网络与信息安全技术经典丛书

继“黑客大曝光”之后的又一力作

HARDENING Linux 中文版

Bulletproof your systems before you are hacked!

为你的系统构筑坚固的安全堡垒

John H. Terpstra Paul Love Ronald P. Reck Tim Scanlon 著

Series Editor: Roberta Bragg, CISSP, Security+

王建桥 杨晓云 杨涛 译

McGraw Hill Osborne

McGraw Hill

清华大学出版社

网络与信息安全技术经典丛书

Hardening Linux 中文版

[美] John H. Terpstra
Paul Love
Ronald P. Reck
Tim Scanlon 著

王建桥 杨晓云 杨 涛 译

清 华 大 学 出 版 社
北 京

John H. Terpstra , Paul Love , Ronald P. Reck , Tim Scanlon
Hardening Linux
EISBN 0-07-225497-1
Copyright © 2004 by The McGraw-Hill Companies.

Original language published by the McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education (Asia) Co., within the territory of the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版（亚洲）公司授权清华大学出版社在中华人民共和国境内（不包括中国香港、澳门特别行政区和中国台湾）独家出版发行。未经许可之出口，视为违反著作权法，将受法律之制裁。未经出版者预先书面许可，不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号　图字：01-2005-1431

版权所有，翻印必究。举报电话：010-62782989　13501256678　13801310933

本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

北京市版权局著作权合同登记号　图字 01-2005-1431 号

图书在版编目（CIP）数据

Hardening Linux 中文版/（美）托普斯特（Terpstra,J.H.）等著；
王建桥等译. －北京：清华大学出版社，2006.1
书名原文：Hardening Linux
ISBN 7-302-12258-X

Ⅰ. H…　Ⅱ. ①托…　②王…　Ⅲ. Linux 操作系统　Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字（2005）第 152395 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-82896445
组稿编辑：夏非彼
文稿编辑：何武
封面设计：林陶
版式设计：科海
印 刷 者：北京市耀华印刷有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×230　　**印张**：26　　**字数**：568 千字
版　　次：2006 年 2 月第 1 版　2006 年 2 月第 1 次印刷
书　　号：ISBN 7-302-12258-X/TP・7881
印　　数：0 001~3 000
定　　价：48.00 元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：（010）82896445

内 容 提 要

"Hardening" 系列是美国 McGraw-Hill 公司新近推出的又一套信息安全系列丛书，与久负盛名的"黑客大曝光"系列携手，为信息安全界奉献了一道饕餮大餐。

本书是 "Hardening" 系列成员之一，由数位信息安全领域的著名专家编写，通过四段式系统强化教学法，从技术和管理制度两方面，详细介绍 Linux 系统的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入探讨，旨在帮助读者把 Linux 系统建设成信息安全堡垒。

全书共分 4 大部分 16 章，第 1 部分给出降低系统威胁的 7 个关键步骤，是系统阻止入侵的必要措施；第 2 部分则是本书的重中之重，自顶向下系统讲述强化 Linux 系统的具体方法和措施；第 3 部分告诫人们：一劳不能永逸，需要利用各种监控技术持续监控系统，教会读者阅读各种日志文件内容、判断系统受损程度；第 4 部分对信息安全工作的预算制订和审批工作进行讨论，同类书中少见。

本书是 Linux 系统管理员的福音，所有对 Linux 系统安全感兴趣者必备。

序 1

Dave Wreski

信息安防工作的全部内容其实就是寻求一个最佳平衡点：若是决策既正确又合理，就能让不同级别的用户对各自所享有的信息和资源访问级别感到满意；若是决策不正确或正确但不合理，就会给用户在维护有关信息和资源的安全性方面带来诸多不便——如果需要由用户完成的信息安防工作超出了挑选一个好的口令字或定义一条简单的防火墙或过滤器规则，系统管理员就难以指望用户严格遵守这样的信息安防决策。

现在，随时随地都能访问所需信息已是用户的一种普遍预期。随着 Linux 系统的日益流行和越来越多的套装 Linux 发行版本被设计成只要安装完毕就可以执行任意任务，系统管理员开始更加频繁地发现自己身陷一种两难境地：既要赶在几乎无法完成的截止日期前让系统上网运行，又要从一开始就为系统建立起牢固的安全防线以防范来自因特网的各种威胁，防止组织内部和外部的恶意人士窃取他们不应该享有的访问权限。

在严格控制信息的访问权限和妥善保护敏感信息之间求得最佳平衡并不是件简单的事情。现在的 Linux 服务器系统管理员往往还要负责其他有相当难度的日常工作，再让他们抽出时间和精力去调控好每位用户的访问权限，显然是力不从心。Linux 发行版本的供应商也在为怎样才能在不影响系统安全性和性能的前提下向系统管理员提供更多更具吸引力的管理工具而绞尽脑汁。

本书对各种常用 Linux 系统的安全防护工作做了全面细致的讲解，还对系统管理员容易疏忽或犯错的许多细节问题进行了探讨。

本书对与 Linux 系统强化工作有关的技术性问题和管理制度问题做了深入探讨，即使你不是一位信息安全专家，也可以在本书的帮助下逐步地把 Linux 系统打造成坚固的安全堡垒。

本书的各位作者都是信息安全领域的著名专家，他们尽了最大的努力来保证中等水平的读者也能充分掌握 Linux 系统的各种强化技术并学会如何制定和实施一套行之有效的信息安防策略。虽然主流的 Linux 供应商在提高其产品安全性方面已经取得了巨大的进步，但本书对渴望在满足自己的核心业务需求与改善 Linux 系统信息安全性之间求得完美平衡的人来说仍是有着无限价值。

此为试读，需要完整PDF请访问：www.ertongbook.com

如果你想拥有“安全的”Linux 服务器，如果你想在第一时间发现来犯之敌并变被动为主动，或者如果你有志于解决现实世界的各种信息安全问题，这本书（以及包括 LinuxSecurity.com 网站在内的其他宝贵资源）将是你前进道路上必不可少的伴侣。

Dave Wreski
Guardian Digital 公司 首席执行官
Linux Security HOWTO 合著者
EnGarde Secure Linux 项目总指挥

Dave Wreski 在信息技术和信息安全领域从业 10 多年。他在 1999 年初创建了 Guardian Digital 公司，向有兴趣使用开源代码来解决关键业务信息安全问题的企业提供服务，该公司目前已拥有数百家企业级客户。在创建 Guardian Digital 公司之前，Wreski 曾是 UPS Worldwide 公司的一名高级系统设计师，主要负责对该公司数据中心的信息安防体系进行设计和管理。向公众传播开放源代码的信息安防知识和提高 Linux 在企业中的接受程度是 Wreski 最热心的两件事。

序 2

Corey D. Schou

你的系统在顾客最需要它的时候瘫痪了。你刚刚发现有人下载了你的银行资料。你的计算机不知在谁的控制下正在攻击因特网上的其他系统。某医院的生命维持系统刚刚启动了一台不该启动的机器去抢救一位生命垂危的患者。从噩梦中醒来，你全身冷汗！

这些噩梦中的场景（还有比它们更糟糕的）每天都在发生，而其中有相当大的一部分是因为用户和经理不了解应该如何对计算机系统进行安全防护而导致的。他们所犯的都是些相当低级的错误，比如把一个新的计算机系统未加任何安防处理就直接接入了因特网。这等于是把一辆崭新的保时捷跑车停放在市区街道上，但敞着车门、插着车钥匙并把行车执照摆在车座上。

在日常生活里，我们都会不假思索地采取一些基本的预防措施。在你离开住所时，你会把门锁上。当你准备丢弃一些用不着的文件时，如果文件里有你的银行帐号，你会把它们撕得粉碎。当你停放汽车时，你会随手拔下车钥匙带走。对计算机也应该做同样的事。

一旦意识到这些潜在的问题，就应该学会保护自己的系统。无论是对想提高安防能力的初学者，还是想确保能够面面俱到地保护系统的资深管理员，本书都是不可多得的宝贵资源。

安全化的操作系统是计算机系统的第一道信息安全防线。本书的几位作者对 Linux 系统的安全防护技术做了独到的分析和介绍，他们将带领大家把各种 Linux 系统打造成为令人放心的信息安全堡垒。

几位作者深入浅出地阐明了一个道理：在对系统进行安防处理的时候，必须切实做好 5 项最基本的信息安全服务：保密性、可用性、完整性、不可否认性和身份验证。

这几项服务将为传输、存储和处理中的敏感信息提供有效的保护。稍微具体地说，本书的第 2 章将向大家介绍如何通过各种网络访问权限强化技术来保证数据在传输过程中的安全性，第 10 章又进一步对数据通讯过程本身的安全问题做了详细的讨论。对于存储在硬盘或其他介质上的数据，本书在介绍各种数据加密工具的有关章节里对它们的保护措施做了简明扼要的讨论。数据在处理过程中的完整性问题将在本书讨论各种操作系统内核强化技术和软件补丁管理技术的时候得到解决。

本书关于信息安全策略的探讨增加了它的趣味性。信息安全策略是人们为应付意外而提前制定出来的一套正规的信息安全操作流程。如果你们的信息安全策略不够完备，在发现系统已被他人恶意侵入时就会因为仓促应战而难免手忙脚乱。本书的几位作者已经预见到了这种局面并在书中演示了如何提前采取各种监控技术，如何通过各种日志文件研判系统的受损程度以及如何阅读各种日志文件内容的技巧。

本书的几位作者甚至对信息安全工作的预算制定和审批工作进行了讨论，这在其他同类书籍中难得一见。不客气地讲，绝大多数技术人员都要等到最后关头才会想起还有预算这码事。如果管理层不了解信息安防服务需要多大成本，他们是绝不会支付账单的。本书的几位作者将帮助读者明白这样一个事实：信息安防技术手段只有获得了管理层的肯定和支持才有可能取得成功。即使管理层知道了信息服务的成本，如果他们不明白这个数字的来龙去脉，你将很难让他们心甘情愿地拿出钱来。要是他们真的不肯支付账单，你所预期的技术就不可能得到实施，你绞尽脑汁写出来的信息安防计划书也就只能沦为一纸空文。

在阅读和学习本书的时候，希望大家能随时留心三种信息状态（传输、存储、处理）、五项信息安防服务和三大类防范措施（技术、策略、培训）[1]。

当你们学完本书并能熟练运用所学知识的时候，将确保你们的系统是安全的。千万不要忘记本书的第 3 部分的标题：一劳不能永逸！你们必须把系统上的信息安防工作长期坚持下去，只有这样才能保证为它们打造的信息防线能够与信息攻防技术的最新进展保持同步。应该密切监控系统并定期查看有关日志。为确保制定的信息安防策略能跟上潮流，为确保使用的信息技术能得到有效的保护，你们应该每天抽出一些时间来自学各种信息安防技术。本书可以用我任职的研究中心的座右铭来做为总结：

了解-培训-教育
不学无术者无可就药。

Corey D.Schou 博士
信息学博士导师
计算机信息系统教授
美国国家信息保障技术培训和教育中心 院长
爱达荷州立大学

1 请参阅 V. Maconachy、C. Schou、D. Welch 和 D. J. Ragsdale 等人合著的“A Model for Information Assurance: An Integrated Approach”一文。《第 2 届 IEEE 系统、人、网络信息安防工程年会论文集》（Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop）第 306~310 页；本次会议于 2001 年 6 月 5 日到 6 日举办于纽约州 West Point 市。

前　言

我们生活在一个面向消费者的时代。这个时代的特征之一是消费者们普遍认为任何东西都可以非常方便地买到和丢弃。

就拿计算机来说，它们已经变得与普通商品没什么两样，人们在听到企业老总随口说出“我们需要添置一个新的网络”或“我们去哪儿买一个防火墙”这样的话时也不再认为他们是外行。就在不久前，某公司的办公室经理还曾极其恼怒地公开谴责由他负责购买的服务器“根本不安全，因为已经有人侵入了它的内部并把我们的文件弄得一团糟”。

我们编写本书的目的是为了帮助系统管理员或 IT 人士消除书架上和 Web 网上的各种噪音并为 Linux 环境打造一条坚固的信息安全防线。对系统进行强化更像是一段旅途而不是一个目的地。你们必须循序渐进地采取一系列主动措施才能搞好服务器的强化工作。在系统达到令人满意的安全性、可靠性和完整性之后，还需继续努力才能把这些状态保持下去。不管你使用的是哪一种 Linux 版本，本书所讨论的 Linux 系统强化原则都同样适用。事实上，本书不仅向读者提供了大量的技术性概念和技巧，还对为全面部署一整套行之有效的信息安防策略而必须提前解决或得到认同的各种重要的政治问题和财务预算问题进行了探讨。

信息系统黑客是现代版的保险箱或银行金库窃贼。不可否认，有一些网络黑客卖弄自己本领的目的只是为了寻求刺激，但另外一些网络黑客却是从一开始就怀有不可告人的动机。无数事例告诉我们：所谓的最佳防御措施只有在还没有人学会如何攻击并击破它之前才是有效的。

常备不懈才能高枕无忧，而常备不懈意味着你必须花费一定的人力物力在恶意攻击到来之前准备好种种御敌措施。预警措施以及相应的后续手段是否有效与它们的成本高低并没有必然的联系，在有限的预算内也可以建立足够坚固的信息安全防线。我们希望本书能够成为你抵御那些看不见的敌人（等你真的看见他们就太晚了）的战友，让黑客的进攻徒劳无功本来就是大家应该一起迎接的挑战。

针对 Linux 服务器的恶意攻击活动越来越多，所有其他种类的服务器和桌面平台也面临着同样的问题。绝大多数攻击和入侵活动都是因为人们对自己的网络和网络资源所采取的强化措施不够妥当才有机会得逞。因此，我们的系统强化工作将从采取正确步骤关闭可能存在的漏洞开始，然后通过我们共同的努力在信息系统的四周布下铁幕般的安全网。

经常有人故弄玄虚地说，只有被切断了电源并被浇铸在混凝土里的服务器才是绝对安全的，但不幸的是这种纸上谈兵的解决方案无论是从商业角度还是从组织管理角度看都不具备现实意义。还有一种说法是把服务器与全体用户完全隔离开来也能保证它的安全性，但这种做法也同样不具备可行性。在现实世界里，计算机系统的信息安防和强化工作都必须进入这些系统的实际运行环境里。对一台运行中的服务器进行防护有点类似一边穿越敌人的火力网一边躲避四处乱飞的流弹。在有实际意义的解决方案中，最安全的做法是：在离线状态下对服务器进行防护，等对它的强化工作全部完成之后才把它再次投入使用。

对信息系统进行强化的目的并不仅仅是为了提高安全性，让 Linux 服务器恰到好处地适用于它们的预定任务，同时必须提前做好各项准备工作。要想让 Linux 服务器能够长期保持正常运转，就必须采用一整套全面系统的措施对它进行强化。要知道，新生效的计算机安全法规几乎天天都有，系统管理工作和法律责任也在随之增加。组织机构很可能会因为被人发现垃圾邮件源自它的网络系统而承担法律责任。企业高级管理层在确保其数据完整性和安全性方面所需承担的责任正越来越大。诸如信用卡资料之类的保密信息泄露事件很可能会把同是受害者的企业推送到毁灭的边缘。

我们的 Linux 系统强化工作将从 7 项能帮助读者全面控制自己的 Linux 服务器的前期准备工作开始。随后的各个章节需要你有持之以恒的决心和毅力去学习和利用才能帮助你获得并保持对自己所有网络资源的有效控制权，才能不给信息罪犯留下造成更大破坏的可乘之机。

内容概览

本书从一种在 Linux 世界里尚不多见的立场对充满挑战的信息系统强化工作进行了介绍和探讨。我们假设读者使用的 Linux 服务器产品以及相关的商业化技术支持都是从某个信誉良好的软件公司那里购买到的，而软件供应商已经做好了应该由它们做的一切事情来帮助用户为自己的服务器建立信息安全防线。请记住，给自己的系统打上由软件供应商提供的安防补丁是你们自己的责任，本书将假设软件供应商在提供一个安全的信息系统方面都是一流的专家，尤其是在把它们所提供的各种补丁和升级都已打好的时候。

第 1 章

第 1 章将帮助你检查 Linux 服务器的状况是否适合进行强化。在执行这些步骤之前，应该先问自己：“这个系统是不是值得强化？”如果你的 Linux 系统在强化工作开始之前已被入侵，你应该考虑使用一个令人放心的安装介质来重装系统。

如果在检查结束时没有证据表明服务器已被人侵入或被控制，就说明你的服务器状况良好，可以对它进行强化。

第 2 章

你准备强化的系统迟早要接通电源并运行，再谈论诸如“只有切断电源的计算机才安全”之类的话题就无异于浪费笔墨和时间。但既然是服务器，只保留必要的进程应该不是难事。千万不要以为这是一件小事，这将堵死网络黑客利用种种你根本不需要的服务所潜藏的安防漏洞侵入系统的大门。

第 3 章

进入第 3 章，你的系统应该只向外界提供你认为必要的服务。接下来的任务是让服务器在来自公共因特网的窥探中消失。按照这一章介绍的原则，配置出来的防火墙将会让因特网的潜在入侵者或攻击者难以发现和侵入你的系统。这一章的讨论内容是在系统的内部网络接口值得信任的假设下展开的。至于系统的外部网络接口，无论何时都不要假设它们是可信的。

第 4 章

一套完备的信息安防策略必须把所有可能发生的情况都考虑周全，把所有能够采取的防御措施都用上，不给入侵者留下让他们轻易为害的工具。如果你也认同这个观点，请按第 4 章给出的步骤从 Linux 系统里把不需要的所有软件全都删除，只保留必要的服务。

第 5 章

怀有恶意动机并能利用最新发现的安防漏洞或弱点侵入他人计算机系统的黑客越来越多，身为系统管理员的你必须假设你迟早需要重装系统。本章将帮助大家做好准备，虽然你我都希望这种事永远都不要发生。

第 6 章

系统上的根用户（root）访问权限是入侵者梦寐以求的东西，因为他们知道只有这样才能绕过系统上的种种访问限制机制。防范外来敌人固然重要，但你决不能因此而忽略合法用户也会有意或无意地滥用你对他们的信任而给系统带来灾难。在这一章里，你们将学到如何通过技术手段来保护系统上的重要文件不会被普通用户偷窥和随意访问。利用这一章学到的技术，你们甚至可以把全局可写子目录的安全性提高，只有某个文件的属主才能对它进行写操作。

此为试读，需要完整PDF请访问：www.ertongbook.com

第 7 章

本章将介绍如何通过数据加密技术来保护系统上的敏感信息。按照本章给出的步骤对 Linux 系统进行强化之后，恶意的外来入侵者和好奇的内部用户就算弄到了重要文件，也无法读出里面的敏感数据。你们还将学到如何保护系统中的用户身份信息和敏感的财务记录。对加密文件系统的充分利用可以给你的事业增加更多发展的机会。

第 8 章

对计算机系统的身份验证机制和系统访问控制功能的理解可以帮助你们提供更好的信息保护锁和改善对非授权系统访问活动的监控工作。本章对 Linux 系统中具体负责核心身份验证和访问控制工作的可插入式身份验证模块（pluggable authentication module，PAM）和命名服务切换器（name service switcher，NSS）做了重点介绍。

第 9 章

UNIX 系统允许进程在运行时把文件系统的某个分支当做它的根目录，让它看上去就好像是整个机器。此时，该进程将运行在由整个文件系统的一部分所构成的封闭区域里，即使某位用户碰巧侵入了这个受保护的进程并造成了损失，其范围也仅限于这个区域而不会波及到整个机器。这意味着我们可以设法把黑客入侵所造成的损失限制在只与被攻破的服务有关的部分而帮助未被黑客攻破的服务继续保持正常运转。本章在讨论中涉及到大量的细节问题，这些细节将帮助大家在系统集成方面获得坚实的立足点。

第 10 章

内部专用网络和外部公用网络上的数据通讯是必须讨论的话题。本章将帮助大家对所有必须穿越一段公共网络才能到达目的地的私密数据进行安全防护。你们将要学习如何运用各种安全的数据通讯技巧和如何使用各种安全的通讯工具。

第 11 章

这一章将介绍一些系统监控工具的用途和用法，还将介绍几种可以用来证明 Linux 系统是否存在安防弱点的穿刺测试工具。

第 12 章

在本书的各相关章节里，经常会看到各种日志或其他关键信息。现在，开始学习如何配置一个中央日志服务器并给它分配自动化的日志文件扫描和报警工具。不给信息罪犯以任何可乘之机；当你这里响起警报的时候，入侵者也许还不知道他的一举一动早已在你的监视之下了。

第 13 章

你也许认为给系统打补丁和进行升级是一件再容易不过的事情，但事实并非如此。这一章将帮助大家做好这项最占用时间和精力、责任也最重大的信息安防工作。经验丰富的专家都会在给系统打补丁和进行软件升级的前后把系统的配置变化情况记录在案并妥善保管，这种良好的习惯将给今后的工作带来极大的方便。千万不要因为本章内容看起来很浅显而让自己与这些好习惯带来的好处失之交臂。我们相信，即便是最有经验的信息安全老手也可以从这一章里学到些新东西。

第 14 章

怀疑自己生病时，除了去医院检查还有什么其他的办法？本章向那些总是怀疑自己的系统在信息安全方面出问题的读者提供了一个可以了解实情的办法——让系统进行自我监控。系统自我监控工具可以让人们随时了解系统的完整性是否完好无损。本章对这类工具进行了介绍。

第 15 章

本章将帮助大家寻求企业管理层对 Linux 系统强化工作的支持。这一章介绍的窍门和工具将帮助你完成对信息安防投资回报的分析和计算工作，这些数字是管理层乐于见到的。

第 16 章

最后，服务器得到了保护，管理层也为你的信息安防工作“埋了单”。为了把管理层和用户对你的支持保持下去，还需要学习如何设定目标和如何把信息安防策略和实践长久地坚持下去。

书中使用的 Linux 产品名简称

在这本书里，我们将使用以下缩写来代表 SUSE 公司、Red Hat 公司的各种 Linux 产品以及美国国家安全局（National Security Agency，NSA）的 Security-enhanced Linux 项目所开发的 Linux 内核。

- Security-enhanced Linux 将被简称为 SELinux。
- SUSE LINUX Enterprise Server 将被缩写为 SLES，书中会经常出现 SLES8、SLES9 和 SLES8/9 这样的缩写形式。SUSE 公司的 Linux 系列产品主要包括以下几种：

- SUSE LINUX 9.1 Personal（个人版）
- SUSE LINUX 9.1 Professional（专业版）
- SUSE LINUX Desktop（桌面版）
- SUSE LINUX Enterprise Server 8（企业级服务器第 8 版）
- SUSE LINUX Enterprise Server 9（企业级服务器第 9 版）
- SUSE LINUX Openexchange Server 4.1（网络级服务器第 4.1 版）

◈ Red Hat 公司的 Linux 产品也将以各自的缩写形式出现在书中。Red Hat Enterprise Linux Server 3.0 将被缩写为 RHEL，而 Red Hat Enterprise Linux Advanced Server 3.0 将被缩写为 RHAS。Red Hat 公司的 Linux 系列产品主要包括以下几种：

- Red Hat Linux 9
- Red Hat Fedora Core 1
- Red Hat Fedora Core 2
- Red Hat Enterprise Linux Server 3.0（企业级服务器第 3.0 版）
- Red Hat Enterprise Linux Advanced Server 3.0（高级企业级服务器第 3.0 版）

作为本书的作者，我们要特别感谢 Red Hat Linux 和 Novell（SUSE 公司的新东家）这两家公司，正是有了它们的通力支持、宝贵意见和慷慨赞助的 Linux 产品，我们才有机会把这本书呈现在读者面前。

关 于 作 者

John H. Terpstra 是 PrimaStasys 公司的总裁兼 CTO，该公司的主要业务是向各类信息技术公司提供人员技术培训，并帮助对方进行业务流程重组以提高其赢利能力。他是 Desktop Linux Consortium（桌面 Linux 论坛）决策委员会的成员之一，Samba Team（Samba 团队，Open Source 组织的重点项目之一）的资深成员，还是开源社区里积极参与各种商业化运作的著名推动者和评论家。他是 Open Source Software Institute（开放源代码学院）顾问团（Advisory Board）的成员之一，曾在 Linux Standard Base（Linux 标准集）、Li18nux（即现在的 OpenI18N.Org）、Linux Professional Institute（Linux 职业学院）等机构工作过，而且还是 Prentice Hall 出版公司出版的畅销书 *The Official Samba-3 HOWTO and Reference Guide* 和 *Samba-3 by Example: Practical Exercises to Successful Deployment* 的作者。

John 曾在 SCO Group（即以前的 Caldera 公司）和 Turbolinux®公司任高级职务。在 1999 年移居美国之前，John 曾创办 Aquasoft Pty Ltd.公司（澳大利亚）并经营该公司达 10 年之久。他拥有澳大利亚 UTS 大学市场营销专业的毕业证书（学分制）和澳大利亚 QUT 学院化学专业的应用科学证书。

Paul Love 持有 CISSP、CISA、CISM、Security+等多项证书，在 IT 行业工作了 15 年。Paul 拥有网络安全专业的科学硕士学位和信息系统专业的学士学位，是 Linux 和 Unix 方面 10 多本畅销书的技术编辑，在“.com”时代还创建过一个相当成功的 Linux 门户网站。Paul 目前在一家大型公用服务提供商就任信息安全经理。

Ronald P. Reck 成长并受教于大底特律地区，他至今仍经常回忆起被他称之为“老家”的那个地方的老朋友和文化氛围。他接受过正规的语法学理论教育，对各种语言以及它们所揭示的人性一直怀有浓厚的兴趣。Ronald 在语言方面的钻研精神和在计算机方面的丰富经验为他提供了很多学习和使用 Perl、XML 等程序设计语言以及运行在*nix 操作系统下的 Semantic Web（语义学 Web）技术的就业机会并因此而受益良多。他对自己为各种难题开发出通用性好、可适性强的开放源代码解决方案的本领充满了自信和自豪。Ronald 目前与他可爱的妻子 Olga 和两只小猫住在华盛顿附近。

Timothy Scanlon 是 IT 界的元老级高手，曾在美国国内和国际上的许多 IT 和信息安全项目中大显身手。他曾以项目甲方代表和项目乙方代表的身份为很多《财富》500 强公司以及 UUNet 等新兴公司工作过。在他担任乙方代表的项目中，以各种 R&D 中心、部门和

分支机构的个体承包商身份开展工作的。他的职业兴趣包括数据加密、应用软件和体系结构设计、信息安防、游戏博奕理论、系统仿真和模型化等。他认为如今的 Linux 操作系统已经从几张软盘就可以容纳其全部内容的时代向前迈出了很大的一步。

关于本书的其他撰稿人

Mike Shema 是 NT Objectives 公司的研发总监，重点负责对 Web 应用程序的信息安全水平做出评估并提供相应的风险应对策略。在他以前做咨询师的工作经历中，Mike 曾从事过网络穿刺测试、Web 应用程序安全性评估和无线网络安全性审计等工作。他在 Web 应用程序的信息安防方面有着丰富的经验，是 *Hacking Exposed: Web Applications* 一书的合著者和 *Hack Notes: Web Application Security* 的作者。他还是 *The Anti-Hacker Toolkit* 一书的合著者，该书目前已出版到第 2 版了。他时不时地会抽出时间玩角色扮演游戏或棋类游戏。

Paul Robertson 在信息技术和安全领域已经工作了 20 多年；他特别引以为豪的两件事是在美国陆军服役期间为白宫站过岗和帮助 USA Today（今日美国报）在因特网上建立 Web 站点。Paul 目前就职于 TruSecure®公司，主要工作是帮助该公司的几百家企业级客户进行风险管理。他积极发起建立了 www.personalfirewallday.org 网站，同时还是 Firewall-Wizards 邮件表的版主。

关于本书的技术编辑

Makan Pourzandi 于 1995 年从法国里昂大学获得了并行与分布式计算专业的博士学位。他就职于 Ericsson Research Canada（爱立信加拿大研究中心）的开放系统实验室（Open Systems Lab Department）。曾在各种专业技术刊物和学术会议上发表 25 篇以上的文章。他在几年前才开始接触 Linux 9，但目前已是好几个开放源代码项目的参与者。他是 Carrier-Grade Linux Server（CGL）2.0 版本中信息安全需求的主创人员，也是为来自 Open Source Development Lab（OSDL，开放源代码开发实验室）的 CGL 3.0 版本起草信息安全需求的工作组成员之一。

关于本系列丛书的主编

Roberta Bragg 居住美国蒙大拿州的 Grain Valley 市，拥有 CISSP、MSCE:Security、MVP、Security+、ETI-Client Server、Certified Technical Trainer、IBM Certified Trainer、DB2-UDB、Citrix Certified Administrator 等多项证书。Roberta 至今已担任 MCP 杂志“Security Advisor”（信息安防顾问）专栏作家达 6 年之久，她是 searchWin2000.com 网站上“Security Expert”（信息安防专家）栏目的主持人之一，由她编写的“Security Watch”（信息安防技术动向）手册有超过 55 000 名的订阅者。Roberta 设计、计划、促成并参加了于 2002 年在美国华盛顿州西雅图市举办的第一届 Windows Security Summit（Windows 信息安防技术高峰会议）。Roberta 还是为期三天的安全化网络构建技术强化短训计划“Windows Security Academy”（Windows 信息安防技术学院）的发起人和授课老师。她曾任教于 SANS 和 MIS 等安全技术培训机构。微软公司在 2004 年度的 Security Summits 会议上把她评选为 IT 职场成功人士的典型代表之一。Roberta 称得上是一位信息安防技术的传教士，她经常穿梭于世界各地对有关网络和 Windows 的信息安全问题进行咨询、评估和培训。她是 Ceel Pasternak 和 Linda Thornburg 合写的“Cool Careers for Girls”（女性热门职业）丛书的原型人物之一。Roberta 还是西雅图太平洋大学和 Johnson 县立公共学院的助教，主要负责 Windows 2000 安防体系设计和网络安防体系设计等课程的教学工作。Roberta 是 *MCSE Self-Paced Training Kit (Exam 70-298) : Designing Security for a Microsoft Windows Server 2003 Network* 一书的作者，是 McGraw-Hill 公司出版的 *Network Security: The Complete Reference* 一书的主要作者。她还为 QUE 和 New Riders 等出版公司撰写了不少关于 SQL Server 2000、CISSP 和 Windows 安全技术方面的文章。

此为试读，需要完整PDF请访问：www.ertongbook.com