北京科海培训中心

黑客

就这么几招

阎雪 编著

万方数据电子出版社

黑客就这么几招

内 容 提 要

由于因特网本身的设计缺陷及其开放性，它极易受到黑客的攻击。为了帮助广大网民“认识黑客、了解黑客、防御黑客”，本书全面、详尽地介绍了黑客的种种攻击技术，并附有大量的攻击实例，其中大部分攻击实例是从未公开过的；并且在介绍每种攻击方法的同时，都给出了相应的用户对策，使广大网民和网络管理员可以保障自己系统与信息的安全，完善自己的网络环境。

本书共分 4 个部分。第 1 部分主要介绍黑客的历史、行为准则以及相关的基础知识；第 2 部分主要介绍黑客对普通用户的攻击手段；第 3 部分主要介绍黑客对网站、网络的攻击手段；第 4 部分对网络安全防护体系的一些组成部分做了简要介绍。本书的光盘中包含了大量常用的黑客软件。

本书适用于计算机网络管理员、系统维护人员、网络用户、计算机爱好者及大专院校有关专业师生阅读参考。

敬告：破坏性的黑客行为违反我国有关法律规定，对他人实施攻击可能需要承担法律责任。出版本书(盘)的目的只是为了更有效地保障用户的系统与信息安全。

书　名：黑客就这么几招
作　者：阎雪
出版者：万方数据电子出版社
印刷者：北京门头沟胶印厂
发　行：新华书店总店北京科技发行所
开　本：16　印张：19.5　字数：453 千字
版　次：2000 年 12 月第 1 版　2001 年 2 月第 2 次印刷
印　数：5001～8000
书　号：ISBN 7-900050-68-X/TM・34
定　价：29.00 元 (1CD)

前　言

随着因特网的日益普及，上网对于许多人来说已经成为生活中必不可少的一部分，新老网民们通过网络来查找资料、交流信息。对于企业而言，网络更是占有举足轻重的地位，电子商务已经有逐步取代传统企业经营方式的趋势。但网络在带给我们极大便利的同时，也带来了另外一个棘手的问题，就是“黑客”问题。

由于因特网本身的设计缺陷及其开放性，使其极易受到黑客的攻击。根据美国有关安全部门统计，因特网上 98%的计算机受到过黑客的攻击性分析，50%的机器被黑客成功入侵，而被入侵机器中有 20%的管理员尚未发现自己已经被入侵。网络的安全性已经成为阻碍因特网在全球发展的重要因素之一。最近，美国包括“雅虎”、“亚马逊”、CNN 在内的一些著名网站遭到黑客的大规模袭击，蒙受了巨大经济损失，引起了全世界对网络安全的密切关注。越来越多的人意识到，黑客已经成为全球新的公害，必须采取有力措施保护网络免受其扰。

在许多人眼中，“黑客”是一些高深莫测的神秘人物，他们利用手中所掌握的技术肆意攻击网站、盗取商业机密。加上一些媒体对黑客事件不负责任的夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘面纱。其实，黑客以及黑客技术并不神秘，也并不高深。一个普通网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无须任何知识，只要学会使用一些黑客软件，同样可以对网络实施攻击，这也正是如今网络攻击如此盛行的原因之一。

俗话说，“知己知彼，百战不殆”。想要更好地保护自己不受黑客的伤害，就必须对黑客技术有一定的了解。只有对黑客的种种攻击手段有了详尽的认识，才能进行更有效、更具针对性的防护，使自己免受黑客攻击。我们本着使中国广大网民“认识黑客，了解黑客、防御黑客”的原则编写了这本书，从攻击技术的角度对黑客的种种手段作了详尽的介绍，目的在于让普通网民以及网络管理员对黑客技术有一个大致的了解，从而能够保护自己免受伤害，或把损失降低到最小程度。需要强调的是，黑客行为是违反我国有关法律规定的，如果对别人实施攻击并造成了损失，则必须对自己的行为负法律责任。基于上述原因，本书在每介绍一种攻击手法的同时，都会给出与之相对应的详尽的防护方法，希望读者能够善用本书。

本书的重点在于介绍黑客的攻击手段和提供相应的保护措施，在组织结构上共分四个部分：

第 1 部分主要介绍黑客的历史、行为准则以及相关的基础知识，包括第 1 章“黑客的历史”和第 2 章“基础知识介绍”。

第 2 部分主要介绍黑客对普通用户的攻击手段，包括第 3 章“计算机病毒”、第 4 章“特洛伊木马”和第 5 章“网络炸弹”。

第 3 部分包括第 6 章“网络攻击的一般步骤及实例”、第 7 章“扫描器”、第 8 章“缓

冲区溢出”、第 9 章“密码破解”、第 10 章“sniffer”、第 11 章“利用 Web 进行攻击”、第 12 章“拒绝服务攻击”、第 13 章“IP 欺骗攻击”和第 14 章“常见的系统漏洞及攻击实例”。这一部分主要介绍黑客对网站、网络的攻击手段。

第 4 部分对网络安全防护体系的一些组成部分做了简要介绍，包括第 15 章“数据加密技术”、第 16 章“防火墙技术”和第 17 章“入侵检测系统”。

由于作者本人水平有限，加之时间仓促，书中难免有不当之处，还望广大读者多提宝贵意见。

作者

2000 年 11 月

目　录

第 1 部分　基 础 知 识

第 2 部分 攻击普通用户

第 3 部分　攻击网络与网站

第 4 部分 网络安全防护

第1部分 基础知识

第1章 黑客的历史

在网上聊天时，常常听到网友谈论："我昨天被某某某黑了！"在很多人眼里，"黑客"就是网络破坏者的代名词。实际上大多数人并不了解什么是真正的黑客，更不了解黑客的历史。其实真正的黑客并不是攻击者，而是创造者。本书的第 1 章主要介绍黑客的历史以及黑客的精神。

1.1 黑客文化简史

在虚拟的网络世界里，活跃着一批特殊的人，他们为电脑而生，是真正的程序员，有过人的才能和乐此不倦的创造欲。技术的进步给了他们表现自己的美好天地，因为有了他们的存在，才使原本森严冰冷的计算机技术世界多了一份戏谑，多了一份调侃。一般人们把他们称之为"黑客"，即 Hacker。下面首先介绍一下黑客文化的发展历史。

1.1.1 古典黑客时代

说到黑客的历史，首先要从"真正的程序员（Real Programmer）"开始。"真正的程序员"这个名词在 20 世纪 80 年代才出现，但早自 1945 年起，电脑科学便不断地吸引世界上头脑最顶尖、想象力最丰富的人投入其中。从 Eckert & Mauchly 发明电子数字积分计算机（ENIAC）后，便不断有狂热的程序员投入其中，他们以编写软件与玩弄各种程序设计技巧为乐，逐渐形成具有自我意识的一套科技文化。

当时这批"真正的程序员"主要来自工程界与物理界，他们戴着厚厚的眼镜，穿着聚酯纤维 T 恤与纯白袜子，用机器语言、汇编语言、FORTRAN 及很多古老的语言编写程序。他们是黑客时代的先驱者，默默贡献，却鲜为人知。从二次世界大战结束到 20 世纪 70 年代早期，是打卡计算机与大型机（mainframes）流行的年代，由"真正的程序员"主宰电脑文化。

"真正的程序员"的时代步入尾声后，取而代之的是逐渐盛行的交互式计算（Interactive Computing），各大学成立电算相关科系并建立电脑网络。黑客时代始于 1961 年麻省理工学院（MIT）出现的第一台电脑——DEC PDP-1。麻省理工学院的技术模型铁路俱乐部（Tech Model Railroad Club，简称 TMRC）的动力信号组（Power and Signals Group）买了这台机器后，把它当成最时髦的科技玩具，各种程序工具与电脑术语由此开始出现，整个环境与

文化一直发展下去，直到今日。20 世纪 80 年代早期学术界人工智能的权威——麻省理工学院的人工智能实验室（Artificial Intelligence Laboratory），其核心人物皆来自 TMRC。从 1969 年起，也就是 ARPANET 建制的第一年，这群人在电脑科学界便不断有重大突破与贡献。ARPANET 是第一个横跨美国的高速网络，由美国国防部出资兴建，从一个实验性质的数据通信网络，逐渐成长成联系各大学、国防部承包商及研究机构的大型网络。各地研究人员能以史无前例的速度与弹性交流信息，而这种超高效率的合作模式导致了科技的突飞猛进。ARPANET 的另一项好处是，信息高速公路使得全世界的黑客能聚在一起，不再像以前那样孤立地在各地形成一股股短命的文化，网络把他们汇集成一股强大的力量。

开始有人感受到黑客文化的存在，动手整理一些术语放在网络上，在网上发表讽刺文学并讨论黑客所应有的道德规范。黑客文化在连接到 ARPANET 的各大学间快速发展，特别是（但不全是）在与信息相关的科系内。一开始，整个黑客文化的发展以麻省理工学院的人工智能实验室为中心，但斯坦福大学（Stanford University）的人工智能实验室（Artificial Intelligence Laboratory，简称 SAIL）与稍后的卡内基-梅隆大学（Carnegie-Mellon University，简称 CMU）也快速崛起了。这三个都是大型的信息科学研究中心及人工智能方面的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对黑客文化都有极高的贡献。

随着科技的进步，麻省理工学院人工智能实验室逐渐淡出舞台。从麻省理工学院那台 PDP-1 开始，黑客们的主要程序开发平台都是数字装备公司（Digital Equipment Corporation）的 PDP 迷你电脑系列。DEC 率先发展出以商业用途为主的交互式计算机（Interactive Computer）及时间共享（Time-Sharing）操作系统，当时许多大学都买 DEC 的机器，因为它兼具弹性与速度，还很便宜（相对于较快的大型电脑）。便宜的分时系统是黑客文化能快速成长的因素之一。在 PDP 流行的时代，ARPANET 上是 DEC 机器的天下，其中最主要的便是 PDP-10，它受到黑客们的青睐达 15 年之久；TOPS-10（DEC 的操作系统）与 MACRO-10 使用得也很普遍。

麻省理工学院也用 PDP-10，但他们不屑用 DEC 的操作系统。他们偏要自己写一个，即赫赫有名的 ITS，其全名是矛盾分时共享系统（Incompatible Time Sharing System）。ITS 始终不稳，设计古怪，臭虫也不少，但仍有许多独到的创见，似乎还是分时系统中开机时间最久的记录保持者。ITS 大部分是用汇编语言写的，其他部分用 LISP 写成。LISP 在当时是一种威力强大、极具弹性的程序设计语言。事实上，25 年后的今天，它的设计仍优于目前大多数的编程语言。LISP 让 ITS 的黑客得以尽情发挥想象力。LISP 是麻省理工学院人工智能实验室成功的最大功臣，现在它仍是黑客们的最爱之一。很多 ITS 的产品到现在仍流行着，EMACS 大概是最有名的一个。SAIL 的骨干后来成为 PC 界或图形界面开发的重要角色。CMU 的黑客则开发出第一个实用的大型专家系统与工业用机器人。

1969 年，也就是 ARPANET 成立的那一年，AT&T 贝尔实验室的年轻小伙子肯·桑普森（Ken Thompson）发明了 Unix。桑普森曾经参与 Multics 的开发。Multics 源自 ITS 的操作系统，用来实验当时一些较新的操作系统理论，如把操作系统较复杂的内部结构隐藏起来，仅提供一个界面，使程序员不用深入了解操作系统与硬件设备也能快速开发程序。

直到后来 C 语言发明以后，桑普森用 C 把原来用汇编语言写的 Unix 重写一遍。C 的设计原则是好用、自由与弹性。C 与 Unix 很快在贝尔实验室得到欢迎。1971 年桑普森与里特驰（Ritchie）争取到一个办公室自动化系统的项目，Unix 开始在贝尔实验室中流行起

来。不过桑普森与里特驰的雄心壮志还不止于此。那时的传统是，一个操作系统必须完全用汇编语言写成，才能让机器发挥最高的效能。桑普森与里特驰是首先掌握硬件与编译器技术的学者，他们已经进步到可以完全用高级语言（如 C）来编写操作系统，而仍保持不错的功能。5 年后，Unix 已经成功地移植到数种机器上。

第一部 PC 出现在 1975 年，其后 Apple 计算机公司在 1977 年成立，并以飞快的速度成长。微电脑的潜力立刻吸引了另一批年轻的黑客。他们最爱的编程语言是 BASIC，由于它过于简单，PDP-10 的爱好者与 Unix 迷们根本不屑用它，更看不起使用它的人。这群人中有一位大家一定熟悉，他的名字叫比尔•盖茨，最初就是他在 8080 处理器上发展 BASIC 编译器的。而由盖茨建立起来的微软帝国也标志着古典黑客时代的结束。

1.1.2　现代黑客时代

应该说前面提到的古典黑客和传统思想所理解的黑客是不同的。古典黑客是真正的程序员和纯粹的理想主义者，可以说是他们创造并推动了计算机工业的发展。但是到了 80 年代，随着工业化进程的推进，在技术方面，黑客们越来越多地把精力放到寻找各种各样的系统漏洞上，并通过暴露网络系统中的缺陷、非法更改服务器的行为来达到表现自我、反对权威的目的。1995 年初，当维萨（VISA）、万事达（MASTER）、微软和网景结成联盟，允诺在互联网上建立安全商业服务时。网景于当年 9 月 18 日发表了一个供人们通过因特网进行信用卡购物的软件，但第二天报纸上就出现轰动性新闻：两名加州大学的研究生黑客伊恩 • 戈德伯格和大卫 • 瓦格纳发现了软件程序中的一个漏洞。网景随后立刻推出修正版。然而仅隔 8 天，一位法国黑客又破译了这个新版本，同时警告说那些声称金融交易安全无虞的公司将很快发现他们的声明受到挑战。戈德伯格们遵循黑客文化群由来已久的查找缺陷并予以公开发表的传统，这样做的目的无非是要求无休止地完善软件。

这时，在黑客界中也产生了分歧，一些思想传统的黑客认为黑客应该是那些热衷于编程和查找并公布系统漏洞的人，而那些通过利用系统漏洞进行网络攻击来表现自我的人是不配叫做黑客的。所以又有了黑客（Hacker）和骇客（Cracker）之分，前者指具有反传统精神的程序员，后者则是指利用工具攻击别人的攻击者，具有很明显的贬义。无论是黑客还是骇客，都是具备高超的计算机知识的人，即使要达到骇客的水准也是相当不容易的。

到了信息技术高度发达的今天，黑客又有了新的特征。

首先是黑客组织化、集团化。以前那样单兵作战的黑客越来越少了，取而代之的是大量的黑客组织。黑客组织的优势是利用成员各自的不同特长进行合作攻击，从而提高成功率。另外成员之间便于互相交流，提高整体水平。世界著名的黑客组织有德国的混沌计算机俱乐部（Chaos Computer Club）、美国的大屠杀 2600（Genocide2600）和地下兵团（Underground）等，本章第 4 节会对其中一些组织做详细介绍。

现代黑客的第二个特点是商业化。除了少数黑客通过进行攻击活动来得到巨额非法收入外，更多的黑客把自己的技术当作谋生的手段，他们受雇于网络安全公司。由于熟悉黑客攻击技术，这些人可以为互联网公司提供较为有效的安全防护措施。例如世界著名网络安全公司 ISS 的克劳斯，本来是美国著名的黑客，现在已经是美国总统的网络安全顾问。ISS 公司在国际网络安全市场的份额超过 50%，现已成为全球前 500 强企业中许多公司以及全美前 25 家最大商业银行中的 21 家、10 家最大电信公司中的 9 家，以及 35 家政府机

构最值得信赖的重要安全顾问。再如国内原著名的黑客组织“绿色兵团”，曾经攻击过一系列印尼军政站点和国内的某大型网站。现在“绿色兵团”已经改名为绿盟公司，并成为国内最大的商业性网络安全公司之一。

现代黑客的另一个特点是政治化。由于网络在国民生产生活、尤其是国家军事安全中占有越来越重要的地位，网络安全可能会直接影响到国家安全，各国政府都在准备迎接信息战争的挑战。相当多的黑客被政府部门雇佣，从事国家网络安全防护与攻击的研究。在科索沃战争期间，美国总统克林顿命令美国政府雇佣的电脑黑客冲破障碍，查到米洛舍维奇在外国银行里的存款，并抽走他隐藏的财富。这是美国中央情报局旨在推翻南斯拉夫总统的秘密计划的一部分。

黑客不仅作为一种技术现象，更作为一种文化，已经在网络世界里发展了几十年，并且深深地扎下了根，可以说黑客是伴随计算机工业的发展而产生和演变的。可以预料，在今后相当长的一段时期内，它还会继续发展下去。如果想要靠打击、封杀来消灭黑客是不可能的，只有充分了解黑客、认识黑客，才能真正把黑客引向正途，让黑客技术为国家、为社会服务。

下一节将介绍作为一名黑客所应当遵守的行为准则。

1.2 黑客行为准则

首先，作为一名黑客必须搞清楚黑客行为的目的，因为世界上充满着急待被解决的迷人问题，黑客应该从解决问题的过程中获得快乐。而这是一种因为努力而得到成果所带来的快乐。除道义以外，黑客也应该遵循一定的行为准则，下面是在世界范围内得到比较广泛认可的黑客行为准则：

- Never damage any system. This will only get you into trouble.

不恶意破坏任何系统，这样做只会带来麻烦。恶意破坏他人的软件或系统将导致法律刑责。

- Never alter any of the systems files, except for those needed to insure that you are not detected, and those to insure that you have access into that computer in the future.

绝不修改任何系统文件，除非有绝对的必要，或者改那些文件是为了使以后更容易地再次进入这个系统。

- Do not share any information about your hacking projects with anyone but those you'd trust.

不要将已破解的任何信息与人分享，除非此人绝对可以信赖。

- Never use anyone's real name or real phone number when posting on a BBS.

在 BBS 上发表文章的时候不使用真名和真实的电话号码。

- DO NOT hack government computers.

千万不要入侵或破坏政府机关的主机。

- To become a real hacker, you have to hack. You can't just sit around reading text files and hanging out on BBS's. This is not what hacking is all about.

真正的黑客，必须真枪实弹去做黑客应该做的事情（例如对系统作详尽的研究，而不是简单地入侵某个系统）。不能仅仅靠坐在家里读些黑客之类的文章或者从 BBS 中找点东西，就能成为黑客，这不是“黑客”的真正含义。

1.3　黑客必须具备的技能

黑客的精神态度虽然是很重要的，但是真正对信息社会构成威胁的还是黑客所具备的强大技术。真正的黑客必须是一名计算机天才，并且必须对获取新知识、创造新技术有着强烈的渴望而不感到疲倦。当然这里说的“黑客”，是指真正对网络安全形成威胁的人，而不是那些使用某种现成的工具对网络进行攻击的攻击者。真正的黑客管这种人叫做 script kid（只会使用工具的孩子），虽然 script kid 也会对网络安全构成一定的威胁，但是这类进攻是比较容易防范的。而真正厉害的角色是那些具备相当深厚的系统知识的人，如果他们发起进攻，那么打击将会是难以抵抗和致命的。

其实黑客应该对所有计算机知识了如指掌，而不是单单掌握与攻击相关的知识。当然，从单纯攻击方面来讲还是必须了解一些与其他计算机工作人员所不同的内容，列举如下：

1. 必须对网络上常见的操作系统有深入的研究，例如 Unix、Windows NT 等。这里说的是深入的研究，而不是简单地学会使用，应该了解系统内核的工作原理以及系统上运行的常用软件的使用方法。
2. 应该熟悉各种网络协议，在因特网上主要是 TCP/IP 协议。
3. 黑客首先应该是程序员。如果对编程一窍不通，只是简单地使用工具，那只能对个别特定的系统进行攻击，是不可能真正威胁到大量系统安全的。
4. 收集相关的系统漏洞。对已知漏洞的分析有利于发现新的漏洞和提高安全防护能力。

即使对上述知识完全掌握了，也不能算作一名真正的黑客，正如前面提到的，黑客真正可怕之处在于他对新知识的渴望与不懈的创造力。

1.4　世界著名的黑客及组织

看了这么多有关黑客历史以及精神方面的讲述，大家一定想看一看世界著名黑客的风采吧。下面就介绍一下大名鼎鼎的美国黑客组织“大屠杀 2600”（Genocide2600）和被公认为“世界头号电脑黑客”的凯文·米特尼克。

1.4.1　大屠杀 2600

美国鼎鼎大名的“大屠杀 2600”（Genocide2600）黑客组织，现在已经拥有 150 多万成员。他们来自各行各业，年龄从 14 岁至 57 岁。他们外表上和常人没什么区别，没准儿就是一个加油站的伙计或者送牛奶的孩子。但他们的群体扩展得非常之快，按他们自己的说法，“像知识传播一样快”。一般人绝对想不到的是，他们其中有人完全不懂任何专业的