TURING

3rd Edition

Hacking FOR DUMMIES

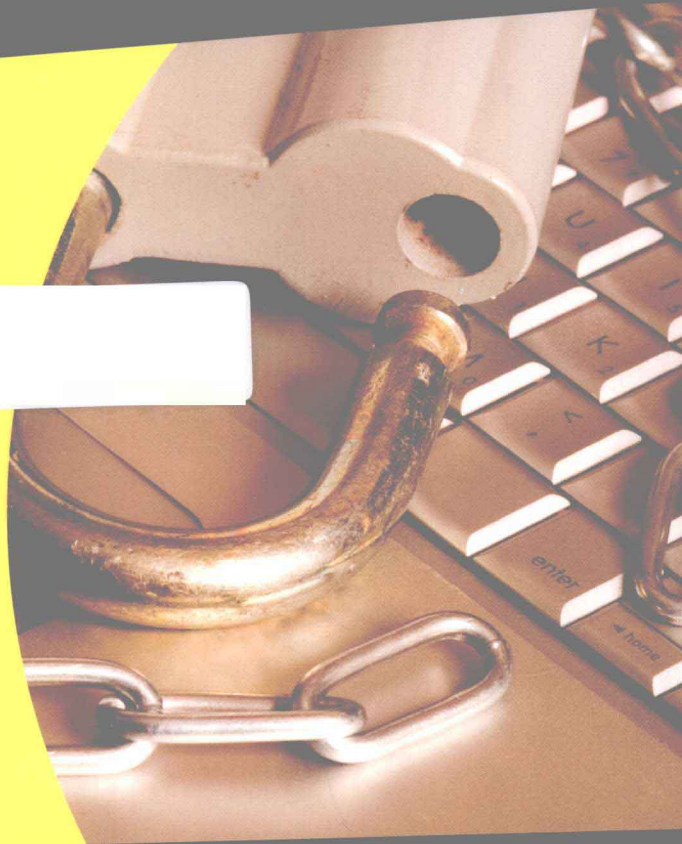
达人迷

黑客达人迷

（第3版）

从本书可以学到：

- 使用最新道德黑客攻击方法和工具
- 测试 Windows 或 Linux 系统
- 利用攻击检测数据库、VoIP 系统和 Web 应用
- 汇报测试漏洞，改善信息安全

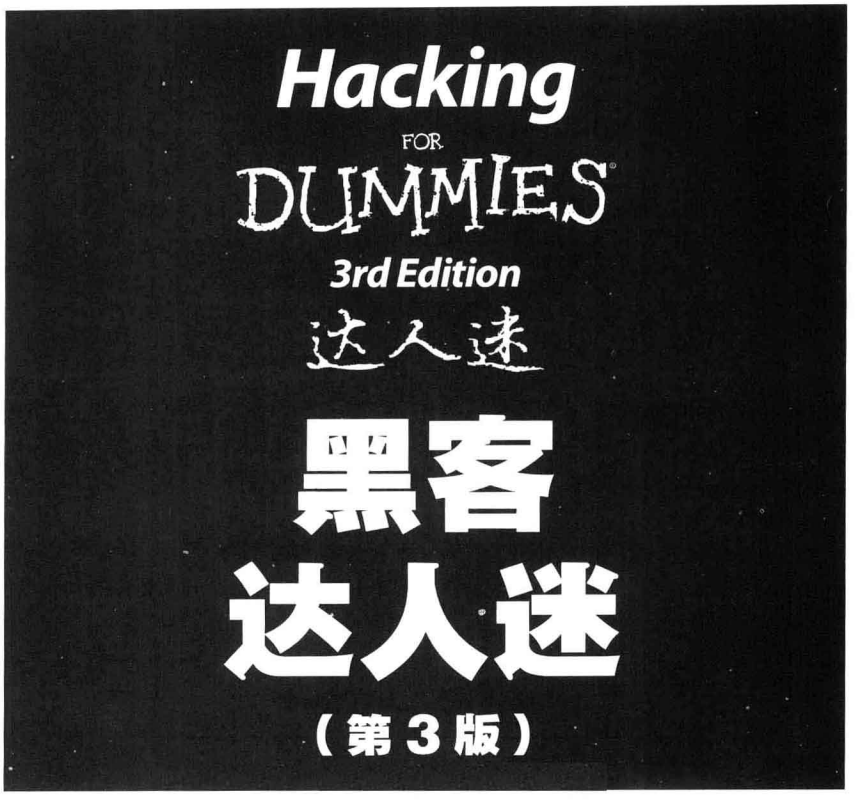


◎ [美] Kevin Beaver 著

◎ 傅尔也 译

人民邮电出版社
POSTS & TELECOM PRESS

TURING



◎[美] Kevin Beaver 著
◎傅尔也 译

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客达人迷 : 第3版 / (美) 比弗 (Beaver, K.) 著; 傅尔也译. -- 北京 : 人民邮电出版社, 2013.1
书名原文: Hacking For Dummies, 3rd Edition
ISBN 978-7-115-29348-0

Ⅰ. ①黑… Ⅱ. ①比… ②傅… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第220678号

内 容 提 要

本书以别具一格的视角、幽默生动的语言详尽地介绍了道德黑客攻击的全过程，旨在帮助读者在网络安全战争中知己知彼，百战不殆。本书以道德黑客攻击计划为主线，系统讲述了常见黑客攻击方法及防御对策，并辅之以知名信息安全专家的安全测试案例，结构清晰，内容全面，是企业和个人进行计算机系统安全测试与评估的参考指南。

作为“达人迷”系列书之一，本书不仅适用于对计算机系统测试评估和IT安全感兴趣的初学者，而且对于网络管理员、信息安全经理、信息安全顾问、安全审计人员等专业人士也具有很大的参考价值。

黑客达人迷（第3版）

◆ 著 [美] Kevin Beaver
译 傅尔也
责任编辑 朱 巍
执行编辑 张 霞

◆ 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 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：21.5
字数：439千字 2013年1月第1版
印数：1-4 000册 2013年1月北京第1次印刷
著作权合同登记号 图字：01-2012-0710号

ISBN 978-7-115-29348-0

定价：49.00元

读者服务热线：(010)51095186转604 印装质量热线：(010)67129223
反盗版热线：(010)67171154

序

十几年之前，IT安全还只是襁褓中的新生儿。1994年，安全专业人员屈指可数，很少有进行过安全实践的，真正理解安全的就更少了。那时候的安全技术无非是杀毒软件和包过滤路由器。而且“黑客”（hacker）一词主要源于好莱坞电影《战争游戏》（*WarGames*），更多是指那些高尔夫打得不好的人。结果，就像喜剧演员罗德尼·丹泽菲尔德所说的，它“没有受到重视”，没人愿意拿正眼瞧它。IT专业人员大都讨厌它，对其不予理睬，直到受到它的影响，才开始重视起来。

现在，全世界获得CISSP（Certified Information Systems Security Professionals，国际认证信息系统安全专家）认证的IT安全人员已经达到61 000人（www.isc2.org），而且安全公司也如雨后春笋般涌现出来。当今的安全技术涵盖了从认证和授权到防火墙和虚拟专用网络（VPN）等诸多领域。解决安全问题的方法有很多，多到考虑备选方案都能让人头疼。而现在术语“黑客”已经成为日常用语的一部分，就像每天头条新闻中定义的那样。世界（和犯罪分子）已经发生了翻天覆地的变化。

那么这一切对按下计算机电源按钮时就被推入危险的网络世界的你我、家庭（或最终）用户，或IT（或安全）专业人员来说意味着什么呢？答案是，一切。数字世界里散布着各种稍加触碰就会爆炸甚至会自动引爆的地雷。考虑考虑以下这些简单情景吧。

- ✓ 如果没有正确地配置防火墙就直接将自己的计算机连接到互联网，不等比萨饼送上门，也就是不到30分钟，就可能被黑客攻陷。
- ✓ 打开来自家庭成员、朋友或同事的电子邮件附件可能会在系统中安装后门，使黑客能够任意地访问自己的计算机。
- ✓ 通过互联网消息（IM）程序下载和执行文件可能会使自己原来的桌面变成疾病控制中心的高危区，满是名字稀奇古怪的病毒。
- ✓ 浏览无害（或可信）的网站可能彻底破坏计算机，让黑客可以查看敏感文件，甚至是删除它们。

相信我，在信息高速路上被黑客“打劫”的可能性非常大。

经常有人问我：“对网络恐怖主义恐惧、不确定和怀疑是否合理？网络恐怖分

子是否像新时代预言家所说的那样，能真正影响我们的计算机系统和公共基础设施？”我的答案就是：“确实，是的。”发生数字珍珠港事件的可能性要比很多人想象的更大。像基地组织这样的恐怖组织几乎每周都会被搜查，而当计算机被发现时，它们的硬盘里满是网络黑客攻击计划、美国基础设施蓝图和攻击美国计算机和基础设施目标的指令。

大家相信能源委员会给出的美国史上最大停电事故的报告吗？那次发生在2003年8月14日的停电事故，使得美国五分之一的人口（约5000万人）停电逾12个小时。大家相信那只是未修剪的树木和控制措施不力导致的吗？如果相信奥卡姆剃刀（Occam's Razor）原理，那么好的，最简单的解释通常就是正确的解释，不过请记住：这次停电事故正好发生在微软冲击波蠕虫爆发的三天之后，该蠕虫是互联网上释出的最恶毒的计算机蠕虫之一。巧合？也许吧。

有些人可能还会质疑，说：“那好，如果威胁如此真实，为什么还没发生过什么糟糕的事情呢？”我的回应很简单：“如果我在2001年9月10日跟你说，不久之后会有人劫持商用飞机当做炸弹，在5小时内杀死3000多人，你会相信我吗？”我理解大家的质疑，而且大家也应该有所质疑，不过在发生不测之前，我们希望得到大家的信任，希望大家有信心。相信我们知道真相，相信我们知道什么是可能的，相信我们知道敌人的想法。我想我们至少都认同这样一点，那就是我们不能让他们得逞。

每时每刻，都会有政府团体、有组织的犯罪团伙和黑客团体转动房屋的门把手，看看有没有未上锁的大门。他们会弄响窗户，四处转悠，找寻可供他们入室的机会、漏洞或途径。难道大家要引狼入室？难道大家会坐视不理，看着坏人洗劫自己的财物，利用自己的设施，亵渎自己的避风港？还是说大家要武装自己，教育自己，防止他们取胜？这些问题的回答最终取决于大家现在的行动。

不要绝望，希望尚在人间。提高安全性更多的是一种心态。安全如同健身。如果不定期锻炼，健身就不会成为生活方式的一部分。如果不是生活方式的一部分，那么很快就会被抛之脑后，避之不及。也就是说，身体不会健康。安全问题同样如此。如果没有认识到安全是一个过程而不是目标，就永远不可能将其列为例行职责，那么，它很快就会被抛之脑后，避之不及。如果对安全避之不及的话，最终会反受其害的。

学习是给自己最好的礼物。我们不知道的事物可能不会有致命的危害，但它们很可能严重影响我们或我们关心的人。知道自己不知道什么是真正的关键。填补知识空缺对预防那些重大的攻击来说是至关重要的。本书就能为大家填补这些空缺。凯文非常不错，他把针对Windows、Novell和Linux的黑客方法论，以及与物理安全、社会工程学和恶意软件这种很少被提及的主题有关的有价值的独特材料展示给了

大家。本书涵盖各种与安全相关的主题，这些主题可以帮助大家更为彻底地理解黑客们的想法以及他们的行为方式，并最终成为大家在未来可以免遭攻击的唯一保障。仔细阅读，从中学习，并在自己可以实践的领域去实践书中的知识吧。

没错，数字战场是非常真实的。它既没有开头，也没有结尾，还没有边界，更没有规则可言。阅读本书，学习书中知识，用其武装自己，否则我们可能会输掉这场数字大战。

Stuart McClure是畅销书*Hacking Exposed*系列（McGraw-Hill出版）的主创人与合著者，也是McAfee旗下公司Foundstone的创始人、总裁兼首席技术官。可以通过他的电子邮箱stu@foundstone.com与他联系。

妈妈，这本书献给您。您在顽强地同癌魔做着斗争，从未想到您给我带来了多大的灵感。我深深地爱您，想念您。

前　言

欢迎阅读《黑客达人迷》。本书以平实的日常用语简要介绍了计算机黑客的技巧和技术，利用它们，可以评估信息系统的安全性，找出重要的安全漏洞，并在黑客犯罪分子和恶意用户利用这些漏洞前进行修复。这种黑客攻击是专业、公开而且合法的安全测试，我在全书中都会称其为*道德黑客攻击*（ethical hacking）。

计算机和网络安全是个复杂多变的主题。大家必须登高望远，才能确保自己的信息得到保护，不受坏人侵扰。这就是我在本书中介绍的工具和技术能派上用场的地方。

大家可以实施这里介绍的所有安全技术，以及其他可以运用的最佳做法，这样大家的系统可能就安全了，就如你所知。不过，只有了解了恶意攻击者的想法，运用这种了解，使用合适工具从恶意攻击者的角度对系统进行评估，大家才能真正明白自己的信息到底有多安全。

道德黑客攻击融合了正式且有条不紊的渗透测试、白帽黑客攻击和漏洞测试，对找出安全漏洞并确保信息系统始终处于真正安全的状态来说是必需的。本书为大家提供了成功实施道德黑客攻击计划所需的知识，还介绍了可以用来防止外部黑客和恶意用户影响业务的对策。

读者对象

声明：如果利用书中信息进行黑客攻击或未经授权恶意侵入计算机系统，一切责任自负。我以及其他与本书相关的人员，都不会为利用本书介绍的方法和工具进行非文明或犯罪的行为承担任何责任。本书的意图仅限于让IT和信息安全专业人员在得到授权的情况下测试（自有系统或客户系统的）信息安全。

好了，现在题外话扯完了，言归正传！本书面向网络管理员、信息安全经理、安全顾问、安全审计人员、合规经理，或那些有兴趣更多地了解计算机系统正规测试以及IT运营从而让系统更安全的人。

作为在执行周密信息安全评估的道德黑客，大家可以检测并指出其他情况下可能被忽视的安全漏洞。如果是在自己的系统上执行这些测试，那么在测试中发现的数据将有助于说服管理层，证明信息安全真是应该认真对待的业务问题。如果是在为客户执行这些测试，将有助于在坏人有机会利用安全漏洞之前修补它们。

本书提供的信息可以帮助大家在这场安全游戏中占据先机，让大家享受帮助组织和客户防止信息受危害所赢得的声誉和荣耀。

关于本书

本书是通过攻击系统以提高安全性的参考指南。这些道德黑客攻击技术都基于计算机系统渗透测试、漏洞测试和信息安全最佳做法中各种成文和不成文的规则。本书涵盖了各种内容，从制订黑客攻击计划，到对系统进行测试，再到修复漏洞，直至维持长期的道德黑客攻击计划。实际上，对很多网络、操作系统和应用而言，可能存在几千种黑客攻击。我要介绍的是多种平台和系统中的主要攻击。不管是需要评估小型家庭办公室网络，还是要评估中等规模的企业网络，抑或是为大型企业系统进行评估，本书都能为大家提供所需的信息。

如何利用本书

本书具有以下特性。

- ✓ 多种技术上的和非技术的黑客攻击，及其详细方法；
- ✓ 来自知名信息安全专家的信息安全测试案例研究；
- ✓ 应对黑客攻击的具体保护对策。

在开始攻击自己的系统之前，要熟悉第一部分中介绍的信息，让自己对这些任务成竹在胸。“如果不做计划，那就等着失败”（if you fail to plan, you plan to fail），这在道德黑客攻击过程中特别正确。如果大家想要取得成功，就必须获得授权，并且制订可靠的测试计划。

请不要将这些资料用于不文明或非法的黑客攻击，不要依靠这些内容让自己实现从脚本小子到大黑客的飞跃。本书只是为了让大家了解以文明且合法的方式对自己或客户的系统进行黑客攻击所需的知识，以增强信息安全。

不需要阅读的内容

根据自己的计算机和网络配置的不同，大家可以跳过某些章节。例如，如果大家没有使用Linux系统或无线网络，那么就可以跳过相关章节。

傻瓜假设

我在这里对你们这些有抱负的安全专业人员作出了一些假设：

- ✓ 熟悉与计算机安全、网络安全和信息安全相关的基本概念和术语；
- ✓ 对黑客和恶意用户的行为有基本的了解；
- ✓ 可以访问使用这些技术的计算机和网络；
- ✓ 可以访问互联网，获取用于道德黑客攻击过程的各种工具；
- ✓ 有权执行本书中描述的道德黑客技术。

本书结构

本书分为七个部分，所以大家可以按照自己的需要跳过某个部分直接阅读其他部分。每一章都提供了可用于道德黑客攻击过程的可行方法，包括可使用工具的清单和来源，以及互联网上的资源。

第一部分：打下道德黑客攻击的基础

本部分涵盖了道德黑客攻击的基础知识。首先概述了道德黑客攻击的价值，以及在道德黑客攻击过程中该做和不该做的事。接着带大家深入了解恶意心态，并告诉大家如何计划自己的道德黑客攻击测试。最后，本部分介绍了道德黑客攻击的步骤，其中包括如何选择合适的工具。

第二部分：发动道德黑客攻击

本部分开启了道德黑客攻击的过程。首先介绍了数种广泛使用的知名黑客攻击，包括社会工程学攻击和破解密码，作为这场道德黑客攻击大戏的开始。接着介绍了信息安全中的人员要素和物理安全因素，这二者可能是信息安全计划中最脆弱的环节。在阅读这些主题之后，大家将了解对系统执行常见的一般性黑客攻击所需要的奇技赢巧，以及保障信息系统安全的具体对策。

第三部分：攻击网络

从较大的网络开始，本部分介绍了为系统测试各种知名网络基础设施漏洞的方法。从TCP/IP协议组的弱点，到无线网络的不安全性，大家可以学习如何借助特定手段和有缺陷网络通信去攻陷网络，并了解避免自己受其危害的对策。本部分还包括一些有关网络黑客攻击的案例研究。

第四部分：攻击操作系统

几乎所有的操作系统都具有黑客经常利用的知名漏洞。本部分介绍了如何对三种广泛使用的操作系统（Windows、Linux和NetWare）进行黑客攻击。这些黑客攻击方法包括对操作系统进行漏洞扫描并对特定主机进行枚举，从而获得详细的信息。本部分还介绍了如果利用这些操作系统中的知名漏洞进行攻击和远程攻占系统，以及让操作系统更加安全的具体对策。本部分还含有操作系统黑客攻击的案例研究。

第五部分：攻击应用程序

如今应用程序的安全在信息安全领域也越来越不可小视了。直接瞄准各种应用的攻击不断增多，这些攻击往往能绕过防火墙、入侵监测系统和杀毒软件。本部分讨论了对特定应用和数据库（包括电子邮件系统、即时消息系统、IP电话系统和存储系统）的黑客攻击，并介绍了让系统可以更加安全的实用对策。

针对Web应用的攻击是特别常见的网络攻击。几乎所有防火墙都允许Web流量进出网络，所以大多数攻击是针对几乎任何人都可以下载的数百万Web应用展开的。本部分还介绍了Web应用黑客攻击相应对策，以及一些现实安全测试中的应用程序黑客攻击案例研究。

第六部分：道德黑客攻击的结果

在执行了道德黑客攻击之后，应该如何处理收集到的数据？是束之高阁还是四处炫耀？该如何往前推进？本部分就回答了这些问题，并介绍了更多内容。从制订要提交给高管的报告，到修复自己发现的安全漏洞，再到为自己继续进行的道德黑客测试制定一套程序，本部分将整个道德黑客攻击过程结成了一个完整的循环。这些信息不仅能确保大家的精力和时间得其所用，而且可以证明信息安全是依靠计算机和信息技术的企业取得成功的基本要素。

第七部分：三个十项

本部分包含了一些有助于道德黑客攻击计划取得成功的提示。大家会了解到如何让自己的道德黑客攻击计划得到高管的支持，以使自己可以行动起来，保护自己的系统。本部分还介绍了大家必须避免的十大道德黑客攻击错误。

本部分还包含了附录，附录中提供了道德黑客工具和资源参考清单。大家可以在本书在线小抄（www.dummies.com/cheatsheet/hacking）的附录中找到这些链接。

本书中使用的图标

本图标指代有趣但对理解正讨论的主题来说不太重要的技术信息。

本图标指代值得记住的信息。

本图标指代可能对道德黑客攻击测试造成负面影响的信息，所以请仔细阅读！

本图标指代有助于突出或澄清要点的建议。

作者寄语

对外部黑客和内部不法人员的行为方式以及该如何对系统进行测试了解得越多，就越能更好地保障计算机系统的安全。本书提供了为自己的组织和客户制订并维护成功道德黑客攻击计划所需的基础知识。

要记住，道德黑客的高层级概念不会像自己要防范的具体信息安全漏洞那样经常变化。道德黑客攻击是这个不断变化的领域中一门恒久不变的艺术和科学。大家必须了解最新的硬件和软件技术，以及日复一日、年复一年不断出现的各种新漏洞。没有一种一劳永逸的最佳攻击方法，所以要不断更新自己所掌握的信息。（道德）黑客攻击，其乐无穷！

致　　谢

首先，我想感谢艾米、加勒特和玛丽·林在我编著本书时为我提供的支持。你们都是最棒的！我想感谢威立的梅洛迪·莱恩，她是本书第一版的策划编辑，很久以前就与我联系，讨论本书的想法，并给了我这个大好机会。我还想感谢新的策划编辑艾米·范德雷，她接手了这个项目，并为我提供了修订本书并令我为之骄傲的机会。

我想要感谢项目编辑琼·纳尔逊，再次与你合作是件再愉快不过的事，你又为本书增加了不少价值。我还要感谢文字编辑布赖恩·沃尔斯，是他让我精力集中，并保证行文顺畅。还有，十分感谢我的技术编辑、业务伙伴、朋友，也是*Hacking Wireless Networks For Dummies*一书的合著者，彼得·T.戴维斯。我很荣幸能与你再次合作，并非常感谢你的宝贵反馈。你犀利的眼光真的时刻督促着我，使我慎之又慎。

我要感谢艾拉·温克勒和杰克·怀尔斯热情回应我进行案例研究的请求，还要感谢约书亚·赖特和奇普·安德鲁斯为本书贡献了新的案例研究材料。你们为本书贡献了一些很有价值的内容。

非常感激曾在惠普应用安全中心工作的乔·耶格尔，Acunetix的罗伯特·艾贝拉，AirMagnet的关嘉赐，Elcomsoft的弗拉基米尔·卡塔洛夫，Karalon的托尼·海伍德，曾在GFI Software工作的维多利亚·马斯卡特·英格罗特，Northwest Performance Software的柯克·托马斯，Mythicsoft的戴维·维斯特，N-Stalker的蒂亚戈·扎尼诺蒂，Port80 Software的麦克·安德鲁斯和克里斯·内佩斯，TamoSoft的迈克尔·伯格，Amenaza Technologies的特里·英戈尔兹比，以及Identity Finder的艾米特·戈亚尔和弗恩·爱迪生积极回应我的请求，也非常感激我在这里忘了提及的人们。

特别感谢Queensrÿche乐队、Rush乐队和Triumph乐队，感谢你们充满活力的乐曲和鼓舞人心的歌词，感谢你们的音乐伴我度过了编著这本新书的时光。没有你们，我可能都不想去做了！再次感谢尼尔·布尔茨的离经叛道，告诉我在美国和全世界发生着什么。你激励了我这个创业家、小型企业业主和自由意志论者。你道出了真

谛——接着来吧！

再次感谢布赖恩·特蕾西对我在如何做一个更好的人方面不可估量的洞见和指导。不管在为人还是处世方面，你都帮助了我。

最后，我还要对与我这个“杂牌”顾问签约的客户表示诚挚的谢意，感谢你们长期以来与我合作。要不是你们愿意打破“必须签约大公司”的思维定势并持续支持我，我就不会取得今天的成果。非常感谢你们。

目　录