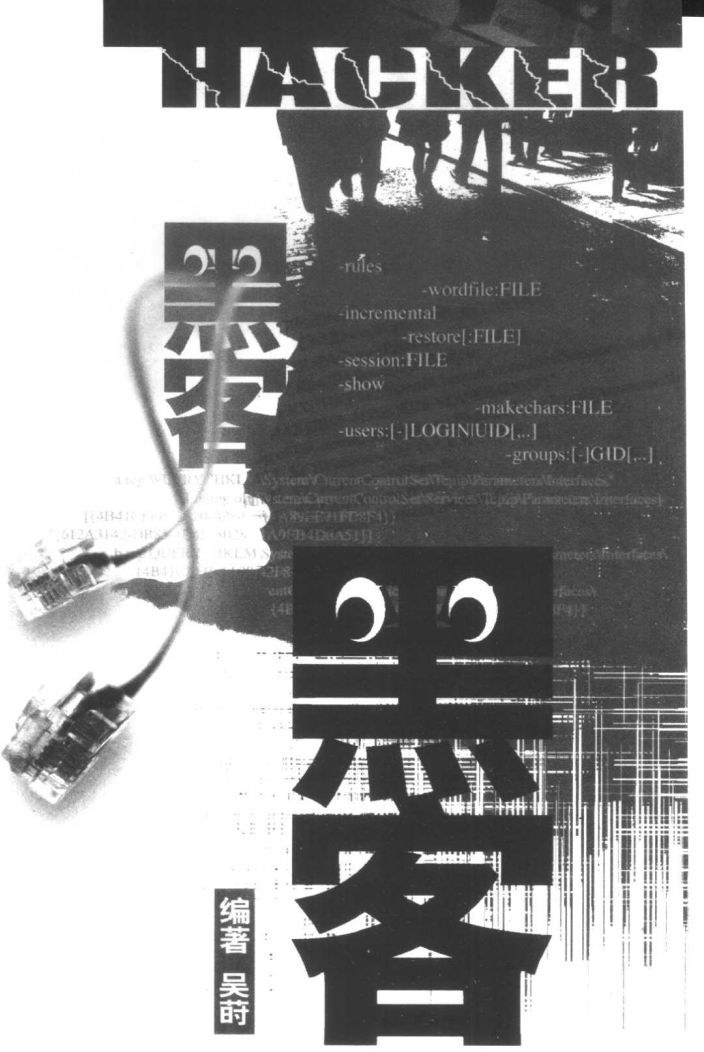
HACKER

# 黑客

崇尚自由、信息共享、热衷挑战、反叛破坏

编著 吴莳

中国经济出版社




# 黑客

编著 吴蔚

中国经济出版社

崇尚自由、信息共享、热衷挑战、反叛破坏

责任编辑:张新安(010-68354170)
封面设计:宋双成

**图书在版编目(CIP)数据**

黑客/吴蒔著.—北京:中国经济出版社,2002.1
ISBN 7-5017-5365-2
Ⅰ.黑… Ⅱ.吴… 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(2001)第 070241 号

# 黑　客

吴　蒔　编著

中国经济出版社
(北京市百万庄北街 3 号)
邮编:100037
三河市印务有限公司印刷　　新华书店经销
开本:850×1168 毫米　1/32　印张 11.875　字数 280 千字
2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
印数:　8000
ISBN 7-5017-5365-2/G·1079
定价:19.80 元

责任编辑：张新安　封面设计　宋双成

# 黑客

HACKER

"网络一家，四海一心"的信息时代，黑客亦正亦邪地充当着"网络英雄"或"网络杀手"的双重角色……他们维护网络财产安全，保卫网络国防是英雄，篡改信息，窃取账号及密码，威胁社会是杀手……

本书可以帮你了解黑客的文化、行为和对社会的危害性，去正视黑客现象做到"孰是孰非，仁者见仁，智者见智"。

定价：19.80元

# 目　录

# 第一章　雾里看花谈黑客

这是个黑客无孔不入的网络时代。当今任何一个软件问世后被黑客发现漏洞的周期越来越短，比如，IE5．0刚出世就被发现有破绽，长期“任劳任怨的HOT－MAIL也被黑客钻了空子；微软公司的操作系统更是被黑客搞得千疮百孔。黑客们作案手段之高，破坏力之大，让人防不胜防，他们斑斑的劣迹，累累的罪行，数不胜数。以至人们谈“黑”色变，对他们深怀敌视之意，忌惮之心。然而，黑客中既有干坏事的，也有很大一部分只是想搞搞恶作剧，开开玩笑，借此展现自己过人的才华。世界上著名的黑客分子大多是15岁到30岁之间的年轻人，他们的每一次恶作剧都让人忍俊不禁，窃窃发笑。而更让人刮目相看的是，在许多黑客的身上，体现着强烈的正义感，他们如骑士般地“路见不平，拔刀相助”，人们亲切地称这些黑客为“红客”，或“网络骑士”。

1991年海湾的战争爆发后，一批不满美国侵略行径的荷兰黑客对美军网络系统进行了无情的攻击，数以百计的美军机密文件被黑客们偷出来提供给伊拉克；1998年，印度不顾国际社会的反对进行核试验后，一群自称“千年虫”的青少年黑客宣布，为了抗议印度接连进行五次核试验，他们曾成攻地进入了印度国家安全要害部门——设在孟买的“巴巴原子研究中心”的电脑网络，盗走了高度敏感的核武器机密；1999年，北约在未经联合国安理会授权的情况下悍然对南联盟发动了军事空袭，来自全球范围内的计算机黑客对美国及其盟友的网站进行了一场无声的攻

击，“爸爸”、“梅利莎”；“疯牛”和“EMAIL”病毒使巴尔干战争中的北约通信陷入瘫痪；2000 年仅美国空军、陆军和海军的电脑网络就遭到了严重的攻击，至少有一百多个政府电脑系统曾被黑客们控制。2001 年初，梵蒂冈广播电台网站遭到了欧洲各国黑客们的攻击，原因就是教皇约翰·保罗发表了不公正的言论……

## 一、探源黑客

实际上，黑客也就是英文“hacker”的音译，“hacker”单词源于动词“hack”，这个词在英语中有“乱砍、劈、砍”之意，还有一个意思是指“受雇于从事艰苦乏味工作的文人”。“hack”的一个引伸意义是指“干了一件非常漂亮的事”。在 19 世纪 60 年代的时候，电脑系统是非常昂贵的，都只是存在于各大院校与科研机构的“玻璃房”中，技术人员使用一次电脑，需要很复杂的手续，而且电脑的效率也不是很高。为了绕过一些限制，最大限度地利用这些昂贵的电脑，最初的程序员们就写出了一些简洁高效的捷径程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为“hack”。在早期美国麻省理工学院中，“hacker”有“恶作剧”的意思，尤指那些手法巧妙、技术高明的恶作剧。可见，至少是在早期，“黑客”这个称谓并无贬意。

“破解，不是学习使用一个什么软件，不是按照说明书来操作，它是一种人和人智力的较量，是一种智慧的战争艺术，是一种知识与知识的较量。从本质上讲，学习‘破解’跟学习其他知识一样，都是要下苦功夫，要靠灵剧，要靠自己思考的。”这就是黑客们对自己行为的诠释。

### 1.“黑客”、“怪客”与“骇客”

骇客，怪客是“cracker”的音译，就是“破坏者”的意思。

这些人做的事更多的是破解商业软件、恶意入侵别人的网络并造成损失。

怪客具有与黑客同样的本领，只不过是在行事上有些差别而已，这也是我们常常很难分清黑客与怪客的原因之一。

其实，黑客也好，骇客、怪客也好，名称只是一种代号而已，应该说他们之间并无绝对的界限，我们也很难将他们区分得很清楚，他们都是非法入侵者。既是非法入侵，再区分什么善意入侵与恶意入侵也没有意义了，而且无论是哪一种入侵，无论是有意还是无意，都有可能造成被入侵者的损失。

## 2．黑客的前世今生

新时代的确立不仅是以文化和知识方式上的转型为其特征的，同时往往要造就一个或几个能够代表它自己的、独特的社会群体和阶层，而黑客显然就是信息时代最令人惊讶的产物之一。

从贝尔发明电话而将信息时代的巨幕逐渐拉开的时候算起，各色各样善于将个人的技术优势凌驾于社会规则之上的黑客组织和个人通过他们自己独特的方式已经将其封印深刻于时代的铭柱之上，他们像传说中的阿波罗一样，驾驭着技术的马车巡游在世界的每个角落。可以说，黑客早就完成了自我的涅槃，早以不是依靠盗打几个长途电话或是突破个把防火墙便能获得满足的快乐。实际上，大到国际政治、小到个人隐私，我们如今已经很难指出哪里还听不到黑客们的声音、哪里还见不到黑客的身影。

在下文中我们将一起回顾黑客逐渐成长的岁月，希望能够从中了解这些隐身在技术帷帐之后神秘难测的人。

1969 以前：萌芽期

早在 1878 年，贝尔电话公司成立的消息已经迅速引来一群爱戏弄人的少年，他们用自制的交换机中断电话或者胡乱接驳线路。诚然，这帮纯粹为捣蛋而捣蛋的小子称不上什么严格意义上

的黑客，但他们却实实在在的应当算作电脑黑客精神上的原型。

至19世纪60年代，黑客家谱中的第一代终于出现，他们对于新兴的电脑科技充满好奇。由于当时的电脑还是那些长达数英里、重达数百吨的大型主机，而技术人员需要劳师动众才能通过它们完成某项如今不值一提的工作，为了尽量发挥它们的潜质，最棒的电脑精英们便编写出了一些简洁高效的工作捷径程序。这些捷径往往较原有的程序系统更完善，而这种行为便被称为Hack。

不过，如果要评选早期最具有价值的黑客行为，相信应当是1969年由贝尔实验室两位职员丹尼斯·里奇及肯·汤普森制作的UNIX操作系统，即使两位创造者采用的全然是黑客手法，但实际上毫无“黑”味儿，不仅如此，在某种程度上讲还大大推动了软件科学的发展。

1970－1979：成长期

19世纪70年代可以说是黑客的少年时期，随着技艺的日渐成熟，他们心中那些迷蒙而散乱的思想也逐步成型，昔日凭借本能行事的第一代黑客们开始了由蛹化蝶的进程。大约在1971年，越战老兵约翰·德雷珀发明了利用汽笛吹入电话听筒而成功打免费电话的奇招。接着，反文化领袖阿比·霍夫曼更明目张胆地出版了一本专门探讨如何入侵电话系统打免费长途的刊物，他极力宣扬个人在大型机构面前应当保有尊严，并鼓吹如果尊严被剥夺人们应具有反击的权利，他的思想和言论所造就的影响力足足流传了20多年。

黑客队伍在这个时期日渐壮大，一些后来在IT技术史中占有重要地位的人物开始崭露头角，其中包括苹果机创始人之一的赫兹尼亚克。越来越多的黑客们在共享着技术所带来的喜悦的时候，发现惟一美中不足的是欠缺互相交流心得的地方。因此，在

1978年，来自芝加哥的兰迪·萦萨及活德·克里斯琴森便制作了第一个供黑客交流的网上公告版，此BBS至今仍在运行之中。

### 3．黑客必须具备的技能

hacker的精神态度是很重要的，但技术则更为重要。hacker的态度虽然是无可取代，但别的hacker开始也叫你hacker前，有些基本的工具和技能是必备的。

(1) 学习程序设计

当然，这是基础的hacking技能。在1997年，理所当然的，必须学会C语言。但是，如果你只是学一种语言，那么不能算是一位hacker，了不起只能算是一个programmer。除此，他们还必须学会以独立于任何程序语言之上的概括性观念来思考一件程序设计上的问题。要成为一位真正的hacker，必须要能在几天之内将manual内容和自己目前已经知道的技术关连起来学会一种新的语言。也就是说，必须学会多个不同的语言。除了C之外，至少还要会LISP或Perl，甚至Java等。除了几个重要的hacking常用语言之外，这些语言提供一些不同的程序设计途径，并且让自己在好的方法中学习。程序设计是一种复杂的技术，没办法展现他们完整的学习步骤，但是能告诉你一些在书本上和课堂上所没有的东西有很多，几乎全部最好的hacker们都是自学得来的。

成为黑客最简单的程序技术为：

①读别人的程序码

②写程序

这两项是不错的方法。学习写程序就像在学习写一种良好的自然语言，最好的方法是去看一些专家们所写的东西，然后写一些自己的东西，然后读更多，再写更多……然后一直持续，一直到发展出一种属于自己的风格和特色。要找到好的程序码来看是很一件很困难的事，因为，对菜鸟hacker们而言，适于供他们阅

读和努力的大型程序的 source 数量很少。但这事已有了戏剧性的变化了；现在免费的供应软件、程序设计工具和操作系统大都公开提供 source，而且全都是由 hacker 们写成的到处可看。

(2) 取得一个免费的 UNIX，并学习使用和维护

拥有一部个人电脑或者是可以使用认何一部电脑是成为黑客的前提条件，取得 hacker 技能的第一个步骤是取得一份 Linux 或者一份免费的 BSD - Unix，并将他安装在自己的机器上，并使之顺利的运作。没错，在这个世界上除了 Unix 之外，还有其他的操作系统。但是他们只提供 bianry，不能看到他们的程序码，也不能修改他们。想要在 DOS 或 Windows 或 MacOS 开始 hacking，无疑就是绑着枷锁跳舞。除此之外，Unix 是 Internet 上的操作系统。在不懂 Unix 的情况下学习使用 Internet 时，就没办法在不懂 Unix 的情况下成为 Internet 的 hacker。因为这个原故，现在的 hacker 文化还是很牢固的以 Unix 为中心绕着。这并不完全是正确的，而且有些活在旧时代的 hacker 甚至也不喜欢这种情形，但是 Unix 和 Internet 之间的共生共成已经到了牢不可破的地步，即使是 Microsoft 的大块肌肉也没能在上面留下明显的伤痕。因此，把 Unix 装起来吧！用他向整个 Internet 喊话、看程序码、改程序，这使得 hacker 得到了比 Microsoft 操作系统所能提供的还要好的程序设计工具（包括 C，Lisp 和 perl)。而且得到快乐，并学到比你想像中的还要多的知识。

(他们常光顾的 Unix 的好地方 - http: //www. ccilorg/esr/faqs/loginataka。html - )

(3) 学习使用 World Wide Web 并学会写 HTML

在 hacker 文化创造出来的东西，大多在他们的活动范围外被使用着，如，在工厂的办公室或大学里被漠漠的使用着。但 web 是一个很大的例外，这个 hacker 眼中的大玩具甚至还被政客们接