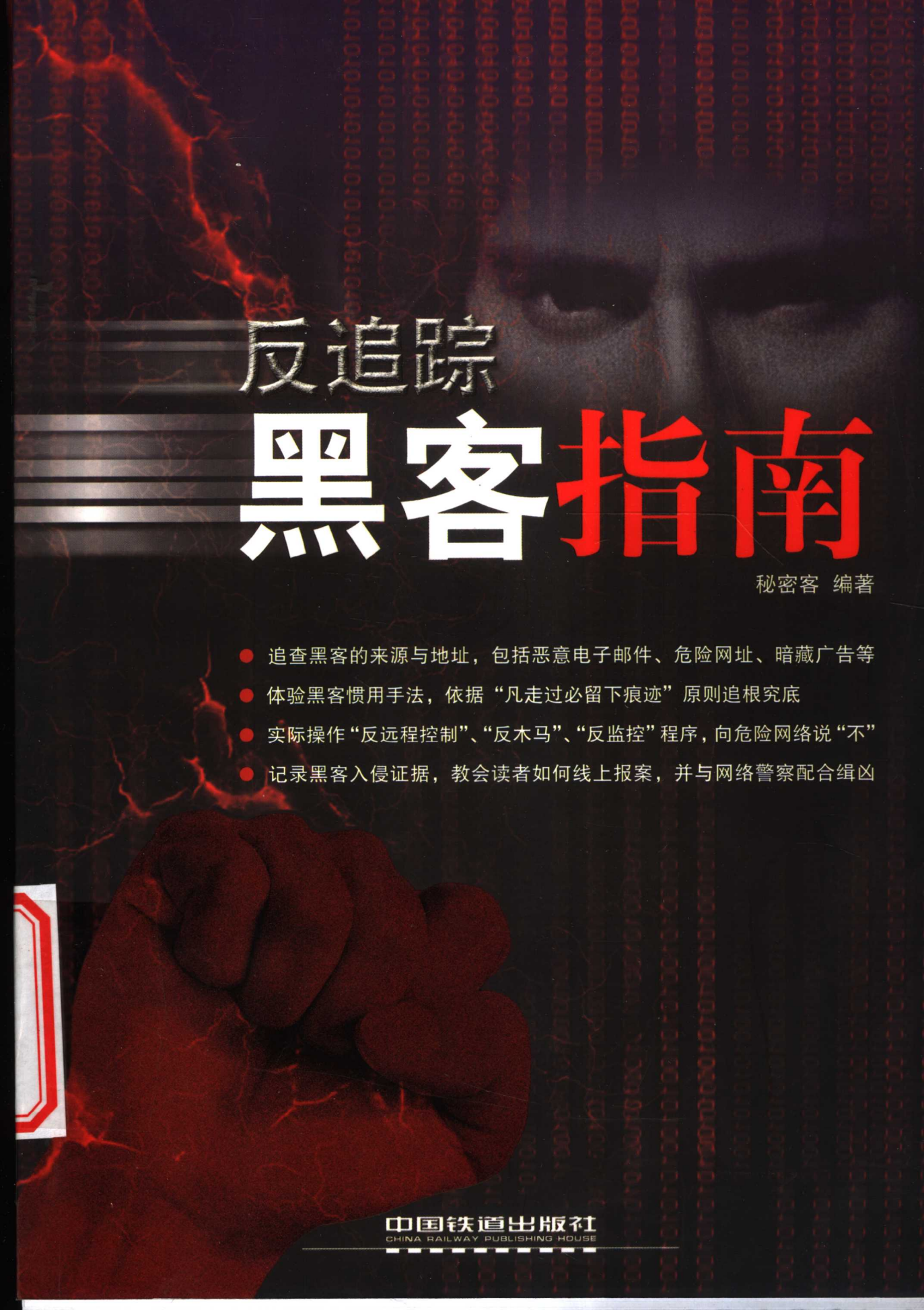




反追踪

黑客指南

秘密客 编著

- 追查黑客的来源与地址，包括恶意电子邮件、危险网址、暗藏广告等
- 体验黑客惯用手法，依据“凡走过必留下痕迹”原则追根究底
- 实际操作“反远程控制”、“反木马”、“反监控”程序，向危险网络说“不”
- 记录黑客入侵证据，教会读者如何线上报案，并与网络警察配合缉凶

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

反追踪黑客指南

秘密客 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

北京市版权局著作权合同登记 图字：01-2006-4839 号

版 权 声 明

本书中文繁体字版为台湾碁峯资讯股份有限公司所有，本书中文简体字版经台湾碁峯资讯股份有限公司授权由中国铁道出版社出版。任何单位或个人未经出版者书面允许，不得以任何手段复制或抄袭本书内容。

图书在版编目 (CIP) 数据

反追踪黑客指南/秘密客编著. —北京：中国铁道出版社，2006.8

ISBN 7-113-07449-9

I. 反... II. 秘... III. 计算机网络—安全技术—指南 IV. TP393.08-62

中国版本图书馆 CIP 数据核字 (2006) 第 102134 号

书 名：反追踪黑客指南

作 者：秘密客

出版发行：中国铁道出版社（100054，北京市宣武区右安门西街8号）

策划编辑：严晓舟 魏 春

责任编辑：苏 茜 荆 波

特邀编辑：彭立辉

封面设计：高 洋

责任校对：王 欣

印 刷：北京鑫正大印刷有限公司

开 本：787×1092 1/16 印张：16 字数：362 千

版 本：2006 年 10 月第 1 版 2006 年 10 月第 1 次印刷

印 数：1~5 000 册

书 号：ISBN 7-113-07449-9/TP·2052

定 价：25.00 元

版权所有 侵权必究

凡购买铁道版的图书，如有缺页、倒页、脱页者，请与本社计算机图书批销部调换。

出版说明

在电影或电视中，人们经常可以看到关于黑客的题材，在报章杂志上也经常能看到某机构被黑客入侵的新闻。本书将介绍追击黑客、分析黑客以及防止黑客的方法，同时也将介绍计算机遭受黑客攻击、入侵后的解决方法。

本书是一本分析追踪黑客攻击技术、行为的书籍，主要内容包括“反远程控制”、“反监控”、“反漏洞”以及“恢复被入侵的系统”等。通过反黑客的专用工具，可使读者学会独立追查黑客攻击的日志、分析黑客的存取行为，进而养成洞穿黑客手法的能力，从而更加有效地防止黑客入侵。

本书首先针对黑客做了一个概略性的介绍，包括黑客的历史、黑客的网站、黑客的攻击手法等。然后，逐章介绍防范黑客的方法，包括反病毒、反蠕虫、反木马、反按键记录等，并说明如何测试黑客计算机，反查黑客所属区域，进而反追踪黑客。最后，还介绍了各种保护计算机的方法，包括防御黑客的各种程序、反数据包拦截、防火墙监控等，并介绍了如何加密数据、快速还原系统、彻底杜绝黑客入侵的方法。整体来说，大致的内容整理如下：

- ① 解析网络连线行为，针对数据包内容进行分析，包括 FTP、Web、E-mail 等。
- ② 追查黑客的来源与地址，包括恶意的电子邮件、危险的网址、暗藏的广告等。
- ③ 体验黑客惯用的手法，依据“凡走过必留下痕迹”原则追根究底。
- ④ 实做“反远程控制”、“反木马”、“反监控”程序，拒绝访问危险的网络。
- ⑤ 记录黑客入侵证据，介绍如何在线报案，与网络警察配合缉凶。

学习完本书，将能彻底了解黑客入侵的各种手法，拥有查出非法连线以及拦截与分析黑客的能力。

本书由台湾碁峯资讯股份有限公司提供版权，经中国铁道出版社计算机图书中心审选，由碁峯资讯股份有限公司完成整稿工作。

中国铁道出版社

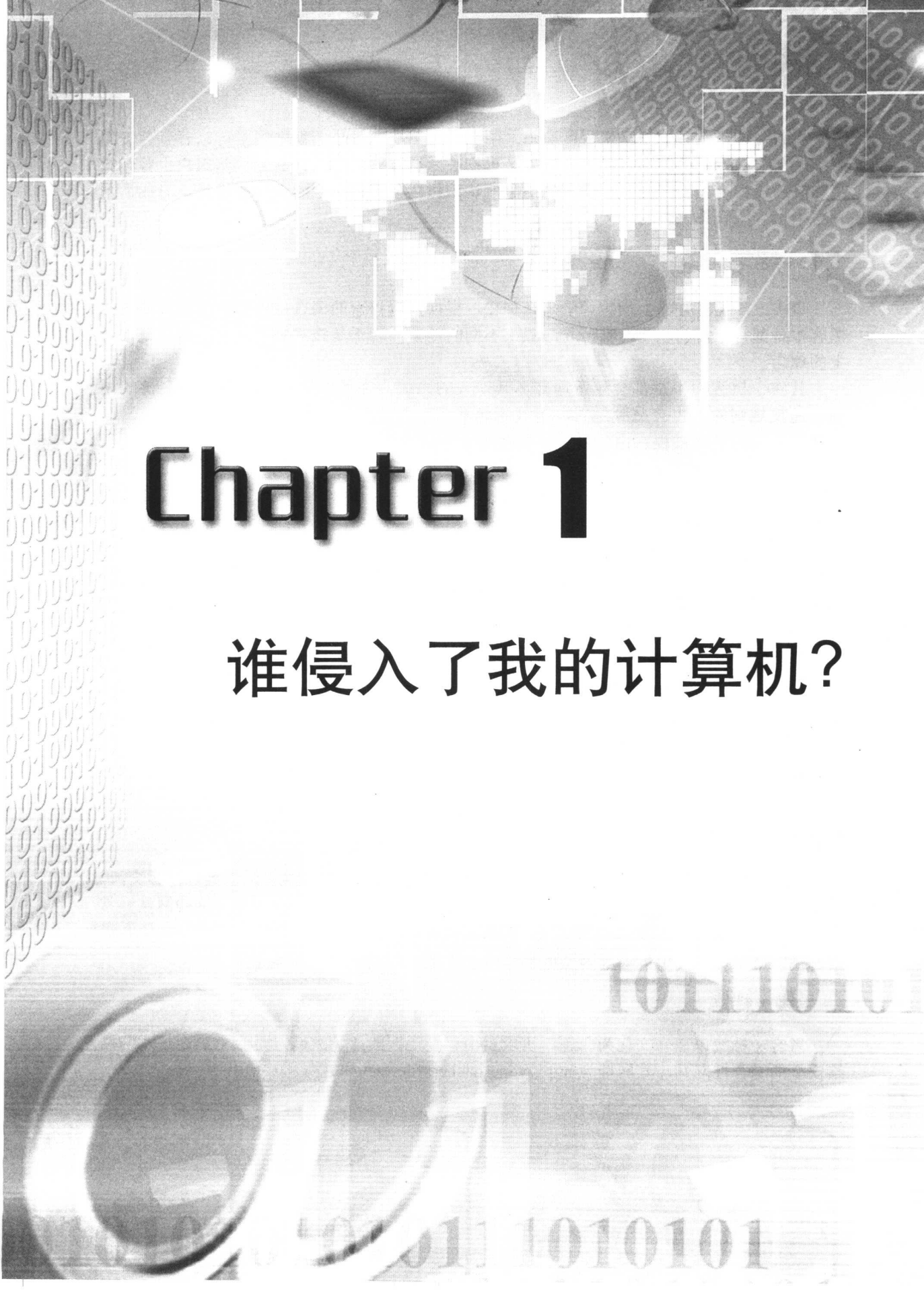
2006 年 9 月

目 录

Chapter 1 谁侵入了我的计算机?	1
1.1 解密黑客	2
1.2 黑客集散地	2
1.2.1 黑客网站	2
1.2.2 黑客杂志	9
1.2.3 黑客常用的搜索引擎	9
1.3 黑客的攻击手法	12
Chapter 2 反病毒	15
2.1 分析病毒	16
2.1.1 认识病毒	16
2.1.2 认识蠕虫病毒	18
2.2 病毒入侵	19
2.2.1 病毒感染计算机的途径	19
2.2.2 常见的病毒入侵	20
2.3 追踪病毒	21
2.3.1 流行的杀毒软件	21
2.3.2 实战防病毒	22
2.4 病毒的预防	35
Chapter 3 反木马程序	39
3.1 木马程序	40
3.1.1 木马如何入侵	40
3.1.2 木马程序的种类	46
3.2 反追踪木马程序	48
3.2.1 以防火墙监控木马	48
3.2.2 清除木马程序	69
3.3 做好还原计算机的准备工作	71
3.3.1 备份系统分区	72
3.3.2 还原系统分区	75
3.3.3 制作灾难恢复启动盘	79
3.3.4 灾难恢复	83

Chapter 4 反键盘记录	87
4.1 认识键盘记录	88
4.1.1 键盘记录的手法	88
4.1.2 常见的键盘记录程序	89
4.1.3 硬件的键盘记录设备	92
4.2 反查键盘记录程序	92
4.2.1 检查与删除暗藏的键盘记录程序	92
4.2.2 专门对付键盘记录的防火墙	99
Chapter 5 扫描黑客	107
5.1 测试黑客计算机	108
5.1.1 Ping 命令	108
5.1.2 取得黑客的路由表	112
5.1.3 反查黑客的域名	114
5.2 认识端口扫描程序	117
5.2.1 什么是端口扫描程序	117
5.2.2 端口种类介绍	117
5.2.3 常见的端口扫描程序	118
5.3 端口扫描程序实战	122
5.3.1 Retina Network Security Scanner	122
5.4 反查黑客所属区域	131
Chapter 6 防御黑客程序	137
6.1 常见的黑客攻击程序	138
6.1.1 电子邮件附件攻击	138
6.1.2 DoS 攻击	138
6.1.3 聊天软件攻击	139
6.2 防御电子邮件附件攻击	140
6.3 防御 DoS 攻击	143
6.4 防御来自聊天软件的攻击	148
6.5 防御来自局域网的攻击	151
Chapter 7 反数据包拦截	163
7.1 认识数据包的拦截	164
7.1.1 认识 Sniffer	164
7.1.2 常见的 Sniffer 软件	164
7.2 拦截数据包	166
7.2.1 检测局域网中的密码是否安全	166
7.2.2 检测局域网内的数据安全	172

7.3 反制数据包拦截行为	183
7.3.1 硬件设备反制数据包拦截的行为	183
7.3.2 加密无线网络数据包的传送	183
Chapter 8 入侵检测与防火墙监控黑客	187
8.1 入侵检测	188
8.1.1 认识入侵检测	188
8.1.2 执行入侵检测	189
8.2 黑客专用的防火墙	192
8.2.1 天网防火墙的功能	193
8.2.2 访问控制与明文警告	194
8.2.3 应用程序网络使用情况	195
8.2.4 导入官方安全规则库	196
8.2.5 添加病毒 IP 规则	199
8.2.6 日志检查与保存	201
8.2.7 接通断开的网络	202
8.3 检查 Windows 事件查看器	203
8.3.1 检查 Windows 事件查看器	203
8.3.2 免费的在线日志扫描	206
8.3.3 检查 Windows 服务器日志	208
Chapter 9 快速复原系统	211
9.1 删除间谍软件	212
9.1.1 间谍软件简介	212
9.1.2 删除间谍软件	213
9.2 还原文件注册类型	222
9.3 还原损坏的文件	225
Chapter 10 保护自己的计算机	227
10.1 密码保卫战	228
10.1.1 建立用户密码	228
10.1.2 更改密码	231
10.1.3 遗忘密码后的解决方法	233
10.2 加密计算机信息	238
10.2.1 加密文件夹及文件	239
10.2.2 与其他用户共享加密文件	241
10.2.3 解密文件及文件夹	243
10.3 隐藏在磁盘中的文件夹	245
10.3.1 隐藏文件夹	245
10.3.2 取消隐藏	247



Chapter 1

谁侵入了我的计算机？

黑客一词对于一般用户来说既熟悉又陌生，虽然在电影或电视中经常可以看到关于黑客的题材，在报章杂志上也经常能看到某机构被黑客入侵的新闻，甚至一些用户也曾经有被黑客入侵的经历。但是，在现实生活中能认识黑客、了解黑客的人仍然很少。对此，本章将概括介绍有关黑客的一些内容。

1.1 解密黑客

事实上，黑客并非人们想像中那么神秘，根据一份秘密的调查报告显示，绝大多数的黑客本身都有正常的职业，唯一与一般人不同的是，黑客都是技术狂热分子，信奉技术至上的理念。

其实，黑客并不是都会随意地破坏其他人的系统，在黑客的世界里也有一套游戏规则，违反规则的人也会遭到惩罚。寻找系统漏洞、入侵系统、通知系统管理员修补漏洞是黑客入侵的经典过程，由此可见，黑客对于网络安全功不可没。

在黑客的世界中也有善恶之分，除了那些信奉技术至上的“正统”黑客外，还存在着另一种黑客通常我们称之为骇客，称为 **Dark-side-Hacker** 或者 **Cracker**。这些人同样具有深厚的计算机技术知识，但是他们却以破坏为乐，其中有一些黑客甚至还受雇于某些公司，为其窃取竞争对手的资料。人们平时所看到关于黑客的报导，绝大部分都是有关 **Cracker** 的内容，真正的黑客对于这些破坏行为其实是非常反感的。一般来说，由于真正的黑客不容易受到人们的注意，因此绝大部分的人都已经把 **Cracker** 当成了黑客。为了叙述方便，本书以后的内容将统一使用“黑客”这个称谓，而不再对两者进行区分。

说明：1.3 节以后所涉及的黑客指的是 **Cracker**。

1.2 黑客集散地

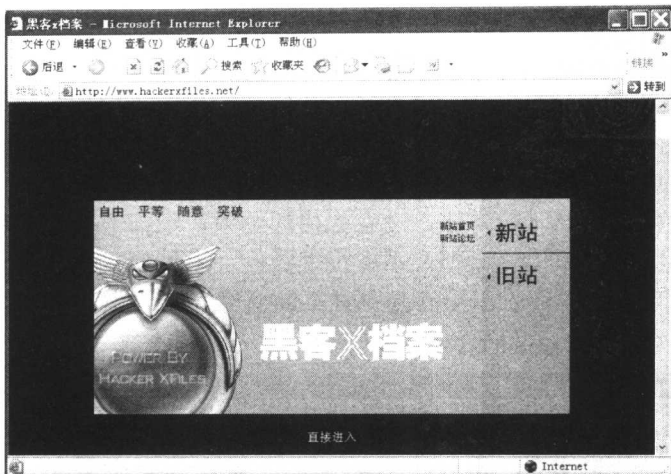
在日常生活中人们难免要与黑客打交道，为了方便交流经验，黑客往往会通过各种方式聚集在一起，例如网站、聊天软件以及黑客杂志等都是黑客的集散地。

1.2.1 黑客网站

网站是黑客互相交流经验的场所，许多网站还专门开设了讨论区，以供黑客互相交流，甚至还有一些为入门黑客开设的讨论区，这类网站在国外及国内都非常多。这些网站经常会发布一些最新的系统安全漏洞信息，因此是黑客最钟爱的地方。下面将介绍一些黑客经常光顾的网站，读者也可通过浏览这些网站，增进对黑客的了解。

● 黑客 x 档案

黑客 x 档案以黑客文化为主题，讲求自由、平等、随意、突破，是一个黑客技术与网络安全的综合性网站，其网址为 <http://www.hackerxfiles.net>。



● 中国鹰派联盟

中国老牌黑客组织【绿色兵团】的成员万涛是中国鹰派联盟的创始人。

网名: eagle,chinaeagle

籍贯: 江西

成立中国鹰派联盟并不是他自发的。他经常在网上军事论坛发帖子, 因此有人鼓励他成立俱乐部, 于是在酝酿了一年多后, 成立了中国鹰派联盟。

【我不是黑客】

“之所以说我不是黑客, 是因为人们对黑客有误解。黑客是有道义、有良知的技术高手, 他与黑客的区别是在进入别人的计算机以后, 一个是善意提醒或悄然离开, 而另一个则大肆破坏。黑客正如侠客, 他是在破坏一些秩序, 但是这种反秩序的行为是为了秩序更趋于合理。中国鹰派认为, 黑客是未来信息社会重要的平衡力量。”

中国鹰派联盟的网址为 <http://www.chinawill.com/>。



● netXeyes

流光软件开发者的个人网站。

网名：小榕

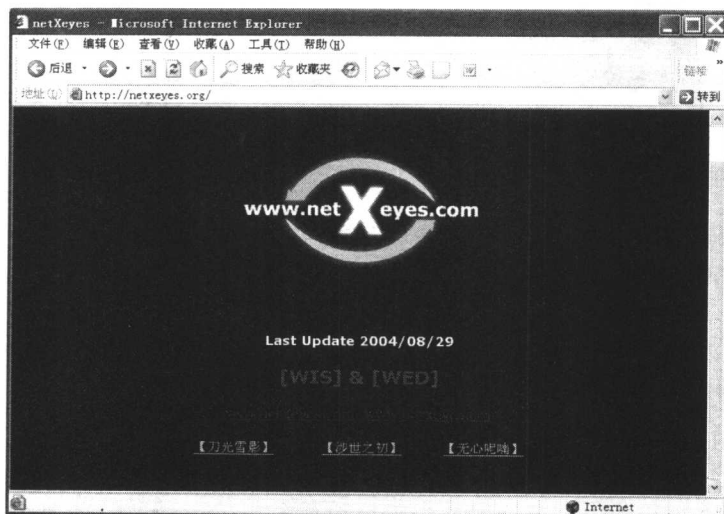
格言：无论在现实或是网络中，我都是孤独的.....

稍有点黑客知识的人，没有不知道流光这个软件的，而小榕就是这个软件的开发者。小榕毋庸置疑是国内目前的顶级黑客，他开发的流光软件是众多小黑客必用的软件之一。

父亲是大学教授的小榕，对黑客的道德观认识得非常清楚：

“黑客像美国西部开发时的牛仔，没有法律的约束，但却有自己的做事准则。黑客要有道德底线，小榕的三条做黑客原则：不能仇视社会，不能给别人制造麻烦，不能给别人带来损失。有人对黑客这样评价：黑客是一种不断研究不断探索的境界”。

netXeyes 的网址为：<http://netxeyes.org/>。



● FETAG.ORG

一代宗师 CoolFire 的个人网站。

网名：CoolFire, Fetag

真名：林正隆

籍贯：中国台湾

林正隆是中国黑客界大师级的人物，他曾经用 CoolFire 这个网名发表过 8 篇黑客入门级的文章，许多人都非常熟悉这样的开头：“这不是一个教学文件，它只是告诉你该如何破解系统，好让你能够将自己的系统做安全的保护，如果你能够将这份文件完全看完，你就能够知道电脑黑客们是如何入侵你的电脑，我是 CoolFire，写这篇文章的目的是要让大家明白电脑安全的重要性，并不是教人 Crack Password”。

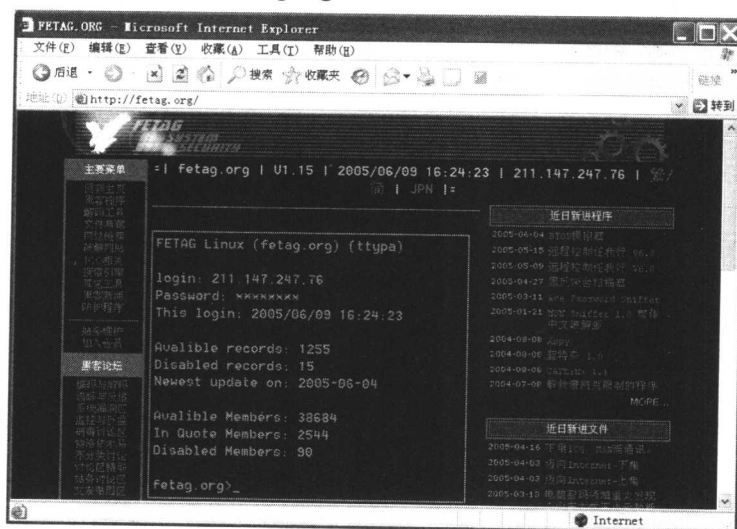
以上是 CoolFire 写的黑客守则，尽管是个人的观点，其中也不乏可取的地方，但是许多人还是将其当作在虚拟世界的一种游戏规则：

不恶意破坏任何系统；恶意破坏他人的软件将导致法律责任；如果只是使用计算机，则仅为非法使用。注意：千万不要破坏别人的软件或资料。

不要修改任何系统文件，如果是为了要进入系统而修改它，可在达到目的后将其改回原状。

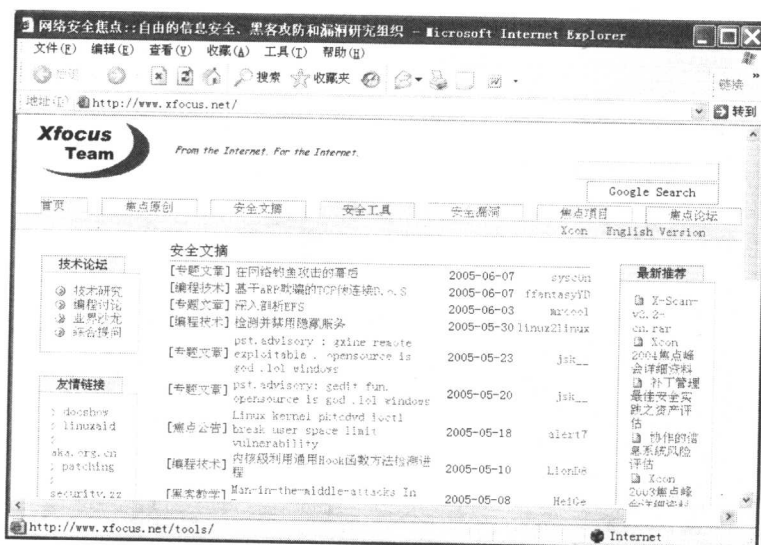
不要輕易地將你要 Hack 的网站告诉不信任的朋友。

不要在 BBS 上谈论你 Hack 的任何事情。
 在公布文章时不要使用真名。
 正在入侵的时候, 不要随意离开计算机。
 不要侵入或破坏政府机关的主机。
 不要在电话中谈论你 Hack 的任何事情。
 将笔记放在安全的地方。
 FETAG.ORG 的网址为 www.fetag.org。



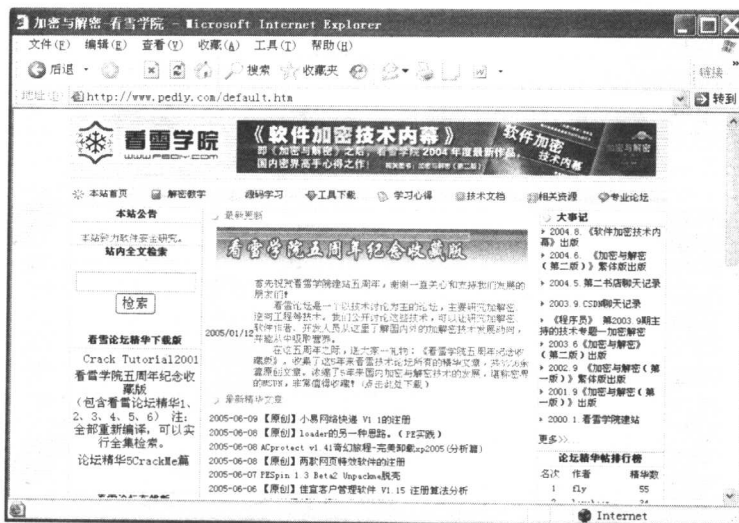
安全焦点

安全焦点是国内目前最顶级的网络安全站点, 其中云集的大批知名黑客足以让其他所有的黑客团体黯然失色。他们开发的网络安全软件已经成为众多网站必选的产品。安全焦点的网址为 <http://www.xfocus.net/>。



● 看雪学院

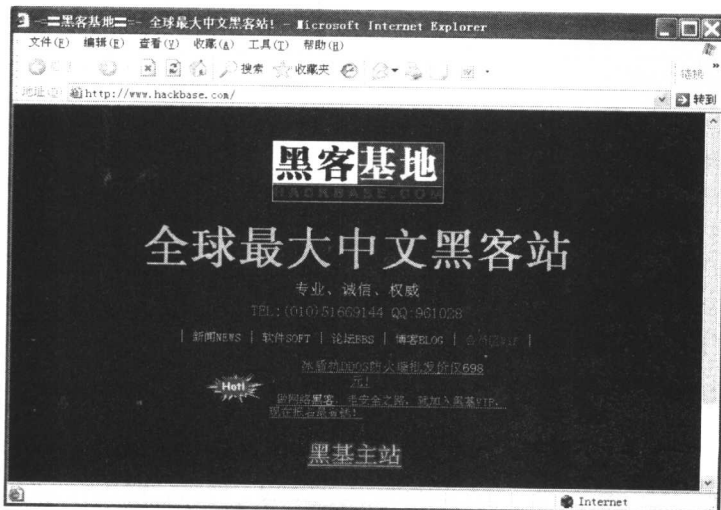
看雪学院网站是国内顶级的破解论坛、资深的软件加解密技术性网站，主要研究加解密、逆向工程等，其网址为 <http://www.pediy.com/>。



● 黑客基地

黑客基地是由国内外大型IT公司和安全公司的网络精英和安全专家共同联合发起设立，专门从事黑客技术与安全防范研究的非赢利性组织。黑客基地拥有国内最大、最强的黑客安全技术团队，黑客基地成员以前均为高水平的黑客高手，精通漏洞、木马、病毒、蠕虫、攻击/反攻击技术，深刻理解黑客技术精髓，有着丰富的黑客经验，掌握着最新的黑客和反黑客技术，不仅能够实施最强的黑客渗透攻击，而且能够采取最高强度的安全防范措施。

黑客基地的网址为 <http://www.hackbase.com/>。



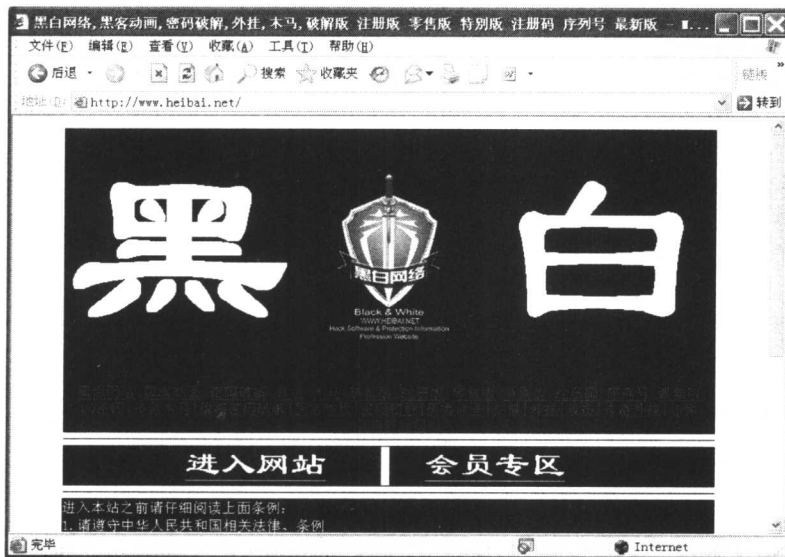
● 中国 X 黑客小组

中国 X 黑客小组是一个集黑客技术、安全防御、编程技术于一体的黑客网站，内容比较新颖，其网址为 <http://www.cnxhacker.com/>。



● 黑白网络

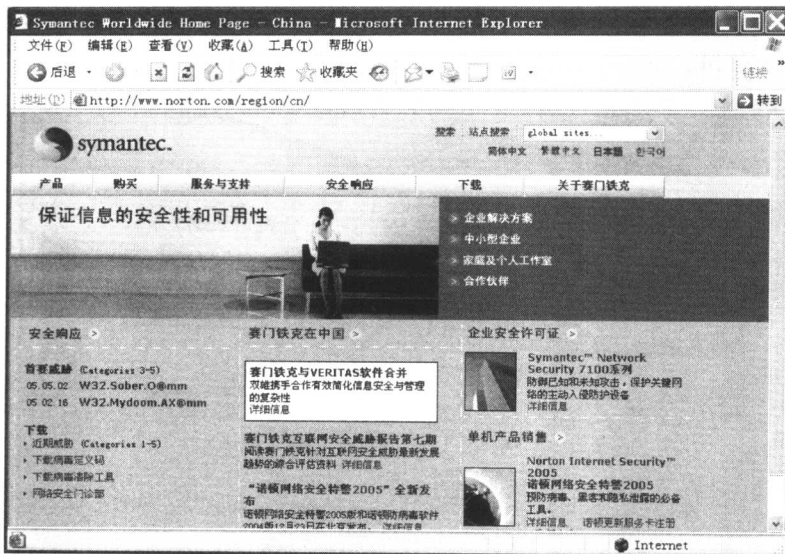
黑白网络主要介绍各种黑客软件、黑客教程及黑客技术等，其网址为 <http://www.heibai.net/>。



● 赛门铁克

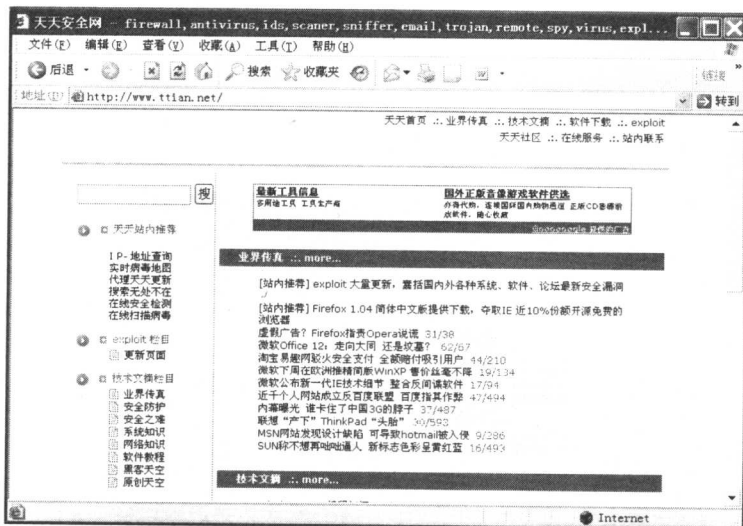
赛门铁克是全球著名的信息安全企业，在安全领域具有相当权威的地位，正因为如此，

其官方提供的技术文件也成为黑客的理想教材。赛门铁克的网址为 <http://www.norton.com/region/cn>。



● 天天安全网

天天安全网是国内一个相当著名的黑客网站，除了提供大量黑客软件及黑客教程外，还提供最新的黑客软件升级信息以及系统、软件的相关安全新闻，其网址为 <http://www.ttian.net/>。



● Microsoft

作为全球最大的个人计算机操作系统开发商，Microsoft（微软）的官方网站上有大量的技术文件，这些文件都是黑客感兴趣的目標。此外，微软为了使其操作系统更安全，每当发现漏洞时就会立即在其官方网站发布系统补丁。但这样做反而为黑客了解操作系统的漏洞提供了方便。微软的中文网址为 <http://www.microsoft.com/china>。



以上介绍的只是黑客经常光顾的一部分网站, 如果想了解更多此类网站, 可通过本章后续介绍的搜索引擎进行搜索。

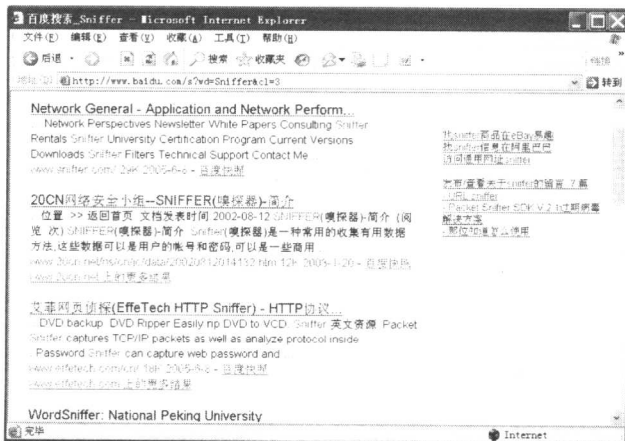
1.2.2 黑客杂志

黑客杂志也是黑客交流经验及了解最新信息的途径之一, 世界上有很多国家都没有明文规定不能出版黑客杂志, 因此黑客杂志在某些国家是非常流行的。此外, 由于黑客技术与网络安全本身有着紧密的关系, 因此也有一些黑客杂志公然打着网络安全的旗号出版, 例如黑客 x 档案、看雪论坛等网站都有期刊出版, 并且会出一些电子版书籍, 供用户有偿下载。

值得一提的是, 一些黑客杂志也有相关的官方网站, 在这些网站上能看到部分杂志的内容。因此在无法购买到杂志的情况下, 用户也可通过网站了解关于黑客的信息。

1.2.3 黑客常用的搜索引擎

网络上与黑客相关的信息虽然很多, 但是这些信息往往非常杂乱, 即使是有经验的黑客也难以在网站中找出自己需要的信息, 因此黑客常会借助搜索引擎来寻找信息。例如, 某黑客在使用某个 Sniffer 软件时遇到了困难, 但一时又找不到关于这个软件的说明, 此时就可以通过搜索引擎在网络上寻找相关的信息。

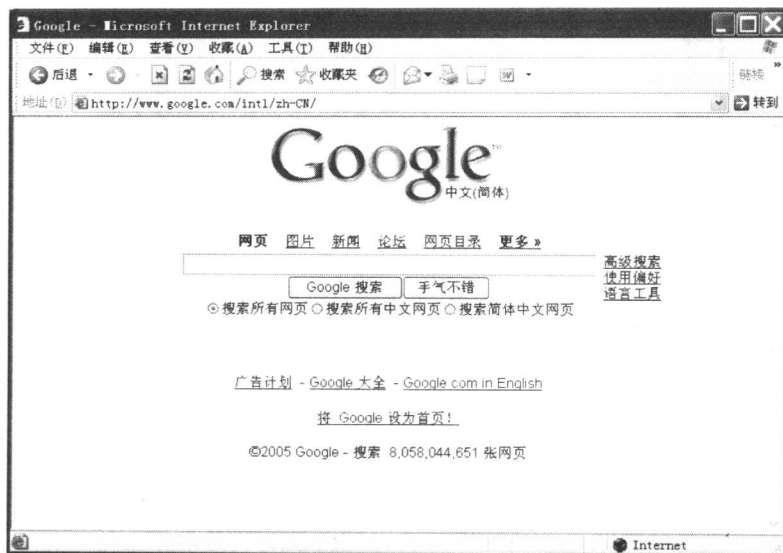




合理地利用搜索引擎，可以获得大量有用的信息，下面将介绍一些功能比较强大的搜索引擎。

● Google

Google 是世界上用户数量最多的搜索引擎之一，以搜索功能强大而著称，但其缺点是搜索的结果较为散乱，用户必须从中筛选出有用的信息。Google 的网址为 <http://www.google.com/>。



● Yahoo!

Yahoo!的搜索引擎也是黑客常用的引擎之一，与 Google 相比，Yahoo! 的功能显然要弱一些，但由于 Yahoo! 的搜索结果是经过精心筛选的，因此搜索的准确性要高于 Google，用户更容易从搜索结果中找出所需要的信息。yahoo!搜索引擎的网址为 <http://cn.search.yahoo.com/>。

