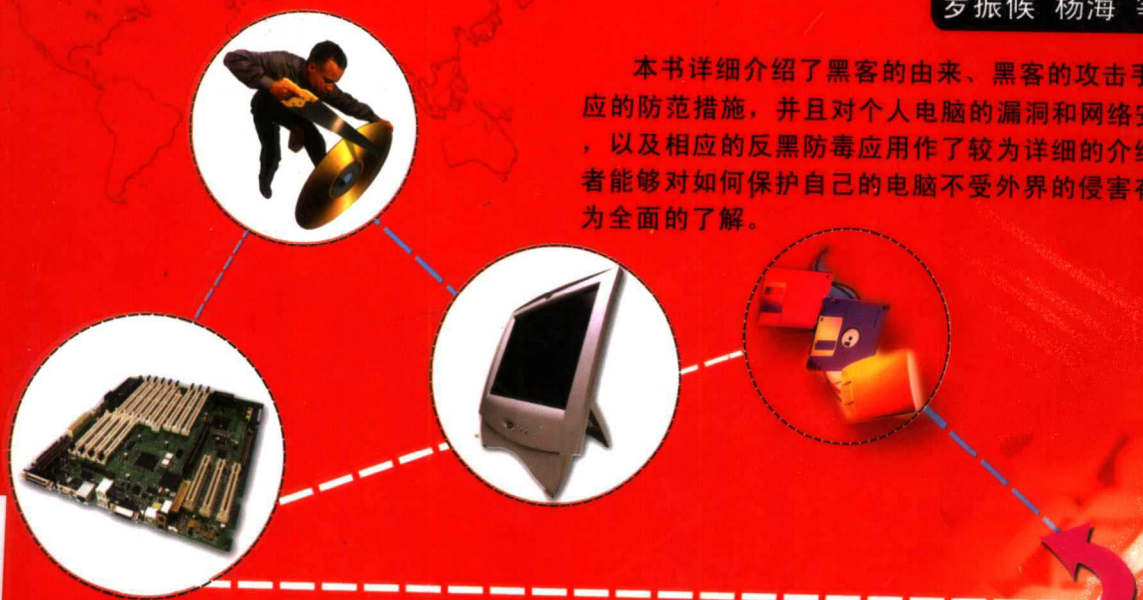
中国电脑教育报
CCID CHINA COMPUTER EDUCATION

黑客秘技万事通

罗振候 杨海 等编著

本书详细介绍了黑客的由来、黑客的攻击手段及相应的防范措施，并且对个人电脑的漏洞和网络安全知识，以及相应的反黑防毒应用作了较为详细的介绍，使读者能够对如何保护自己的电脑不受外界的侵害有一个较为全面的了解。



上海科学普及出版社

黑客秘技万事通

罗振候 杨海 等 编著

上海科学普及出版社

图书在版编目（CIP）数据

黑客秘技万事通 / 罗振候等编著. —上海：上海科学普及出版社，2005.11
ISBN 7-5427-2908-X

Ⅰ.黑… Ⅱ.罗… 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（2005）第 099882 号

策划编辑 胡名正
责任编辑 徐丽萍

黑客秘技万事通
罗振候 杨海 等编著
上海科学普及出版社出版发行
（上海中山北路 832 号 邮政编码 200070）
http://www.pspsh.com

各地新华书店经销 北京市燕山印刷厂印刷
开本 787×1092 1/16 印张 21.5 字数 512000
2005 年 11 月第 1 版 2005 年 11 月第 1 次印刷
印数 1—7100

ISBN 7-5427-2908-X/ TP · 650 定价：29.50 元

内容提要

本书由浅入深地介绍了黑客的由来、黑客的攻击手段及相应的防范措施，并且对个人电脑的漏洞和网络安全知识，以及相应的反黑防毒应用作了较为详细的介绍，使读者能够对如何保护自己的电脑不受外界的侵害有一个较为全面的了解。同时，本书还列举了各种病毒和木马的攻击与防范实例，指导读者针对各种不同的情况，使用正确的方法来解决具体问题，使自己的电脑能够安全地工作。另外，本书还给出了各种不同的计算机端口和网络命令的高级运用，使读者阅读本书后能对自己的电脑及网络构架有一个深入的了解，能够防范各种常见的黑客攻击，成为一个反黑防毒的高手。

本书内容新颖、详实，操作步骤详细明了，思路清晰，技巧丰富，并穿插有相应的提示和专业基础知识，使读者能真正做到理论与实践相结合。

本书适合不同水平层次的电脑爱好者，对一般的用户来说是一本较好的指导书籍，对专业计算机人士来说，也是一本很有参考价值的工具类书籍。

前　言

在黑客日益猖獗的今天，越来越多的电脑用户遭到黑客的威胁和侵害，但是黑客是通过何种途径入侵自己的电脑，自己的电脑又存在哪些不安全的因素呢？很多电脑用户对这方面的知识还是很缺乏。而且现在各种病毒和木马泛滥，每周都会有新的病毒出现，用户如何发现自己的电脑是否受到了病毒或者木马的侵袭，又该如何清除这些病毒和木马呢？也许大多数电脑用户对此还没有很好的办法。

针对上述一系列问题，我们参阅了大量的相关文献和资料，并总结了各位电脑高手的宝贵经验，编写了《黑客秘技万事通》一书。书中对黑客的攻击手段、各种电脑系统存在的漏洞和各种病毒、木马的防范进行了详尽的介绍，并使读者能在较短的时间内掌握注册表中关于电脑和网络安全方面的基础知识。同时本书还列举了各种常见的攻击实例，使读者能依照本书自己解决在使用电脑时所遇到的各种常见的黑客问题。另外，读者通过对本书中有关网络安全章节内容的学习，能够对如何构建一个较为安全的网络有比较全面的了解，并使自己的电脑能够工作在相对安全的环境中。本书有如下几个特点：

■ 内容详实

本书精心收录了日常使用电脑时会遇到的各种病毒或者木马攻击实例，并且对每一个实例都给出具体可行的解决办法，使读者能够根据本书的指导独立地解决在日常使用电脑时所遇到的各种常见黑客问题。

■ 内容新颖

本书挑选的例子多以最新或者最常见的病毒和木马攻击为主，能够满足绝大部分读者的需要。

■ 分类详细，便于查找

本书将各种黑客攻击针对不同的对象进行了分类，有专门独立的 MSN 和 QQ 章节、电子邮件章节、网络游戏章节、密码章节等，便于用户针对具体的情况进行查找。

■ 语言通俗易懂

本书的文字叙述力求简洁明了，通俗易懂，并在各个操作步骤中配有相关插图与提示栏，使读者无师自通。

全书共分为 14 章：第 1 章主要介绍黑客的由来及其特点；第 2 章主要介绍网络安全的基础知识；第 3 章到第 5 章则分别介绍黑客的入侵手段及防范措施、各种操作系统的漏洞；从第 6 章开始则以不同的章节分类介绍各种黑客或者病毒、木马攻击的实例及相应的防范措施；第 14 章介绍几种常见防火墙软件的使用。

上海振业电子科技有限公司组织本书的编写。本书主要由罗振候、杨海编写，杨万里高级工程师主审，参加本书编写的还有李骥、汪浩栋等人，在此一并感谢。

由于编者水平有限，又加上时间仓促，错误与不足之处在所难免，如读者在阅读过程中有什么意见或建议，请与我们联系，E-mail 发至 **heroyh@sina.com.cn**。

编　者

2005 年 8 月

目 录

第 1 章　当今黑客与网络安全

1.1　认知黑客

提起黑客，总是那么神秘莫测。在羡慕者的眼中，他们是一些聪明绝顶、翱翔于网络空间的自由之神；在受害者眼中，他们是放荡不羁、作恶多端的害群之马，是不折不扣的电脑捣蛋分子。

那么黑客究竟是伊甸园里的那条蛇还是为人类盗来火种的普罗米修斯？是人类共同的罪犯抑或电子时代的牛仔？黑客又怎么跟电脑捣蛋分子联系在一起的呢？我们想通过本章的漫谈撩开黑客的神秘面纱。

1.1.1　黑客定义及其基本态度

“黑客”（Hacker）源于英语动词 hack，意为“劈砍”，引伸为干一件非常漂亮的工作。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤其指那种手法巧妙、技术高明的恶作剧。而日本的《新黑客词典》中，把黑客定义为：“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”微软公司在其出版的 1996 年百科全书（光盘版）里曾对黑客下了个定义：从 20 世纪 80 年代开始，黑客这个词作为对一些人的称谓出现在计算机软件和计算机技术里。“黑客”有轻蔑的含义，通常是指喜欢通过个人计算机和拨号上网秘密地侵入另外一些计算机或计算机网络，然后查看或破坏存储在其中的数据和程序的人。更确切地说，黑客就是指那些通过不合法的途径进入别人的网络寻找意外满足的人。因而在如今的公众眼中，黑客又更多地与电脑捣蛋分子联系在一起，更多的情况下，他们是专搞破坏的“骇客”。

要给“黑客”下一个准确的定义是非常困难的，因为在其发展的历史中，它自身一直在进行着微妙的演变。

一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。20 世纪 60 年代，“黑客”指独立思考、奉公守法的计算机迷。他们利用分时技术允许多个用户同时执行多道程序，扩大了计算机及网络的使用范围。20 世纪 70 年代，黑客倡导了一场个人计算机革命，他们发明并生产了个人计算机，打破了以往计算机技术只掌握在少数人手里的局面，并提出了计算机为人们所用的观点。这一代“黑客”是电脑史上的英雄。其领头人是苹果公司的创建人史蒂夫·乔布斯。在这一时期，黑客们也发明了一些侵入计算机系统的基本技巧，如破解口令（Password cracking）、开天窗（Trapdoor）等。20 世纪 80 年代，黑客的代表是软件设计师，包括比尔·盖茨在内的这一代黑客为个人电脑设计出了各种应用软件。与此同时，随着计算机重要性的提高，大型数据库越来越多，而信息又越来越集中在少数人手里。黑客开始为信息共享而奋斗，这时黑客开始频繁入侵各大计算机系统。如今的黑客队伍人员杂乱，既有善意的以发现计算机系统漏洞为乐趣的“电脑黑客”

（Hacker），又有玩世不恭好恶作剧的“电脑朋客”（Cyberbunk），还有纯粹以私利为目的、任意篡改数据、非法获取信息的“电脑攻击者”（Cracker）。如今的黑客队伍人员太多太杂，而且个个喜欢标新立异、与众不同。本书从公众理解黑客的视角出发，把黑客广义地理解为那些利用某种技术手段，善意或恶意地进入其权限以外的计算机网络空间的人。

黑客有其自身的文化，他们提倡解决问题，建设事物，信仰自由和双向的帮助，遵循着“人人为我，我为人人”的信条。要获得其他黑客的尊敬，他（她）可以做以下五种事情：

（1）写开放源码的软件；

（2）帮助测试并修改开放源码的软件；

（3）公布有用的信息；

（4）帮助维护基础设施的运转；

（5）为黑客文化本身服务。

黑客们虽然喜欢标新立异，与众不同，但是他们身上都有着下述一些共同的生活态度和行为特征。

崇尚自由：黑客文化首先给人的感觉就是体现出一种自由不羁的精神。黑客在电脑虚拟世界发挥着自己极致的自由，随意登录世界各地网站，完成着现实生活无法企及的冒险旅程，实现着个人生命的虚拟体验。

反叛精神：黑客骨子里对世界充满着反叛的倾向，渴望自由和平等。因特网的一个显著特点，是用户人人平等。但是，网络存在着许多禁区，有许多禁止人们随意访问的地方。黑客们认为这是有违网络特征的，他们希望建立一个没有权威、没有既定秩序的社会。所以黑客们一般都喜欢与传统、权威和集权做永不休止的斗争。

热衷挑战：黑客喜欢挑战自己的智力，编写高难度程序、破译电脑密码。而运用自己的智慧和电脑技术去突破某些著名的、防卫措施森严的站点更是一件富有刺激性、挑战性的冒险活动。这也往往是黑客价值实现的手段，“高级黑客”受人尊敬也往往是由于挑战获得成功的结果。

主张信息共享：黑客认为所有的信息都应当是免费的和公开的。黑客就是要突破对信息本身所加的限制，实现资源共享。他们认为计算机应是大众的工具，而不应是有钱人私有的。信息应该也是不受限制的，它属于每个人，拥有知识或信息是每个人的权利。

破坏心理：黑客的破坏心理源自其行为的前几个特征。黑客要在网络空间来去自由，蔑视权威，就必然要夹带着在计算机系统中的破坏举动。只有突破计算机领域防护才能随意登录各式站点；只有颠覆权威设置的程序才能反抗权威；只有摧毁网络秩序才能达到人人平等的信息共享目标。当然这和所谓的“骇客”是截然不同的，因为黑客们建设，而骇客们破坏。

1.1.2 黑客的基本技术

知己知彼，百战不殆。要想在防止黑客入侵、确保网络安全的没有硝烟的战场上处于不败之地，了解黑客攻击所必备的基本技术是必需的。

（1）具有一定的英文水平

现在大多数资料和教程都是英文版本的，而且有关黑客的新闻也是从国外过来的，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当我们看到中文介绍的时候，这个漏洞可能早已不存在了。因