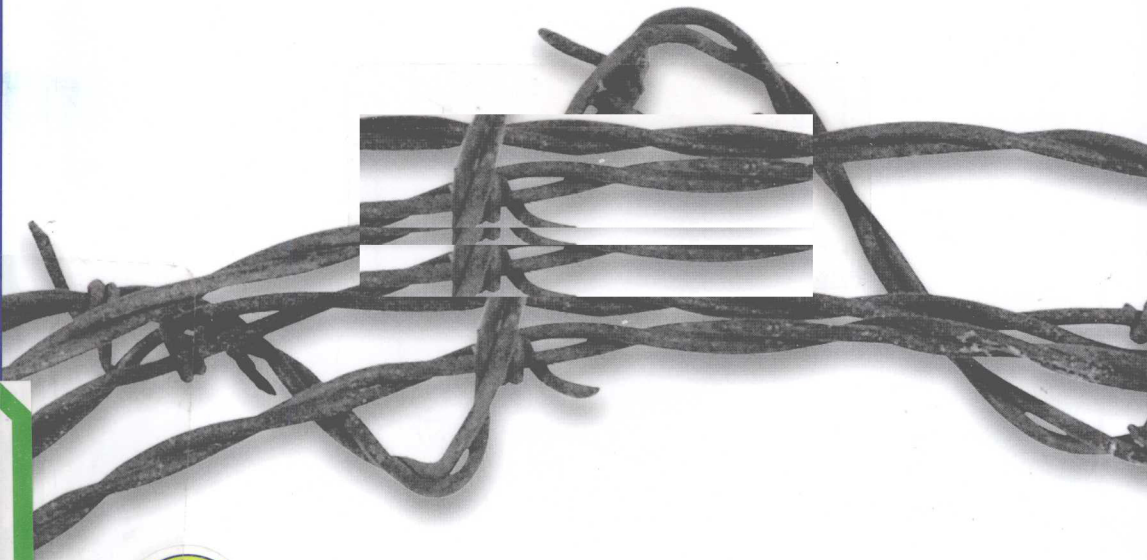
网络安全 HACKS™

第二版

保护隐私的技巧与工具

NETWORK SECURITY HACKS



中国电力出版社 CHINA ELECTRIC POWER PRESS

O'REILLY®
中国电力出版社
HACKS SERIES™

Andrew Lockhart 著
陈新 译

网络安全 HACKS™

第二版

——保护隐私的技巧与工具

Andrew Lockhart 著

陈新 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

网络安全HACKS：第二版 /（美）洛克哈特（Lockhart, A.）著；陈新译.
—北京：中国电力出版社，2009
书名原文：Network Security Hacks™, Second Edition
ISBN 978-7-5083-9279-0

I. 网… II. ①洛… ②陈… III. ①计算机网络－安全技术 ②关系数据库－数据库管理系统－程序设计 IV. TP393.08 TP311.138

中国版本图书馆CIP数据核字（2009）第138371号

北京市版权局著作权合同登记
图字：01-2009-7870号

书　　名/ 网络安全HACKS（第二版）
书　　号/ ISBN 978-7-5083-9279-0
责任编辑/ 胡顺增
封面设计/ Karen Montgomery，张健
出版发行/ 中国电力出版社（www.infopower.com.cn）
地　　址/ 北京三里河路6号（邮政编码100044）
经　　销/ 全国新华书店
印　　刷/ 汇鑫印务有限公司
开　　本/ 787毫米×1092毫米　18开本　26印张　480千字
版　　次/ 2010年3月第1版　2010年3月第1次印刷
印　　数/ 0001－4000册
定　　价/ 48.00元（册）

O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc. 授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的 *The Whole Internet User's Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc. 一直处于 Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得 O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在则编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以O'Reilly Media, Inc. 知道市场上真正需要什么图书。

目录

荣誉

关于作者

Andrew Lockhart 原来居住在美国南卡罗莱纳州，现在居住于美国科罗拉多州北部。Andrew 在那里学习了如何审计反汇编后的二进文件，并努力防止由于天气寒冷而被冻死。他拥有科罗拉多州立大学计算机系的理学学士学位，并担任该州某些小型公司的安全顾问。现在当不写作的时候，他在 Network Chemistry 公司担当资深安全分析员，该公司是无线安全解决方案最主要的提供商。Andrew 还是无线漏洞及其应用项目（*http://www.wirelessve.org*）的编辑委员会成员之一，并经常为他们刊登在 Network-World 上的无线安全专栏（*http://www.networkworld.com/topics/wireless-security.html*）出力。在业余时间里，他为一个名为 Snort-Wireless（*http://snort-wireless.org*）的项目组工作。该项目组主要研究如何为流行的开源 IDS Snort 增加无线入侵检测功能。

贡献者

下面人员对本书贡献了他们的技术和灵感：

- Oktay Altunergil是Free Linux CD 项目组（*http://www.freelinuxcd.org*）的创始人和Turk-PHP.com（一个土耳其PHP门户网站）的维护人员之一。另外，他的专职工作是担任 Unix 系统管理员和 PHP 程序员。
- Michael D. (Mick) Bauer（*http://mick.wiremonkeys.org*）是 *Linux*

Journal "Paranoid Penguin" 安全栏目的专栏作者。此外，他白天主要的工作是研究如何防止陌生人对银行计算机网络的攻击。

- Schuyler Erle（*http://nocat.net*）是一个自由软件开发者和激进主义分子。他对绘图学、无线网络、社会与政治对软件的影响和语义网感兴趣。同时，Schuyler还是NoCatAuth的主要开发人员，NoCatAuth是一个具有领导地位的开源无线门户网站。

- Bob Fleck（*http://www.securesoftware.com*）是Secure Software公司安全服务的主管。他从事于安全的开发环境和无线网络安全领域的研究，并且他也是《802.11安全手册》（由O'Reilly出版）的合著者。可以在*http://bluetooth.shmoo.com*找到他最近在蓝牙安全方面的研究。

- Rob Flickenger（*http://nocat.net*）是O'Reilly的Hacks系列图书的作者和编辑之一。他现在从事于多个项目并推动无线网络社区的建设。

- Preston Gralla是30多本计算机与因特网著作的作者，这些书被翻译成15种语言，其中包括《Windows XP Hacks》（由O'Reilly出版）、《Internet Annoyances》（由O'Reilly出版）、《Windows XP Power Hound》（由Pogue出版社出版）等。他从PC时代开始就撰写技术文章，Preston曾经是多个全国性的报纸、杂志和网站的编辑，他是《PC Week》的初创编辑之一，在《PC/Computing》杂志先后担当过初创编辑、编辑和编辑部主任，并且担当过ZDNet/CNet的执行编辑。Preston为大量杂志撰写过文章，其中包括*PC Magazine*、*Computerworld*、*CIO Magazine*、*Computer Shopper*、*Los Angeles Times*、*USA Today*和*Dallas Morning News*（担任技术专栏作家）等。他曾经是ZDNet/CNet的技术专栏作家，现在是TechTarget.com网站的技术专栏作家。他关于技术的评论被国家公共电台评为"All Things Considered"，并获得计算机出版协会授予的计算机出版物最佳奖。在他的校订下，*PC/Computing*入围了全国杂志大奖General Excellence类的决赛。Preston还是O'Reilly公司的WindowsDevCenter.com网站编辑。他和他的妻子及两个孩子住在马萨诸塞州Cambridge市——尽管他的女儿刚刚离开这个家去上大学去了。除了写书、文章和专栏以外，他还经常游泳、打网球、去看歌剧，有时还沉思于挂在他办公室墙上的公羊的头骨。

- Michael Lucas（*http://www.blackhelicopters.org/~mwlucas/*）和他的妻子Liz及很多啮齿动物、鱼住在密歇根州底特律市的一个神出鬼没的

地方。他是一个宠物争论者，同时也是图书馆管理员和安全顾问。他现在Great Lakes科技集团担任网络工程师和系统管理员。他是《Absolute BSD》、《Absolute OpenBSD》和《Cisco Routers》三本书的作者。现在准备写一本关于NetBSD方面的书。

- Matt Messier（*http://www.securesoftware.com*）是Secure Software公司的工程主管，并且是一个拥有近20年编程经验的安全权威。他还是O'Reilly出版的《Secure Programming Cookbook for C》和《C++ and Network Security with OpenSSL》这两本书的合著者。Matt还合著编写了《Safe C String Library (SafeStr), XXL, RATS, and EGADS》。

- Ivan Ristic（*http://www.modsecurity.org*）是Web安全专家，他还是`mod_security`的作者，这是一种用于Web应用的开源入侵检测和预防的引擎。他是OASIS网页应用程序安全技术委员会的成员，他在那里从事于网页应用程序保护的标准制定。

- Hans Schefske是myITforum.com（*http://www.myitforum.com*）网站的专栏作家。他有8年多工程与设计微软的基于client/server网络解决方案的架构与实现的经验。他在IT工业担当了很多项目的顾问和领导，他为例如Nabisco、Prudential、AIG、Simpson、Thatcher and Bartlett、Novartis和Hoffman LaRoche Pharmaceuticals这样的大型企业级公司提供在设计与实现其基础设施领域的专家技术经验。在2003年，由于Hans杰出的技术技能和主动地与大家分享知识，Hans获得了微软存储管理服务（SMS）方面最有价值专家（MVP）奖。作为myITforum.com网站的技术作家，他为IT职业人员和管理员提供了技术信息、工具、脚本和实用工具，以便帮助他们更好地管理基于微软的解决方案。Hans现在在佐治亚州亚特兰大市的一家大型电信公司担当资深Active Diretory和SMS的顾问。

- Rod Trent是myITforum.com（*http://www.myitforum.com*）网站的经理，他是微软SMS方面的首席专家。他有超过18年的从事IT业方面经验，其中8年他专注于研究SMS。他是《Microsoft SMS Installer》、《Admin911:SMS》和《Windows 2000 IIS 5.0:A Beginner's Guide》（都是由McGraw-Hill出版社出版）三本书的作者，另外还撰写了上千篇技术专题文章。myITforum.com是第三方SMS支持的中心单元，同时也是一个IT职业人士和社区众所周知的在线聚集地。Rod每年至少要在各

种会议上发表三次演讲，并且担当NetImpress有限公司（*http://www.netimpress.com*）的负责人。

- Mitch Tulloch（*http://www.mitit.com*）是MTIT公司（该公司位于加拿大的Winnipeg州，是一个IT内容开发公司）的董事长。在1998年创建自己的公司之前，Mitch在Productivity Point International公司担当微软认证训练员。在Windows管理、网络及安全方面，Mitch是一个广泛公认的专家。他在配置Windows平台、产品和解决方案方面还获得了微软最有价值专家（MVP）奖。Mitch现在还是Jones国际大学（JIU）的教授，在那里他教授信息安全管理方面的研究生课程，该课程是他和他的妻子Ingrid Tulloch一起为JIU大学的MBA开发的。Mitch是14本书的作者，其中包括《Windows Server Hacks》（由O'Reilly出版）、《Windows Server 2003 in a Nutshell》（由O'Reilly出版）、《the Microsoft Encyclopedia of Networking》（由微软出版社出版）、《the Microsoft Encyclopedia of Security》（由微软出版社出版）、《IIS 6 Administration》（由Osborne/McGraw-Hill公司出版）等。Mitch还为例如《NetworkWorld》、《Microsoft Certified Professional Magazine》等业内杂志撰写特稿，并经常为O'Reilly的一些网站（WindowsDevCenter.com、ITWorld.com和WindowsNetworking.com）贡献文章。Mitch的文章也被广泛地在其他IT网站（例如Computerworld.com、Smallbusiness.com，甚至是CNN.com）联合发表。

- John Viega（*http://www.securesoftware.com*）是Secure Software公司的首席技术官和创始人。他也是许多软件安全书籍的合著者，其中包括《Secure Programming Cookbook for C and C++》（由O'Reilly出版）和《Building Secure Software》（由Addison-Wesley出版）。此外，John还负责大量软件安全工具，他还是Mailman（一个GNU邮件列表管理器）的发明者。

致谢

我再一次必须感谢Karen（a.k.a. DJ Jackalope for Defcon attendees），感谢她一直以来的支持和鼓励，感谢她忍受长期以来的辛劳。

我还要感谢Brian Sawyer，感谢他在本书编写的整个过程中的耐心帮助。同时也要感谢O'Reilly公司的所有其他优秀的工作者，是他们的努力使得这本书变为切实可能。感谢John Hoopes，他为这个版本在技术上进行了复查，John的建议有助于使得本书变得更好。

最后要感谢的是我的父母，感谢他们持续不断地给我鼓励。

前言

在网络安全领域，人们常常会误解黑客这个词的意思。这是可以理解的，因为网络安全专家会使用工具来探测自身网络的稳健性，然而攻击者也可以用这些工具实施对因特网上主机的攻击。系统管理员合法地测试自己的机器，而系统破坏者则试图获得未授权的访问权限。他们在技术上和使用工具方面并没有什么不同，但是他们的意图却完全不同。毕竟，和任何强大的技术一样，没有一个安全工具天生是正义的或恶意的——这完全取决于如何使用该工具。同一个锤头可以用来建造城墙，也可以用来推倒城墙。

“白帽子”黑客和“黑帽子”黑客的区别并不在于他们所使用的工具或技术（甚至是他们帽子的颜色），而是在于他们的意图。这样的区别很微妙，但是却十分重要。白帽子黑客将构建安全的系统作为一项有趣的挑战，并且希望构建的系统的安全性可以彻底通过真实环境下的测试（假定该环境下攻击者拥有所有破坏系统的技术和工具）。黑帽子黑客（更合适的称呼是骇客）学习和白帽子黑客相同的技术，但是对构建系统的人员及他们攻击的服务器并不关心。黑帽子黑客使用自己的技术来破坏这些系统，从而获得自己个人的收益，他们经常破坏被他们渗透的系统。

当然，国际上有一些大胆的依靠技术“抢劫”的人以及一袭黑衣、叼着香烟、挥舞着笔记本的邪恶的计算机天才，他们的故事往往比单纯构建一个健壮网络的工程师的故事受人们欢迎，因此，“hacking”这个词在媒体中享有的声誉比较差。媒体通常将黑客看做是那些闯入系统或用计算机作为武器来发起破坏行为的人。然而那些解决计算机实际问题的人们通常将“hack”这个词看做是快速解决某个问题，或者是一个完成某件事情的巧妙的方法。而黑客