中国大陆第一部全面叙述中国黑客成长历史的文本

中国黑客

古风 编著

学林出版社

中国黑客

古风 编著

学林出版社

图书在版编目(CIP)数据

中国黑客／古风编著．—上海：学林出版社，
2004.7
ISBN 7-80668-795-5

Ⅰ．中… Ⅱ．古… Ⅲ．因特网—发展史—中国
Ⅳ．TP393.4-092

中国版本图书馆 CIP 数据核字(2004)第 071484 号

中国黑客

编　　著／古　风
策　　划／上海大用今世文化传播有限公司
责任编辑／吴伦仲
责任监制／应黎声
封面设计／钦州锋
版面设计／灵岩剑客
出　　版／上海世纪出版集团
学林出版社（钦州南路 81 号 3 楼）
电话：64515005　传真：64515005
发　　行／新华书店 上海发行所
学林图书发行部（钦州南路 81 号 1 楼）
电话：64515012　传真：64844088
印　　刷／上海交大印务有限公司
开　　本／890 × 1240　1/32
印　　张／8.25
字　　数／17 万
版　　次／2004 年 7 月第 1 版
2004 年 7 月第 1 次印刷
印　　数／8000 册
书　　号／ISBN 7-80668-795-5/G · 281
定　　价／18.00 元

引 言

当我在键盘上打下这个题目，并开始把这部被我趣之为《中国黑客》的书付诸实施的时候，我此时竟然有点自嘲自己的这个举动，作为一个计算机的白痴，2001年8月间由激情MM引荐到鹰派，屈指算算居然也有两年的时间，在这两年的时间里，我由鹰派的一个普通会员到鹰派论坛的管理员以至联盟的顾问，期间经历的许多故事犹在眼前。在这里认识了许多的朋友，也亲眼看到许多朋友因为种种原因就这样悄然离去，也可以说，我今天有心想把那些网上让我们崇拜“大侠”的故事呈现给各位的时候，与来自心底的那份难以割舍的感情有很密切的关系。说句真心话，我怀念那些鹰派曾经的老朋友，我更希望有一天能够再在这里见到他们……

“巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰。”

——凯文·米特尼克

上世纪60年代加拿大传播理论家马歇尔·麦克卢汉曾经预言，电子媒介可以把地球变成一个村落，他不无乐观地指出：“住处的即索即得能创造出更深层次的民主，未来的全球村舒适而开放。”然而，这个村落既没有“乡规民俗”，更缺少道德法律。而那些电脑领域的天才型人物也就堂是地高挂“黑客”招牌，在比特世界神出鬼没为所欲为。在因特网上，他们有点像古龙笔下的陆小凤游戏江湖、也有点像金庸笔下的“老顽童”，风流倜傥爱搞点恶作剧逗你玩；没钱的时候，也会学着孔乙己一样，盗点住处换酒喝，并嚷着“读书人窃不算分”；有时也会扮演一个玩世不恭、英雄救美人的罗宾汉，制造一点点神幻的浪温。

黑客有白帽子、黑帽子和灰帽子之分。研究漏洞、发明追求最先进技术并让大家共享的黑客，被称之为“白帽子”；以破坏入侵为目的的黑客，被冠以“黑帽子”，介于以上两者之间的，叫做“灰帽子”，这是一个追求网上信息公开的群体，他们不破坏，但要进入别人的网站去拿信息。

中国鹰派联盟的负责人chinaeagle一直是我本人欣赏的一位江湖侠上，他早年毕业于中国北方交通大学，大学时代，他编制的测试病毒曾成功地绕进了号称能侦测未知病毒的某著名病毒卡，中国老牌黑客组织“绿色兵团”的早期成员，2001年中美黑客

大战的领军人物，现在是某IT公司的CE.从一个知名的网上黑客到现在的网络安全专家，他见证了中国黑客团体成长：

> 信息时代需要安全保障，建立在国外技术之上的中国民族信息产业还格外脆弱，更是需要大量的优秀的安全人才加盟。
>
> 先天不足和相对滞后是我们必须面对的现实，但如果最终的结果也是另外一种形式的头脑简单四肢发达，则将是中国网络安全爱好者的悲哀！
>
> 为了让大家能够理解鹰派存在的理由以及发展的动力之一，为了让大家学武不忘武德。联盟特别开设此频道，为了我们长远的未来。
>
> 在此，我们要向我们所有的前辈致敬！
>
> 无论其的国籍如何……。
>
> 在此，让我们缅怀先辈的宣言：
>
> 通往电脑的路不止一条
>
> 所有的信息者应当是免费的
>
> 打破电脑特权
>
> 在电脑上创造艺术和美
>
> 计算机将使生活更美好

老鹰的这段话预示着中国黑客的成熟，现在的中国黑客绝不是偷人家QQ、邮箱，黑别人计算机的下三滥，中国的黑客正在赢得世界其他国家黑客们的尊重。

目 录

论 剑

为黑客“正名”

提起黑客，总是令人感到神秘莫测。在人们眼中，黑客似乎是一群聪明绝顶、精力旺盛的年轻人，一门心思地破译各种密码，以便偷偷地、未经允许地打入他人的计算机系统，窥视其隐私。那么，究竟什么是黑客呢？

黑客（*Hacker*），源于英语动词Hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期美国麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤其是指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”由这些定义中，我们还看不出过于贬义的意味。他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统。“黑客”能使

更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。

另一种入侵者是那些利用网络漏洞破坏网络的人。他们往往做一些重复的工作(如采用暴力法破解口令)，他们也具备广泛的电脑知识，但与黑客不同的是他们以破坏为目的。这些群体被称为“骇客”。当然也有一种人介于黑客与“骇客”之间。

一般认为，黑客起源于20世纪50年代美国麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。60、70年代，“黑客”一词极富褒义，用于指代那些独立思考、奉公守法的计算机迷，他们智力超群，对电脑全身心投入，对电脑的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大贡献。正是这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构，打破了以往计算机技术只掌握在少数人手里的局面，开了个人计算机的先河，提出了“计算机为人民所用”的观点，他们是电脑发展史上的英雄。现在黑客使用的侵入计算机系统的基本技巧，例如破解口令(Password Cracking)、开天窗(Trapdoor)、走后门(Backdoor)、安放特洛伊木马(Trojan Horse)等，都是在这一时期发明的。从事黑客活动的经历，成为后来许多计算机业巨子简历上不可或缺的一部分。苹果公司创始人之一乔布斯就是一个典型的例子。

在60年代，计算机的使用还远未普及，并没有多少存储重要信息的数据库，也谈不上黑客对数据的非法拷贝等问题。到了80、90年代，计算机越来越重要，大型数据库也越来越多，同时，信息越来越集中在少数人的手里。这样一场新时期的“圈地运动”引起了黑客们的极大反感。黑客认为，信息应共享而不应被少

数人所垄断，于是将注意力转移到涉及各种机密的信息数据库上；而这时，电脑化空间已私有化，成为个人拥有的财产，社会不能再对黑客行为放任不管，必须采取行动，利用法律等手段来进行控制。黑客活动受到了空前的打击。

但是，政府和公司的管理者现在越来越多地要求黑客传授给他们有关电脑安全的知识。许多公司和政府机构已经邀请黑客为他们检验系统的安全性，甚至还请他们设计新的保安规程。例如，在两名黑客连续发现网景公司设计的信用卡购物程序的缺陷并向商界发出公告之后，网景修正了缺陷并宣布举办名为"网景缺陷大奖赛"的竞赛，那些发现和找到该公司产品中安全漏洞的黑客可获1000美元奖金。无疑，黑客正在对电脑防护技术的发展做出贡献。

黑客攻击术

一些黑客往往会采取几种攻击方法，但是我很想说的是，一个优秀的黑客绝不会随便攻击别人的。

1、一般黑客攻击术

攻击术之一：获取口令

这又有三种方法：一是通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户账号和口

令，对局域网安全威胁巨大；二是在知道用户的账号后（如电子邮件@前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间；三是在获得一个服务器上的用户口令文件（此文件成为Shadow文件）后，用暴力破解程序破解用户口令，该方法的使用前提是黑客获得口令的Shadow文件。此方法在所有方法中危害最大，因为它不需要像第二种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与Shadow文件中的口令相比较就能非常容易地破获用户密码，尤其对那些弱智用户（指口令安全系数极低的用户，如某用户账号为zys，其口令就是zys666、666666、或干脆就是zys等），更是在短短的一两分钟内，甚至几十秒内就可以将其干掉。

攻击术之二：放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在windows启动时悄悄执行的程序。当您连接到因特网上时，这个程序就会通知黑客，来报告您的IP地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改您的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

攻击术之三：WEB的欺骗技术

在网上用户可以利用IE等浏览器进行各种各样的WEB站点的访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等；然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

攻击术之四：电子邮件攻击

电子邮件攻击主要表现为两种方式：一是电子邮件轰炸和电子邮件"滚雪球"，也就是通常所说的邮件炸弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被"炸"，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串），或在貌似正常的附件中加载病毒或其他木马程序（据笔者所知，某些单位的网络管理员有定期给用户免费发送防火墙升级程序的义务，这为黑客成功地利用该方法提供了可乘之机）。这类欺骗只要用户提高警惕，一般危害性不是太大。

攻击术之五：通过一个节点来攻击其他节点

黑客在突破一台主机后，往往以此主机作为根据

地，攻击其他主机(以隐蔽其入侵路径，避免留下蛛丝马迹)。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过IP欺骗和主机信任关系，攻击其他主机。这类攻击很狡猾，但由于某些技术很难掌握，如IP欺骗，因此较少被黑客使用。

攻击术之六：网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接受到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接受方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，例如NetXray for windows 95/98/nt，sniffit for Linux、solaries等就可以轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

攻击术之七：寻找系统漏洞

许多系统都有这样那样的安全漏洞(Bugs)，其中某些是操作系统或应用软件本身具有的，如Sendmail漏洞、win98中的共享目录密码验证漏洞和IE5漏洞等，这些漏洞在补丁未被开发出来之时一般很难防御黑客的破坏，除非你将网线拔掉；还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出，将未加Shadow的用户密码文件以明码方式存放在某一目录下，这都会给黑客带来可乘之机，应及时加以修正。

攻击术之八：利用账号进行攻击

有的黑客会利用操作系统提供的缺省账户和密码进行攻击，例如许多UNIX主机都有FTP和Guest等缺省账户（其密码和账户名同名），有的甚至没有口令。黑客用Unix操作系统提供的命令如Finger和Ruser等收集信息，不断提高自己的攻击能力。这类攻击只要系统管理员提高警惕，将系统提供的缺省账户关掉或提醒无口令用户增加口令，一般都能克服。

攻击术之九：偷取特权

利用各种特洛伊木马程序、后门程序和黑客自己编写的导致缓冲区溢出的程序进行攻击，前者可使黑客非法获得对用户机器的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段一旦奏效，危害性极大。

2、过去五种影响最大的攻击

红色代码：

2001年7月的某天，全球的IDS几乎同时报告遭到不明蠕虫攻击。信息安全组织和专业人士纷纷迅速行动起来，使用蜜罐(Honeypots)技术从因特网上捕获数据包进行分析，最终发现这是一利用微软IIS缓冲溢出漏洞进行感染的变种蠕虫。其实这一安全漏洞早在一个月以前就已经被eEye Digital Security发现，微软也发布了相应的补丁程序，但是却很少有组织和企业的网络对其引起足够的重视，下载并安装了该补丁。在红色代码首次爆发的短短9个小时内，这一小小