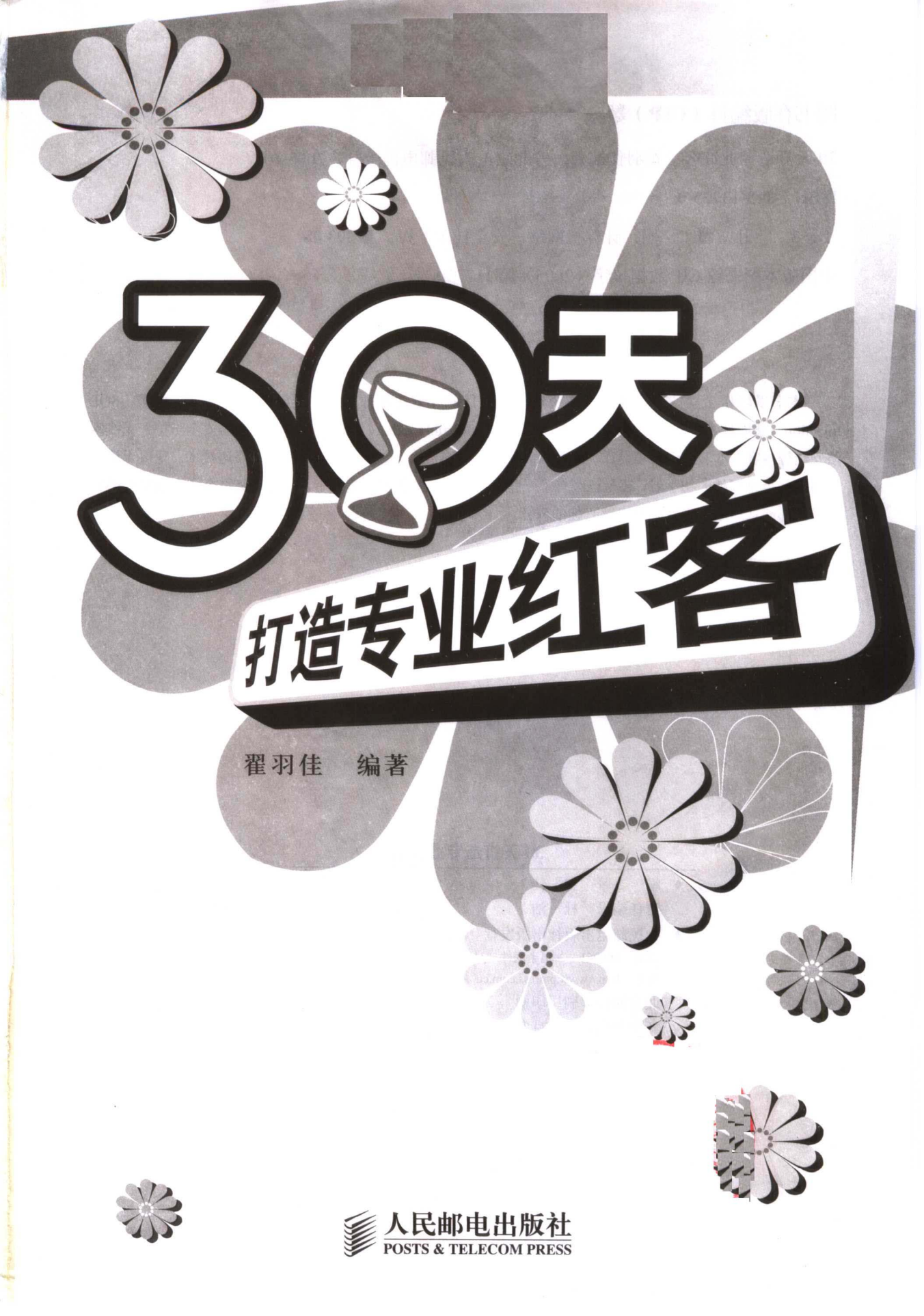
30天打造专业红客

翟羽佳　编著

- 扫描技术原理与应用技巧
- 常见端口渗透思路和权限提升方法
- SQL Injection深入研究及难点总结
- 暴库原理浅释和预防暴库的基本招数
- 跨站Script攻击方式与旁注攻击
- 分布式拒绝服务攻击（DDoS）
- 全面了解80端口攻击
- Google Hacking零接触
- 黑客编程之四书五经
- 服务器安全强化和安全管理
- 基于无线网络协议标准的安全分析
- 45个最佳安全工具完全推荐

人民邮电出版社
POSTS & TELECOM PRESS



翟羽佳　编著

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目（CIP）数据

30 天打造专业红客 / 翟羽佳编著. —北京：人民邮电出版社，2005.10

ISBN 7-115-13725-0

Ⅰ. 3… Ⅱ. 翟… 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 117730 号

内 容 提 要

本书以轻松生动的日记风格，系统地介绍了目前常见的各种网络安全问题，包括网络嗅探、SQL Injection、暴库技术、溢出攻击、跨站 Script 攻击、GoogleHacking、DDoS 攻击、服务器安全防护、无线网络安全等内容。本书结构精心设计，从对端口扫描的讨论开始，由浅入深地讲解网络渗透技术。使得无论是对网络安全感兴趣的初学者，还是已经有了一些网络渗透经验的安全爱好者，或者是负责企业网络安全的管理员，都能从这本书中找到自己感兴趣的部分。

30 天打造专业红客

◆ 编　　著　翟羽佳

责任编辑　杜　洁

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号

邮编　100061　　电子函件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京鸿佳印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：787×1092　1/16

印张：19.25

字数：466 千字　　2005 年 10 月第 1 版

印数：1－6 000 册　　2005 年 10 月北京第 1 次印刷

ISBN 7-115-13725-0/TP・4845

定价：28.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前　言

关于本书

2004年发生了很多惊人的安全事件，从腾讯公司被传遭到攻击勒索到江民网站首页多次被人涂改，网络安全越发地引起公众的注意。许多人希望能进入这个充满神奇色彩的红客世界。但是由于VIP站点的不断增加，使得能从网络上获得的知识变得越来越少，资源共享也开始讲条件了，但是人们对于这方面知识的渴望却越来越强烈。

本书的最初版本是去年3月我在基尔网（http://www.91one.net）上以日记形式发布的，之后迅速被全国各大安全站点转载，包括黑客基地、天天安全网、ChinaUnix、硅谷动力、中国网络安全联盟、动网先锋论坛等。我的信箱曾在一天内收到过来自网友的100多封电子邮件，除了对我表示鼓励和向我寻求疑难问题的解决办法外，更多的朋友还是希望我能够再接再厉把教程写完。当时由于时间的问题，我一直没有写完教程。经过了近一年的不断整理和修改，我终于在今年7月完成了这项工作，修改后的版本除了保留原来的日记形式和轻松讲解的风格外，还对内容做了大量的更新和补充。本书的内容不敢妄称原创，更多的是在前人研究的基础上进一步深入发掘与整理，但是书中的每一个演示实例都经过我的深思熟虑与实际调试，凝聚了我多年积累的经验。

本书面向应用，结合广大读者的实际需求，不但提供了解决实际问题的方法、步骤、代码，还推荐一系列常用工具（提供下载连接），具有很强的可操作性和实用性。本书从任何服务器和终端都常见的一般安全问题开始，以围绕特定配置、操作系统以及相关技术的安全问题结束，深入浅出地讲述了各种关键技术，希望能对各位正在黑客技术道路中前行的朋友们有所帮助。

本书结构

本书分为3个部分，包括30天的内容，具体结构划分如下。

第一部分：初窥门径，包括第1～4天。这部分内容对网络安全的基础知识做了精炼的介绍。对系统与网络安全有一定基础的读者可以跳过这一部分内容。

第二部分：学以致用，包括第5～25天。这部分内容在对常规渗透技术讲解的基础上，还特别针对网络嗅探、SQL Injection、暴库技术、溢出原理、跨站Script攻击、Google Hacking、DDOS等攻击方式做了更深层次的讨论。

第三部分：抛砖引玉，包括第26～30天。这部分内容是前面内容的晋升，对网络编程、黑客软件的二次工程、服务器安全强化、无线网络安全等问题做了深入的探讨。

本书的读者对象

本书适用于对网络安全感兴趣的学习爱好者，负责安全保障工作的网络管理员和系统管理员，也可以作为相关培训机构的培训教材。

阅读本书的基础

书到用时方恨少。虽然本书是从基础讲起，但仍然需要初级的计算机应用能力。如果你有一定的网络安全知识和C语言编程基础，在阅读本书的时候会更加如鱼得水。

本书约定

1．为了给读者提供更多的学习资源，同时弥补本书篇幅有限的遗憾，本书提供了大量的参考链接，许多本书中无法详细介绍的问题都可以通过这些链接找到答案。本书采取了很多措施来确保这些链接在出版时仍然有效，但这并不意味所有的链接都有效。因为这些链接地址会因时间而有所变动或调整，所以在此说明，这些链接信息仅供参考，本书无法保证所有的这些信息是长期有效的。

2．本书中出现的软件、工具和源代码均可以在基尔网论坛（http://bbs.91one.net）的“30天打造专业红客”板块中找到。

3．本书中使用的网络环境和IP地址均没有任何的实际应用价值，但是书中的每一个演示实例都在一个实际的网络上运行过且测试成功。

4．本书所列出的插图、运行结果可能会与读者实际环境中的操作界面有所差别，这可能是由于操作系统平台、使用工具版本的不同而引起的，在此特别说明，一切以实际情况为准。

5．读者在阅读本书时有任何问题或看法，欢迎到基尔网论坛（http://bbs.91one.net）的“30天打造专业红客”板块进行交流和探讨；也可以通过电子邮件联络本书的责任编辑（dujie@ptpress.com.cn）。

致　谢

要感谢丁睿花费了3个月的时间帮助我对书中的内容进行修改、纠正错误，此书汇聚了他的才华与努力。感谢我的父母，他们一直竭尽所能地养育着我。还要感谢阮晶晶、李志昕、邹大立、王艳、刘倩、曹小洁、金明、李红秀、何玉洁、伍友珊等人对我长久以来的支持和帮助，没有他们，本书不可能完成。

翟羽佳

2005年10月

目　录

第一篇

初窥门径

第 1 天

什么是红客

20 世纪 60～70 年代，一群大学计算机系的知识分子利用“分时系统”技术把计算机主机变成了事实上的个人计算机，从而使更多的人有机会接触计算机。那时有一个由程序员所组成的、具有共享特点的文化社群，这个群体中的成员创造了“Hacker”（黑客）这个词。黑客们参与开发最早的 UNIX 操作系统，黑客们使 Usenet 和 BBS 运作起来，他们是 Internet 上最早的拓荒人，并始终走在 Internet 发展的最前列。

1.1 黑客的最初定义

提起黑客，总是和“神秘莫测”联系在一起。在很多人眼中，黑客是一群聪明绝顶、精力旺盛的年轻人，他们一门心思地破译各种密码，以便偷偷地、未经允许地打入政府、企业或者个人的计算机系统，去做一些他们想做的事情。然而一个真正的黑客（True Hacker）到底是怎么样的呢？

黑客（Hacker）一词来源于英语动词“hack”，原意为“劈、砍”，也就意味着“辟出、开辟”，引申为“干了一件非常漂亮的工作”。关于“Hack”和“Hacker”的含义，日本 1998 年出版的《新黑客网上字典》里列举了 9 种不同的解释，但该字典也收录了一篇由一位叫菲尔的麻省理工学院（MIT）早期黑客所写的文章。菲尔告诉我们：“不要被这些看似很有弹性的解释给蒙了，‘Hack’其实只有一个意思，就是用精细高明的手段去挑战传统思想”。

事实确实如此。早期的黑客特别是第一代黑客——麻省理工学院的“原型火车俱乐部”（Model Railroad Club）的成员，他们当时秘密穿梭于笨拙的穿孔大型机，并从 Xerox PARC（Xerox Palo Alto Research Center）偷取了大量技术，开启了计算机革命的历程，促成了 PC 的诞生，使计算机真正走向大众。他们自由不羁，反抗陈旧规矩，却严格遵循黑客道德准则：自由使用，信息免费，打破权威，推动分权。1990 年，MIT 博物馆发行的刊物中指出：20 世纪 50 年代 MIT 学生所说的“Hack”就是指非恶意并且又有创意的行为；50 年代之后，“Hack”这个字有了更尖锐、更叛逆的含义。

20 世纪 60 年代，MIT 校园里第一个自称计算机黑客的人就是 50 年代末期“原型火车俱乐部”的学生，他属于俱乐部里一个严谨的派系——信号动力（Signal&Power，S&P）。他们支持铁道社的电路设计与组件系统，这个系统复杂程度不下于校园的电话系统。对他们而言，少用一个继电器来操作这条铁轨，就意味着多了一个继电器可以用在别的地方。很快地，他们骄傲地宣称，改善了铁轨的重点设计和组件，做这件事的人就是“黑客”（Hacker）。20 世

纪50年代末期，S&P的成员就将玩赏创新的重心转移到TX-0计算机的控制室里，而且重点从硬件转向软件，从硬件的组合加工，转变为编程和软件的修改，并且逐渐强调集体创新的精神和共享的软件权利，形成了现代意义的黑客概念。

1969年，因特网（Internet）的前身ARPANET出现。以ARPANET为网络，以DEC-PDP系列小型机分时系统为硬件基础，并以UNIX为软件基础，整个黑客文化开始迅速繁荣。形成了以MIT的人工智能实验室为中心，蔓延到斯坦福大学人工智能实验室（SAIL）和稍后出现的卡内基梅隆大学（CMU）。这三个都是大型的计算机研究中心及人工智能的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对黑客文化的发展都有极高的贡献。

20年代70年代后期，第二代黑客领头人物是大名鼎鼎的史蒂夫、乔布斯、伍兹尼亚克和费尔森斯坦。他们都是非学术界的，都具有反文化的特点。他们也是黑客中大发其财的人物。

20年代80年代初出现的第三代黑客，为个人计算机设计了各种教育和娱乐程序，特别是米彻·凯普开发的LOTUS1 1-2-3电子报表程序促成了IBM PC的成功。第四代黑客的出现在80年代中期，他们开发了包罗万象的电子公告牌（BBS）和自由平等的以非层级方式连接的Usenet，并且将美国国防部的ARPANET改造成了今天的因特网。

接着，计算机革命的浪潮开始了，商人来了，政客来了，罪犯也来了，更多的普通人来了。计算机产业不断地发生彻底的改变，黑客群体也开始发生了巨大的变化。越来越多的人开始讨论一个在这个群体产生时最引以自豪的主题——黑客的道德准则。

1.2 黑客的道德准则

因特网现在有数亿用户，他们的平均年龄是30岁。很多人深信，就像个人计算机改变了20世纪的80年代一样，因特网将改变90年代和以后的岁月。“想真正成为黑客，你必须真枪实弹去做黑客应该做的事情。”这是我们听到的黑客宣言，并且被广告天下。这些黑客声称：“不要将你已破解的任何信息与人分享，除非此人绝对可以信赖；不在家庭电话中谈论你Hack的任何事情；当你发送相关信息到BBS的时候，对你当前所做的事尽可能说得含糊一些，以避免BBS受到警告；将你的黑客资料放在安全的地方；在BBS上POST文章的时候不要使用真名和真实的电话号码；如果你黑了某个系统，绝对不要留下任何蛛丝马迹……”。这是我们国内一位最早的黑客提出来的。如果拿它和现在国内一些“黑客”（我更愿意称他们为“骇客”）们的道德标准相比，它确实是一个非常“高”的标准了。但是，很显然，这些所谓的道德准则都是需要打上一个引号的。

自由、平等、共享、互助，这应该是所有黑客都要遵守的道德标准。黑客最重要的信条是不相信权威，提倡依靠自己。有人把美国已故前任总统肯尼迪的话“不要问你的国家能为你做些什么，要问你能为国家做些什么”改成了“不要问你的国家能为你做些什么，你自己做”。因此，我们看到很多黑客一改过去学术界蔑视商界的传统，半途辍学创办起自己的公司，这些人认为信息应该是免费的信息，他们创造了“免费软件”和“共享软件”的概念，使得每个需要这些软件的人都可以免费得到它们，当然在中国更多的人做的是破解软件的事情。在现在这样一个全球化的时代，资讯很可能被极少部分人所掌控，黑客们提出免费的信息就显得更加重要了。

美国的《PHRACK》杂志已被公认为是黑客的“官方”新闻资讯，它把黑客的思想扩展成一些基本原则，其核心思想是“因为设备的高代价超出了大多数黑客的财力，它在感觉上造成的结果是：Hack 是把计算机知识传播给大众的惟一办法”。黑客们反对“权利”只属于那些有权进入和使用现代技术的群体。

1984 年，《新闻周刊》首席科技作家列维出版了《黑客：计算机革命的英雄》。他在书中提出：黑客本来就是计算机革命的主角和英雄。的确，黑客曾是一种荣耀，一种美好的传统。它代表着 20 世纪 60～70 年代反权威却奉公守法的计算机英雄。这群电气工程师和计算机革新者才华横溢但行为孤僻。他们沉迷于技术，视工作为一种艺术。他们不仅仅是计算机革命的重要参与者，而且根本就是计算机革命的主角和英雄。

黑客本身应该是一个值得骄傲和尊敬的称呼，就好比是一个做天体物理研究的科学家。研究计算机和研究反物质是没有本质区别的。但可惜的是，大众化的趋势和媒体的错误报道，再加上本身价值与现实的巨大差异，使得黑客这个曾经多么荣耀的名字，如今已经开始变得五颜六色了。“理想与现实之间还有一个温饱的问题，它使得问题开始变得非常复杂”，这是我的黑客启蒙老师——澳大利亚一个普通的高中历史教师告诉我的。他曾经参加 386BSD 计划（一个编写 UNIX 操作系统——FreeBSD 的计划）。我一直觉得他是一名真正的黑客。在理想和现实之间他选择了理想，当然是解决了基本的温饱问题。他是一个优秀的程序员、一个优秀的历史老师、一个优秀的父亲同时又是一名出色的黑客。

1.3 红客——中国的代表

相对于全球的黑客群体来说，中国黑客的出现就有点晚了。中国的黑客是伴随着互联网的出现而发展起来的。1994 年这一年，中国互联网的大门终于向公众开放了。当时计算机还是个很稀少的东西，“网络”这个词或许只有在搞传销的人群中才能被经常听到。当然在专业性极强的书刊中，还是能够找到与网络相关的名词，而那时候能上网的群体也多数为科研人员和有钱有知识的人（那个时候似乎也没有小资之类的词）。各地电脑发烧友最大的乐趣就是 COPY 一些小游戏和 DOS 等软件类产品，对于广大计算机用户来说，盗版还是一个陌生的名词。

1995 年，那个中国网络最为朦胧的岁月里，大多数玩家用着小“猫”（比现在的拨号要慢得多）在网络上奔驰。那不是我们现在传统意义上的 Internet，而是最为初级的 BBS 站——一种依靠拨电话号码直接连接到 BBS 服务器上的方式。加密解密仍然是当时最热门的东西，当时也确实涌现了很多加密解密方面的高手，只是后来因为法律的进一步完善和网络的迅速发展，大都转行去做网络编程了。

到了 1997 年，中国的第一代黑客终于出现了。不过他们当时所掌握的最高技术也仅仅是使用邮箱炸弹，并且多数是国外的工具，完全没有自己的工具。1998 年，国内第一款特洛伊木马诞生了，这就是网络间谍 NetSpy。在随后的日子里，以谢朝霞、PP（彭泉）、天行（陈伟山）等为代表的程序员开始显露头角，少量的国产工具开始小范围地流行于中国黑客之间。

接下来发生了震惊世界的印尼排华事件，这时候出现了第一次中国黑客的反击，许多人聚集在 IRC 聊天室中以 6～8 人为单位，对印尼的政府站点进行攻击，同时也造就了当时著名的黑客组织——绿色兵团。轰轰烈烈的印尼排华事件过后，中国的黑客终于走上了正轨——对技

术的追求。新的黑客高手也再次涌现，这一时期最具代表性的黑客当属流光、溯雪、乱刀、小榕等。之后又发生了我国驻南大使馆被炸的事件，中国黑客们再次联合起来，并由 Badboy、孤独剑客等人首次提出红客的概念。在极短时间内，建立了一个站点，该站点初步定名为“中国红客之祖国团结阵线”（同年 7 月改名为“中国红客之祖国统一战线”）。在短短的数天内，网站访问量已达 50 多万，并出现在新浪网的新闻链接中，中国红客成为了世界黑客群体中一个特殊的群体，爱国与团结是中国红客永恒的精神理念。

到了 2000 年，全国各地出现了大批的网吧，网络开始进入了千家万户。我也是在 1999 年才第一次接触网络的，记得当时还申请到了一个 5 位 QQ 号。值得骄傲的是，2000 年微软全球公布的 100 多个安全漏洞里，其中有 6 个是袁哥（袁仁广）发现的。

这里我不得不提一下中国红客联盟。中国红客联盟简称 H.U.C，站长是 Lion，2000 年 12 月建站。H.U.C 在中美黑客大战中的鼎盛时期会员超过 8 万人，号称中国最大、世界第五的黑客组织。遗憾的是，2004 年因为种种原因 H.U.C 解散了。无论如何，它曾经带给我们这一代人刻骨铭心的记忆。

中国网络和中国的红客群体中有太多的无奈和悲哀，但我们依然不必要失望或者沉沦，因为 Hack 的精神只是“用精细高明的手段去挑战传统想法”，而并不是普及教育。我想把我所了解的中国杰出红客的名字都罗列出来：Rocky、Dspman、Frankie、袁哥、Adam、PP（彭泉）、小榕、天行、BadBoy、黄鑫、孤独剑客（王献冰）、san、flashsky、chinaeagle（万涛），这是中国红客的过去和荣耀，而新的希望就是你。

1.4 我的一些建议

从我第一次接触计算机开始，至今已有 9 个年头了。我并不认为自己是一个真正的黑客，应该算一个计算机安全爱好者吧。但经常有朋友问我一个问题：“我怎么成为一个黑客或者是红客呢？”我曾经写过一篇文章“我的 20 年之三年网络安全之路”。它主要是推荐一些书籍给新接触“安全”的朋友看。如果可能，我建议你去看一看。至于怎么找到它，我的建议是你必须学会使用搜索，比如 Google、Baidu 等。当然在我的站点——基尔网（http://www.91one.net）上你也可以找到。不过还有一些重要的问题我觉得必须要说。作为一个黑客，首先需要做到的就是严格遵守黑客的道德准则——自由、平等、共享、互助。并且要区别黑客和骇客：黑客创造新事物，骇客破坏事物。

态度决定一切。同所有创造性的艺术一样，成为大师的最有效方法就是模仿大师的精神。不仅从智力上，也要从感情上进行模仿。或许，下面这首现代诗能充分地说明这个意思。

To follow the path:（沿着这样一条道路：）
look to the master,（寻找大师，）
follow the master,（跟随大师，）
walk with the master,（与大师通行，）
see through the master,（洞察大师，）
become the master.（成为大师。）

这是 Eric S.Raymond 在他的“如何成为一名黑客”一文的 FAQ 中引用的，我在这里套用一下。一个健康积极的态度是非常重要的，但我们需要了解态度并不能取代能力或是技术。