见招拆招

黑客攻防工具箱

陈洪彬　谢　哲　赵承源　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

见招拆招

黑客攻防工具箱

陈洪彬　谢　哲　赵承源　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

EVERYTHING THAT HAS A BEGINNING HAS AN END

内 容 简 介

本书主要介绍了黑客常用的和用于防范的一些工具，整合为一本“黑客攻防工具箱”，包括常用系统命令、IP及端口扫描工具、聊天黑客工具与防范、邮件黑客工具与防范、网吧及网络游戏黑客工具与其防护、网页黑客工具与防护、文档密码破译工具与防范、共享软件的加、解密工具、远程控制工具及防护、揭秘局域网黑客工具和攻击防范工具。包罗了黑客攻击及防范的使用方法。从基础开始介绍，详细地讲解了这些工具的使用和防范方法，以及计算机和网络安全的相关知识。

本丛书从黑客攻防的角度切入，适用于网络安全及对黑客攻防感兴趣的读者，特别适用于普通大众读者，即使是没有任何网络操作经验及计算机安全防范经验的读者，也可以按照本书实例轻松地进行操作演练和计算机、网站等安全配置，排除计算机与网络的安全隐患。本书适合作为网络安全爱好者及学生、寻求进入IT领域专业人士的参考用书，对于那些希望拓展自己的知识领域，在网络安全方面开拓视野，循序渐进地学习和研究网络安全知识及技术的读者，本书也有极高的参考价值。

图书在版编目（CIP）数据

见招拆招：黑客攻防工具箱/陈洪彬，谢哲，赵承源编著. —北京：中国铁道出版社，2008.10
（黑客全攻略系列）
ISBN 978-7-113-09218-4

Ⅰ.见… Ⅱ.①陈…②谢…③赵… 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（2008）第152901号

书　　名：见招拆招——黑客攻防工具箱
作　　者：陈洪彬　谢　哲　赵承源　编著

策划编辑：严晓舟　李鹤飞
责任编辑：苏　茜　　编辑部电话：（010）63583215
编辑助理：李鹤飞　张　丹　　封面制作：白　雪
封面设计：付　巍　　责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京市兴顺印刷厂
版　　次：2008年10月第1版　　2008年10月第1次印刷
开　　本：787mm×960mm　1/16　　印张：32.5　　字数：599千
印　　数：5 000册
书　　号：ISBN 978-7-113-09218-4/TP·2989
定　　价：54.00元

前　言

随着计算机以及网络的普及、黑客工具的出现，一些别有用心的人，使用简单的工具，对一些疏于防范的计算机作出攻击，并在侵入他人的计算机后为所欲为。当用户发现自己的密码被盗、资料被修改删除、硬盘变作一片空白，甚至自己的隐私和秘密在不知不觉中早已在网上飞速传播公之于众时，说明你的计算机已遭到黑客的入侵，但发现为时已晚。

本书便是基于防范和保护的目的而诞生，在了解基础的网络知识、熟悉通常的黑客攻击手段与常用黑客软件后，用知识与技巧将计算机与网络更好地保护起来，达到防患于未然的目的。

网络时代产生了无数攻击他人计算机的程序或软件，如木马、病毒、盗号器、暴力破解机等，可能连搜索引擎都可以翻出你的“陈年旧事”，而反病毒软件、木马克星、密码保护等“对策”也应时而生，攻击与防御的“魔”、“道”之争愈演愈烈，究竟是用于破坏的“矛”更加锋利，还是用于防御保护的“盾”更加坚固？当然是“防御”战胜“破坏”。然而世间不存在绝对完美的技术。通过本书，我们或许可以找到一张相当坚固的“防护墙”，却仍要不断学习新技术，防御不断变化和进攻的“技术白蚁”对计算机程序和宝贵资料的“进攻”和“啃噬”，这是学习防御工具和技术的乐趣所在。

本书分为十一章，内容涵盖了常用系统指令、IP 及端口扫描工具、聊天黑客工具与防范、邮件黑客工具与防范、网吧及网络游戏黑客工具与其防护、网页黑客工具与防范、文档密码破译工具与防范、共享软件的加、解密工具、远程控制工具及防护、揭秘局域网黑客工具和攻击防范工具等内容，由浅入深地讲述了黑客攻击的原理、常用手段以及防御措施。希望读者了解技术原理的同时，将破坏的“火焰”挡在门外。

我们有理由相信，拥有了技术的“武器”，当开始网络之旅时，每个人都将成为维护网络安全与正义的“骑士”。

本书由陈洪彬、谢哲、赵承源编写，参加本书资料整理、搜集和编写的还有王江伟、董茜、余甜甜、罗景尚、彭岷、朱浩、罗翼鹏、曾继红、叶峥、林燕霞、汤婷、储健轩、莫晓翔、吴雷、王俊如、徐谡、李红艳、胡暇、徐园、秦兵峰、张梨、陈瑞东、颜廷强、赵鹏飞、朱玺君。在此一并表示感谢。

严正声明：根据国家有关法律规定，任何利用黑客技术攻击他人数据、资料及网络均系违法行为。本书的写作目的是研究技术和加强防范保护能力，绝非支持黑客技术的错误使用，也不承担任何对书中内容的错误使用带来的后果。请读者不要将学习的技术用于破坏，否则后果自负。

编　者

2008 年 8 月 1 日

目　录

第0章 黑客知识简介

0.1 黑客简介

1．黑客的历程

黑客最早出现于20世纪50年代，最早的计算机1946年在宾夕法尼亚大学出现，而最早的黑客出现于麻省理工学院，贝尔实验室也有。最初的黑客一般都是一些高级技术人员，他们热衷于挑战、崇尚自由并主张信息共享。

1994年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且网络也逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了，黑客攻击效果如图0-1所示。

图0-1 黑客攻击效果图

2．黑客的由来

“黑客”一词是由英语Hacker音译出来的，是指专门研究、发现计算机和网络漏洞的计算机爱好者。他们伴随着计算机和网络的发展而产生成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断研究计算机和网络知识，发现计算机和网络中存在的漏洞。他们喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

黑客不干涉政治，不受政治利用，他们的出现推动了计算机和网络的发展与完善。黑客所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡

自由、平等。黑客的存在是由于计算机技术的不健全所至，从某种意义上来讲，计算机的安全需要更多黑客去维护。借用 myhk（黑客英雄网站长）的一句话“黑客存在的意义就是使网络变得日益安全完善”。

但是到了今天，黑客一词已经被用于那些专门利用计算机进行破坏或入侵他人系统的人的代名词，对这些人正确的叫法应该是 Cracker，有人也翻译成“骇客”，也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，被人们认为是在网络上进行破坏的人。根据开放原始码计划创始人 Eric Raymond（埃里克·雷蒙德）对此字的解释：Hacker 与 Cracker 是分属两个不同世界的族群，基本差异在于，Hacker 是有建设性的，而 Cracker 则专门搞破坏。下面是缔造自由软件的三黑客，如图 0-2 所示。

图 0-2　缔造自由软件的三黑客

3．史上五大最著名黑客

（1）黑客代言人——凯文·米特尼克（Kevin Mitnick），如图 0-3 所示。

图 0-3　五大黑客之一

从某种意义上讲，米特尼克也许已经成为黑客的同义词。美国司法部曾经将米特尼克称为“美国历史上被通缉的头号计算机罪犯”，他的所作所为已经被记录在两部好莱坞电影中，分别是“Takedown”和“Freedom Downtime”。

米特尼克“事业”的起点是破解洛杉矶公交车打卡系统，他因此得以免费乘车。在此之后，他也同苹果联合创始人史蒂夫·沃兹尼亚克（Steve Wozniak）一样，试图盗打电话。米特尼克首次被宣判有罪是因为非法侵入 Digital Equipment 公司的计算机网络，并窃取软件。

之后的两年半时间里，米特尼克展开了疯狂的黑

客行动。他开始侵入计算机，破坏电话网络，窃取公司商业秘密，并最终闯入了美国国防部预警系统。最终，他因为入侵计算机专家、黑客 Tsutomu Shimomura 的家用计算机而落网。在长达五年零八个月的单独监禁之后，米特尼克现在的身份是一位计算机安全作家、顾问和演讲者。

（2）“不回家的黑客”——阿德里安·拉莫（Adrian Lamo），如图 0-4 所示。

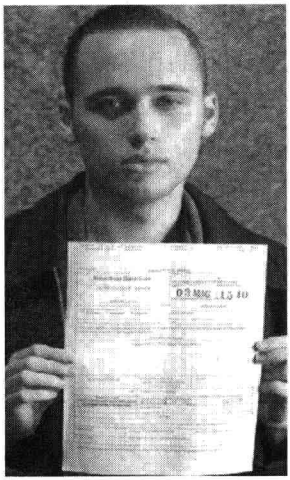

图 0-4　五大黑客之二

拉莫专门找大公司或组织下手，例如入侵微软和《纽约时报》的内部网络。他经常利用咖啡店、金考复印店或图书馆的网络来从事黑客行为，因此他获得了一个“不回家的黑客”的绰号。拉莫经常能发现安全漏洞，并对其加以利用。通常情况下，他会通知企业有关漏洞的信息。

拉莫的受害者名单上包括雅虎、花旗银行、美洲银行和 Cingular 等知名公司。白帽黑客这样做并不违法，因为他们受雇于公司。但是，拉莫却从事着非法行为。由于侵入《纽约时报》内部网络，拉莫成为顶尖数码罪犯之一。也正是因为这一罪行，他被处以 6.5 万美元罚款，以及六个月家庭禁闭和两年缓刑。拉莫现在是一位著名公共发言人，同时还是一名获奖记者。

（3）最年轻的黑客——乔纳森·詹姆斯（Jonathan James），如图 0-5 所示。

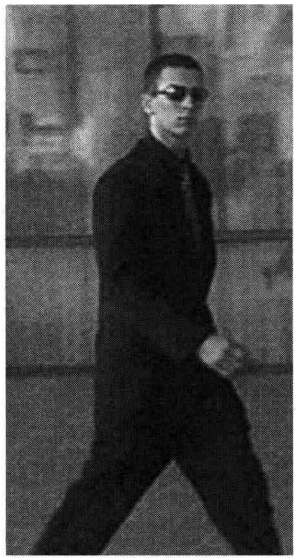

图 0-5　五大黑客之三

在 16 岁时，詹姆斯成为了第一个因为黑客行为而被送入监狱的未成年人，并因此恶名远播。他此后承认自己当初只是为了好玩和寻求挑战。

詹姆斯曾经入侵过很多著名组织，包括美国国防部下设的国防威胁降低局。通过此次黑客行动，他可以捕获用户名和密码，并浏览高度机密的电子邮件。詹姆斯还曾入侵过美国宇航局的计算机，并窃走价值 170 万美元的软件。据美国司法部长称，他所窃取的软件主要用于维护国际空间站的物理环境，包括对湿度和温度的控制。

当詹姆斯的入侵行为被发现后，美国宇航局被迫关闭了整个计算机系统，并因此花费了纳税人的 4.1 万美元。目前，詹姆斯正计划成立一家计算机安全公司。

（4）教授级别黑客——罗伯特·塔潘·莫里斯（Robert Tappan Morris），如图 0-6 所示。

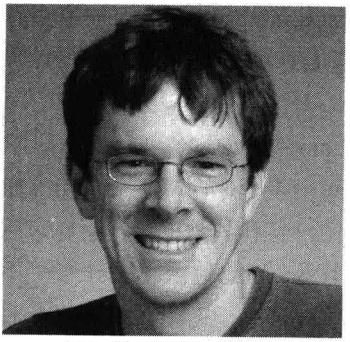

图 0-6　五大黑客之四

莫里斯的父亲是前美国国家安全局的一名科学家，名叫罗伯特·莫里斯 (Robert Morris)。他是莫里斯蠕虫的制造者，这是首个通过互联网传播的蠕虫。正因为如此，他成为了首位依据 1986 年《计算机欺诈和滥用法》被起诉的人。

莫里斯在康奈尔大学就读期间制作了蠕虫，当时的目的仅仅是为了探究互联网有多大。然而，莫里斯蠕虫以无法控制的方式自我复制，造成很多计算机死机。据专家称，约有 6 000 台计算机遭到破坏。他最后被判处 3 年缓刑、400 小时社区服务和 1.05 万美元罚款。

莫里斯目前是麻省理工学院计算机科学和人工智能实验室的一名终身教授，主攻方向是计算机网络架构。

（5）“黑暗但丁”——凯文·鲍尔森（Kevin Poulsen），如图 0-7 所示。

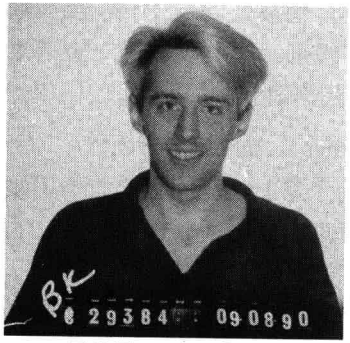

图 0-7　五大黑客之五

鲍尔森经常被称为“黑暗但丁”，他因非法入侵洛杉矶 KIIS-FM 电话线路而闻名全美，同时也因此获得了一辆保时捷汽车。就连美国联邦调查局（FBI）也开始追查鲍尔森，因为他闯入了 FBI 数据库和联邦计算机，目的是获取敏感的窃听信息。

鲍尔森的专长是入侵电话线路，他经常占据一个基站的全部电话线路。鲍尔森还经常重新激活黄页上的电话号码，并提供给自己的伙伴用于出售。他最终在一家超市被捕，并被处以五年监禁。

在监狱服刑期间，鲍尔森担任了《连线》杂志的记者，并升任高级编辑。在他最著名的一篇文章中，主要讲述了他如何通过 MySpace 的个人资料找到 744 名性犯罪者。

0.2　黑客攻击方法原理概述

1．黑客攻击的步骤

（1）隐藏自己的位置。

普通攻击者都会利用别人的计算机隐藏他们真实的 IP 地址。老练的攻击者还会利用 800 电话的无人转接服务连接 ISP，然后再盗用他人的账号上网。

（2）寻找目标主机并分析目标主机。

攻击者首先要寻找目标主机并分析目标主机。在 Internet 上能真正标识主机的是

IP 地址，域名是为了便于记忆主机的 IP 地址而另起的名字，只要利用域名和 IP 地址就可以顺利地找到目标主机了。当然，知道了要攻击目标的位置还是远远不够的，还必须将主机的操作系统类型及其所提供服务等资料做个全面的了解。此时，攻击者们会使用一些扫描工具，轻松获取目标主机运行的是哪种操作系统的哪个版本、系统有哪些账户以及 WWW、FTP、Telnet、SMTP 等服务器程序是何种版本等资料，为入侵做好充分的准备。

（3）获取账号和密码，登录主机。

攻击者要想入侵一台主机，首先要有该主机的账号和密码，否则就会无法登录。这样常促使他们先设法盗窃账户文件，进行破解，从中获取用户的账户和口令，再寻找合适时机以此身份进入主机。当然，利用某些工具或系统漏洞登录主机也是攻击者常用的一种技法。

（4）获得控制权。

攻击者们用 FTP、Telnet 等工具，利用系统漏洞进入目标主机系统获得控制权之后，就会做两件事：清除记录和留下后门。他们会更改某些系统设置、在系统中置入特洛伊木马或其他一些远程操控程序，以便日后可以不被觉察地再次进入系统。大多数后门程序是预先编译好的，只需要想办法修改时间和权限就可以使用了，甚至新文件的大小都和原文件一模一样。攻击者一般会使用 rep 传递这些文件，以便不留下 FTB 记录。清除日志、删除复制的文件等手段来隐藏自己的踪迹之后，攻击者就开始进行下一步的行动。

（5）窃取网络资源和特权。

攻击者找到攻击目标后，会继续下一步的攻击。如，下载敏感信息；实施账号密码、信用卡号等经济窃取；使网络瘫痪。

2．黑客攻击的原理和方法

（1）口令入侵：是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。

这种方法的前提是必须事先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法有很多，例如：利用目标主机的 Finger 功能，当用 Finger 命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示到终端或计算机上；利用目标主机的 X.500 服务，因为有些主机没有关闭 X.500 的目录查询服务，会给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集信息，有些用户的电子邮件地址常会透露其在目标主机上的账号；查看主机是否有习惯性的账号，有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号泄露。