Linux黑客大曝光

第3版

Linux安全机密与解决方案

Hacking Exposed Linux: Linux Security Secrets & Solutions, Third Edition

本书引导读者以一个实用的、现实世界的方法，帮助他们理解所面临的具体风险继而采取恰当的缓解措施。

——Jake Kouns，CISSP、CISM、CISA
开放安全基金会总裁、开放源代码漏洞数据库（OSVDB）项目负责人

[美] 安全研究社团（ISECOM） 编著
夏毓彦
常晓林
史争印 等译

清华大学出版社

Linux 黑客大曝光

Linux安全机密与解决方案（第3版）

Hacking Exposed Linux

Linux Security Secrets & Solutions, Third Edition

（美）安全研究社团（ISECOM） 编著

夏毓彦
常晓林
史争印 等译

清华大学出版社
北 京

本书版权登记号：图字：01-2009-4893

内 容 简 介

《Linux黑客大曝光：Linux安全机密与解决方案》第三版是一个全新的版本。由ISECOM安全研究社团中Linux各领域的专家根据最新、最全面的研究成果对其进行了彻底地重写，包括Linux 2.6内核新增加的诸多安全功能。ISECOM是知名的OSSTMM方法学手册的编著者，专注于提供有关安全性方面的全方位严谨思考和科学论证方法。

本书涵盖的内容十分丰富，包括安全控制、安全分析方法，以及Linux系统、数据网络、网络拨号、VoIP、蓝牙、射频识别、辐射攻击、可信计算、Web应用攻击、邮件服务、域名服务、C代码静态分析、Linux内核等领域的黑客攻防技术。书中的所有组织材料，包括入侵案例都是最新的，在写作中遵循着“黑客大曝光”系列的一贯思路：每章以一个入侵案例展开，然后阐述这一领域的基础知识、可能发生的攻击，最后给出防范措施和安全对策。各领域内容相互独立，因此便于读者针对某一领域进行专门学习。

本书面向各行各业、政府机关、大专院校关注信息安全的从业人员，是Linux信息系统安全专业人士的权威指南，也可作为信息安全相关专业的教材教辅用书。

图书在版编目（CIP）数据

Linux 黑客大曝光：Linux 安全机密与解决方案（第 3 版）/（美）安全研究社团（ISECOM）编著；夏毓彦等译.—北京：清华大学出版社，2011.1

书名原文：Hacking Exposed Linux: Linux Security Secrets & Solutions，Third Edition

ISBN 978-7-302-24245-1

I. ①L… II. ①安… ②夏… III. ①Linux 操作系统—安全技术 IV. ①TP316.89 ②TP393.08

中国版本图书馆 CIP 数据核字（2010）第 231083 号

责任编辑：夏非彼　卢　亮

责任校对：闫秀华

责任印制：王秀菊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座

http://www.tup.com.cn　　**邮　　编**：100084

社　总　机：010-62770175　　**邮　购**：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂

装 订 者：三河市溧源装订厂

经　　销：全国新华书店

开　　本：185×230　**印　张**：38.25　**字　数**：930 千字

版　　次：2011 年 1 月第 1 版　　**印　　次**：2011 年 1 月第1 次印刷

印　　数：1～4000

定　　价：79.00 元

产品编号：033798-01

作为项目领导者，我把这本书奉献给所有志愿者，感谢他们对 ISECOM“Make sense of security”的帮助及贡献，让世界获得多一些的宁静。正是他们这样无私的黑客，使得成为一名黑客是件多么自豪的事情。

我还需要说，如果没有我的妻子 Marta 义无反顾地支持，所有的这些工作足以压跨一切。甚至我的三个孩子 Ayla、Jace 和 Aidan 也把 ISECOM 时常挂在嘴边，同样对写作此书非常有帮助。

—Pete Herzog

关于作者

本书根据 ISECOM（Institute for Security and Open Methodologies，安全和开放方法研究社团）的项目方法论编写。ISECOM 是一个开放的、非营利的安全研究和认证组织，建立于 2001 年 1 月，以提高安全认识为目标。他们遵循开放方法许可，发布了安全标准和方法论供个人和企业使用。

本书由多位作者、审稿人，以及编辑——还有许多不能一一列举的人士——共同合作完成。他们精诚合作，尽其所能以期编写最好的黑客图书。由于没人能够掌握所有关于 Linux 能做什么的知识，团队编写此书能告诉我们如何安全操作 Linux。

下面是为此书做出巨大贡献的人员，在此特别介绍。

关于项目领导者

Pete Herzog

作为董事长（MD），Pete 是 ISECOM 的创始人之一，也是 OSSTMM 的创建者。在工作中，Pete 倾力于进行科学的、严谨的对安全质量控制的测试。目前他负责着多个开发项目，包括为业主安全、青少年的黑客教程、源码静态分析、儿童的批判性思维训练、测试电磁频谱无线认证和培训、安全解决方案——立法者指南、一本苏斯博士型的押韵的儿童书、安全分析教程、“人类安全”指南、大学保安及安全解决方案、国家改革安全使用指南、为婚姻事务咨询师与家庭医生的精确信任程度指南，当然，还有开源安全测试方法论手册（OSSTMM）。

除了管理 ISECOM 项目，Pete 还在巴塞罗那拉萨尔大学教授安全课程，为世界范围的安全认证网络合作伙伴提供支持和培训。Pete 拥有锡拉丘兹大学（Syracuse University）的学士学位。眼下，他的唯一消遣方法是与家人一起去欧洲和北美旅游。

关于项目管理者

Marta Barceló

Marta Barceló 是 ISECOM 的运营部经理，也是创始人之一，负责 ISECOM 的商业运作。在 2003 上半年，她为黑客高等学校（Hacker Highschool）项目设计了流程，开发和设计了针对网站和个人的多语言课程。几年后，她又主管 ISESTORM 会议的财务和 IT 运营工作。在 2006 年，Marta 受邀加入了欧盟赞助的开放可信计算联盟，管理 ISECOM 参与的事务，包括财务和运营过程。2007 年，她开始负责 ISECOM 的宣传广告工作，提供创新技术和指导。Marta 维护 ISECOM 项目的媒体宣传，为网站提供技术服务器的管理。她曾在德国曼海姆应用科学大学学习，并获得计算机科学的硕士学位。

除了维护 ISECOM，Marta 对艺术有着执着的追求，特别是摄影和平面设计，她的第一个学位就是在巴塞罗那 Liceu 音乐学院获得的。

Rick Tucker

Rick Tucker 主要为 ISECOM 负责项目的技术写作、编辑，并为许多项目提供技术支持，包括 SIPES 和黑客高等学校项目。他如今住在美国俄勒冈州的波特兰，就职于一家小型律师事务所，是该律师事务所处理各种平凡而复杂问题的灵魂人物。

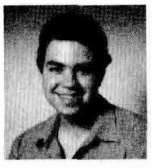
关于作者

Andrea Barisani

Andrea Barisani 是国际知名的安全研究员。他的专业生涯始步于 8 年前，但实际开始于一台 Commodore-64——在他 10 岁的时候。现在，Andrea 的兴趣有大规模的 IDS/防火墙部署管理、取证分析、漏洞评估、渗透测试、安全培训和他的开源项目。最终，Andrea 发现系统与安全管理是唯一令他痴狂的事情。

Andrea 是 OCERT（Open CERT）的创始人和项目协调员，作为安全和基础设施组的一员，他参与了 Gentoo 项目。同时，他也是 OSSTMM 的成员，逐渐成为 ISECOM 的核心成员。此外，他也是 Inverse Path 公司的首席安全工程师和创始人之一。他常在 PacSec、CanSecWest、BlackHat 和 DefCon 会议发表演讲和培训。

Thomas Bader



Thomas Bader 在 Dreamlab 技术公司担任培训师和方案架构师。自 2007 年夏初以来，他负责瑞士境内的 ISECOM 课程。作为 ISECOM 成员，他参加了 OPSE 认证课程、ISECOM 网络测试和 OSSTMM 的开发。

自从 1997 年第一次接触开源软件以来，他就专注于网络与安全技术。在接下来的几年里，他一直工作于这个领域，在很多公司担任顾问和技术人员，从中获得了丰富的经验。自 2001 年以后，Thomas 担任了 LPI 培训课程的开发人员和培训师。2006 年以来，他在 Dreamlab 技术公司工作，作为欧洲德语和法语国家的官方 ISECOM 代表。

Simon Biles

Simon Biles 是 Thinking Security（一个英国信息安全咨询公司）的主管和牵头顾问。他也是 O'Reilly 出版的 The Snort Cookbook 一书的作者，同时也为 ISECOM、Microsoft，以及 SysAdmin 杂志撰写过其他材料。目前他正在 Shrivenham 的国防学院学习计算机取证。Simon 拥有 CISSP、OPSA 证书，是 ISO17799 主任审核员，也是英国计算机协会（BCS）特许会员。已婚，有几个孩子。他的妻子不仅是最漂亮的，而且当他说“我只是同意 ……（时间不断流失）”之类的话时，她是如此有耐心。在空闲时，他会开着心爱的路虎到处逛，而且对拥有一辆“非常可靠的”二手路虎觉得非常自豪。

Colby Clark

Colby Clark 是导航软件网络安全的管理者，他负责每天监督信息安全项目的开发、执行和管理。他有多年的安全管理经验，在财富 500 强企业、律师事务所、金融机构、教育机构、通信公司和其他国有、私营公司都有着良好的信誉，为他们解决过法规遵从方面的咨询和审查（Sarbanes Oxley 和 FTC Consent Order）、安全咨询、业务持续、灾难恢复、事故处理和计算机取证调查方面的难题。Colby 拥有南加州大学商业管理专业的高级学位，保持着 EnCE、CISSP、OPSA，以及 CISA 证书，并在 CEIC（Computer and Enterprise Investigations Conference，计算机及企业调查研讨会）教授过高级计算机取证和事故响应技术的培训课程。他也是 OSSTMM 开发者中的一员，自 2003 年以来，一直为 ISECOM 工作。

Raoul Chiesa

除了 Raoul Chiesa，几乎没有其他人在信息安全领域能有 22 年的经验，以及 11 年的专业知识。他是 Mediaservice.net Srl（一个意大利的安全咨询公司）的创始人和主席。Raoul 现为 OWASP 意大利分会、国际网络安全组织 TSTF（TSTF.net）董事会成员，也是 ISO 国际用户组的成员。自 2007 年，他一直担任联合国区域间犯罪和司法研究所（UNICRI）的咨询顾问工作。

他曾写作 *Hacker Profile*，此书在 2008 年由美国 Taylor & Francis 出版社出版。Raoul 的公司也是 ISECOM 在世界的第一个合作伙伴，早在 2003 年，就创办了 OPST 和 OPSA 课程。在 ISECOM，他是传媒主管，负责加强 ISECOM 在全世界的传播。

Pablo Endres

Pablo Endres 是一名安全工程师兼顾问和技术解决方案架构师，具有很强的技术背景，为很多公司服务过，包括无线电话供应商、VoIP 解决方案供应商、联络中心、大学、咨询机构等等。他与计算机打交道是在 20 世纪 80 年代末（一台 PC-XT），并拥有加拉加斯西蒙玻利瓦尔大学的计算机工程专业学位。Pablo 已经致力于 Linux、Unix，以及网络系统方面的工作和研究 10 多年了。

Pablo 在此感谢 Pete 给了他与 ISECOM 一起编写此书的机会。最后要感谢的是，他的妻子和父母对他的大力支持和与他一起度过的时光。

Richard Feist

Richard Feist 自 1989 年正式成为一名程序员以来，一直工作于计算机领域。他对商业和 IT 领域都有独到的见解，很少有人能够在这两个领域有这么大影响。最近他创办了自己的小型 IT 安全咨询公司 Blue Secure。Richard 拥有各种的安全证书（CISSP、rince2 Practitioner,、OPST/OPSA trainer、MCSE 等），并努力走在前沿。

Andrea Ghirardini

Andrea Ghirardini 在计算机取证分析领域有 7 年多的经验，他领导的实验室（@PSS Labs，http://www.atpss.net）曾协助意大利和瑞士警察特别部队调查了 300 多起案件，其中包括毒品犯罪、诈骗犯罪、偷税漏税、恐怖主义、武器走私、谋杀、绑架、网络钓鱼等等。

他的实验室是意大利最早成立的实验室之一，专门处理和检测数字证据（结合使用开

源以及商业的工具）。在组建 CF 机器和存储系统时得到了公司团队的持续支持。2007 年，Andrea 在意大利出版了第一本关于计算机取证调查和方法（Apogeo Editore）的图书。在书中，还分析了意大利关于这些犯罪的法律。在意大利 Andrea 获得了他的第三个 CISSP 证书。

Julian "HammerJammer" Ho

"HammerJammer" Julian Ho 是 ThinkSECURE Pte 公司（*http://securitystartshere.org*）的创始人之一，也是一个面向亚洲的 IT 安全认证和培训方面的权威，提供专业 IT 安全服务，同时，他还是 ISECOM 认可的 OPST 培训师。

Julian 曾经负责新加坡樟宜国际机场第一和第二候机楼和新达城会议中心的 StarHub 无线热区的安全保障的设计、执行以及维护工作。他是 BlackOPS 设计小组的成员，参加过 2004 年在新加坡举行的安全锦标赛"HackAttack（黑客攻击）2004"，2005 年的 AIRRAID（亚洲首届无线攻击锦标赛）以及 2008 年的 AIRRAID2（泰国首届黑客攻击全国联赛），还为 2006 年 WCCD 漏洞的研究和发布做出了重要贡献。

Julian 开发了 OSWA 助手无线审核工具包（OSWA-Assistant Wireless Auditing Toolkit），并一直负责维护，该工具包被 Security-Database.com 在他们的 Best IT Security and Auditing Software 2007 中评为无线测试类最佳作品，以及 LiveCDs 类的优秀/推荐软件。

Marco Ivaldi

Marco Ivaldi（raptor@mediaservice.net）是一名计算机安全研究员和顾问、软件开发人员以及 Unix 系统管理员，对网络、电话学和密码学有着特殊的兴趣。Marco 是 ISECOM 的核心成员，积极参与到 OSSTMM 的开发进程中。他拥有 OPST 证书，如今在 Mediaservice.net（意大利一家著名的信息安全公司）作为一名红组协调员。每日的工作包括高级渗透测试、ISMS 调度和审计、漏洞研究及利用程序开发。Marco 同时也是 *Linux&C* 杂志（意大利第一本关于 Linux 和开源技术的杂志）的创始人和编委会成员。想要了解他的更多信息，请关注其主页 http://www.0xdeadbeef.info。

Marco 非常感谢 VoIP 的权威：TSTF 的伊曼纽尔·伽代克斯（Emmanuel Gadaix）以及，thegrugq（笔名），在全书的写作过程中，他们给予了非常宝贵的意见和支持。Marco 对本书的贡献是不可替代的。

Dru Lavigne

Dru Lavigne 是一名网络和系统管理员、IT 指导员、课程开发员以及作者。她有十多年的管理和教授 Netware、Microsoft、Cisco、Checkpoint、SCO、Solaris、Linux 以及 BSD 等系统的经验。她也是 *BSD Hacks* 和 *The Best of FreeBSD Basics* 两本书的作者。目前她是介绍开源技术的一本免费月刊 *Open Source Business Resource* 的总编辑。Dru 同时也是 BSD 认证集团公司的创始人及现任主席。BSD 认证集团公司是制订 BSD 系统管理员标准的非营利组织。在 ISECOM，她主要维护开放协议数据库（Open Protocol Database），其博客地址为 http://blogs.ittoolbox.com/unix/bsd。

Stephane Lo Presti

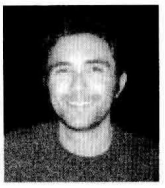
Stephane Lo Presti 是一位研究科学家。在过去几年内，他一直在探索计算机科学中信任的各个方面。Stephane 目前工作于伦敦城市大学，研究面向服务和可信度的架构。他的项目经历包括英国伦敦大学皇家霍洛威学院的开放源代码的可信计算欧洲项目（http://www.opentc.net），以及英国南安普敦大学的可信软件代理和服务（T-SAS）项目。Stephane 喜欢把他的需求分析和正规计算技能运用到现代系统以及一些重要属性（如可信度）当中去。2002 年，Stephane 在法国格勒诺布尔技术研究所获得计算机科学专业博士学位，这里也是他 1998 年在高等计算和应用数学学院作为一名计算机工程师毕业的地方。

Christopher Low

Christopher Low 也是 ThinkSECURE Pte 公司的创办人之一，该公司是一个面向亚洲提供 IT 安全培训、认证和专业 IT 安全服务的组织。Christopher 有超过 10 年的 IT 安全经验以及丰富的安全咨询及渗透测试经验。Christopher 还是一位富有才华的培训师，一位经 ISECOM 认证的 OPST 培训师。凭借着丰富的 IT 领域的安全经验，他主要讲授各种基于实际应用的安全认证课程。他也是 BlackOPS 设计小组的一员，参加过 2004 年在新加坡举行的安全锦标赛“HackAttack（黑客攻击）2004”、2005 年的 AIRRAID（亚洲首届无线攻击锦标赛）以及 2008 年的 AIRRAID2（泰国首届黑客攻击全国联赛）。

Christopher 也是一位热衷于安全研究的专家，他喜欢编码，曾开发了 Probemapper 和 MoocherHunter 工具。在 OSWA 助手无线审核工具包中可以找到这些工具。

Ty Miller



Ty Miller 是悉尼 Pure Hacking 安全公司的首席技术官。Ty 为很多大银行、政府机构、电信，以及保险公司做过渗透测试，而且为澳大利亚教育和航空领域的众多组织负责设计和管理大型安全架构。

在拉斯维加斯举行的 2008 年黑帽大会（Blackhat USA 2008）上，Ty 发表了其关于 DNS 隧道 Shellcode 的研究成果；也参与了 CHAOS Linux 发行版的开发。CHAOS Linux 旨在成为一个最具影响力、最安全的 openMosix 集群平台。Ty 是具 ISECOM OPST 和 OPSA 资质的培训师，参与了 OSSTMM 手册的编写工作。同时，他还为许多的组织或会议开展 Web 应用程序安全课程以及渗透测试方面的教学培训。

Ty 拥有澳大利亚麦夸里大学信息与通信系统专业的技术学位。他的爱好包括 Web 应用渗透测试和 Shellcode 研究（注——Shellcode 是溢出程序和蠕虫病毒的核心）。

Armand Puccetti

Armand Puccetti 是 CEA-LIST ［法国原子能委员会（NEA）的一个部门，http://www-list.cea.fr］的一位研究工程师兼项目经理，他在这个部门的软件安全实验室工作，参与了欧洲好几个 MEDEA+、EUCLID、ESSI 及 FP6 计划的研究项目。Armand 研究兴趣广泛，包括软件和硬件描述语言的形式化方法、程序语言语义学、命题证明、编译，以及基于事件的模拟技术。在 2000 年转入 CEA 之前，Armand 一直在 C-S（Communications & Systems，一家私人软件公司，http://www.c-s.fr/）做项目经理，参与了多个软件和应用项目的开发和研究，从 CASE 工具和编译器开发到军事仿真工具和方法（http://escadre.cad.etca.fr/ESCADRE）的研究和咨询。

Armand 毕业于法国 INPL 大学（http://www.inpl-nancy.fr），1987 年在那里获得 Ada 程序设计语言语义学证明和定理性证明的博士学位。

关于其他有贡献的作者

Görkem Çetin

Görkem Çetin 是一位一直享有盛誉的 Linux 以及开源技术专家，已长达 15 年之久。在博士研究期间，Görkem 就致力于研究免费/开源软件的人机交互问题。Görkem 已经写了 4 本关于 Linux 与网络的书籍，还在技术和行业杂志发表了大量的文章。他现在是土耳其国家密码学和技术研究所（TUBITAK/ UEKAE）的一名项目经理。

Volkan Erol

Volkan Erol 是土耳其电子密码学国家研究所（TUBITAK-NRIEC）的一名研究员。在获得加拉塔萨雷大学工程技术学院的计算机工程专业的理学士学位之后，Volkan 在伊斯坦布尔理工大学的计算机科学继续深造，获得硕士学位。作为软件工程师，他曾参与 Turkcell ShubuoTurtle 项目，并在 2005 年 9 月，加入 TUBITAK-NRIEC，作为一名全职研究员，Volkan 的研究方向是开放的可信计算项目。他的研究领域包括可信计算、实用密码技术、软件开发以及图像处理。

Chris Griffin

Chris Griffin 在信息安全方面有着 9 年的经验。Chris 获得了 OPST、OPSA、CISSP 以及 CNDA 证书，也是 OSSTMM 项目的一名积极作者。前不久，他成了 ISECOM 美国的培训师。Chris 感谢 Pete 给了他这次机会，并感谢他的妻子和孩子耐心的支持。

Fredesvinda Insa Mérida

Fredesvinda Insa Mérida 是 Cybex（赛百斯）的一名战略发展经理。Dr. Insa 毕业于巴塞罗那大学的法律专业（1994~1998），并在马德里大学（又名马德里康普斯顿大学）信息科学与通信专业获得博士学位。在许多次的计算机取证及电子证据会议上，Dr. Insa 都作为 Cybex 的代表。她有着丰富的打击计算机犯罪方面的经验。在 Cybex 期间，她为计算机取证专家提供法律支持。

关于编辑和审稿员

Chuck Truett

Chuck Truett 是一名作家、编辑、SAS 程序员，以及数据分析员。除了在 ISECOM 工作，他写了许多适合于从儿童到角色扮演游戏玩家的小说及非小说类的作品。

Adrien de Beaupré

Adrien de Beaupré 是贝尔（Bell）加拿大电信公司的实践带头人。获得的证书包括：GPEN、GCIH、GSEC、CISSP、OPSA 以及 OPST。Adrien 常活跃于 isc.sans.org，也是一名被 ISECOM 认可的 OSSTMM 讲师。他精通漏洞评估、渗透测试、紧急事件响应以及数字取证等技术。

Mike Hawkins

Mike Hawkins，CISSP，在计算机领域具有超过 10 年的工作经验。他的服务对象大部

分是财富 500 强公司。Mike 现在是一家扬声器公司 Klipsch 的网络安全经理。他作为一个全职的安全专家已经 5 年多了。

Matías Bevilacqua Trabado

Matías Bevilacqua Trabado 毕业于巴萨罗那大学的计算机工程专业，现工作于 Cybex，是一名 IT 经理。由于有着安全背景，Matías 专门从事计算机取证及电子证据的采纳工作。他筹划了并掌管着西班牙的第一个私人取证实验室，现在则在 Cybex 领导着研发部门。

Patrick Boucher

Patrick Boucher 是 Gardien Virtuel 公司的一名高级安全顾问。在道德黑客、安全策略以及战略规划（比如灾难恢复和可持续性计划）等方面，Patrick 都有多年的工作经验。Patrick 的客户包括了财富 500 强的许多公司、金融机构、电信公司，以及遍及加拿大的中小企业。Patrick 拥有 CISSP 和 CISA 证书。

序　言

我对安全的兴趣开始于小时候。那时，我的父亲加入了某著名大学的一个博士项目，这让我非常幸运。当他在做研究时，我在那儿接触了许多的系统（有一台 Vax 11/780，还有其他的系统）。在实验室的那几年，我有了一台个人的 Commodore 64 电脑（注——Commodore International 公司在 1982 年 8 月发行的一款 8 位家用电脑），还有一个 300 bps 的 modem（调制解调器），能够访问神奇的 UUCP 互联世界。我成功完成的第一个黑客之举，就是写一个登录脚本，模拟了一次不是很成功的登录，并将那个受害者输入的用户名和密码写入到了一个文件中。这次攻击使得我可以在没有父亲监管的情况下任意登录那台系统。这次经历，以及后来的经历，教我懂得了无效的安全控制的许多知识。这激发了我去掌握更多的知识。

在 1992 年，我开始成为一名系统管理员，为一家小工程公司工作。我负责大约 30 台工作站、一个使用 UUCP 拨入的 Email 供稿的（feed）BBS 网站、一些 SCO Unix 服务器，以及一台 Novell Netware 服务器。一段时间以后，公司要求我将这个小型网络接入 Internet。这时，我正好在学习 Linux 和 IP 伪装的共享能力方面的技术。接下来的几年，Linux 成为了我工作的核心，在很多项目中我都使用的是 Linux 系统，包括更新 Novell 和 SCO 服务器。

这段时间，大部分的 IT 厂家都很乐意简单地保持系统的正常运作。任何安全控制都被认为有益的，然而却没有一个标准化的方式去衡量这样的有效性。这是安全在私营企业中的一段绝对黑暗时期，因为安全已经普遍地被认为是一种高不可攀的艺术形态。安全，已被束之高阁。

后来的生活中，我成为一名安全顾问，被要求完成一个信息安全测试项目。我已参加过 SANS 课程，读过各种的“Hacking”书籍，会使用很多的工具，但还是觉得远远不够。毕竟是学无止境。在通过互联网搜索一种有条理的安全测试方法后，我非常高兴偶然找到了《开源安全测试方法学手册》（*Open Source Security Testing Methodology Manual*，OSSTMM）的某个最初版本。项目的团队合作深得我心；OSSTMM 允许每一个安全测试专业人士为一

个全面的、可重复的、有条理的测试指南贡献他们的才智。亲身实践的经验证明，这种安全测试的方法大大优于随机抓取和刺探（漏洞）的方法，以前，我们只在“渗透测试”的模糊指导下实现这些方法。现在，我再也不会满足于“安全是一门艺术，不是一门科学”这样一种理念了。

作为 ISECOM 董事会的一员，我非常荣幸地监督和参与了我们所有关键项目的开发过程。ISECOM 成员饱满的激情、追求卓越的决心和把握抽象课题的精神使得作者们不断努力向前。读者手中的这本书，就是他们特别为 Linux 安全而写的劳动成果。

我希望读者好好阅读这本书，就像我们如此乐此不疲一样。如果你希望也加入到我们的 ISECOM 团队，或希望参加我们的任何项目，请访问 http://www.isecom.org 联系我们。

Robert E. Lee
首席安全官
Outpost24 AB

Robert E. Lee 是 Outpost24 AB 的首席安全官，Outpost24 是一个著名的、位于前沿的网络安全解决方案提供商。Outpost24 的解决方案提供全方位全自动的网络漏洞扫描，并提供扫描报告、弱点管理工具。Outpost24 的解决方案可以数小时内部署完毕，也可在世界范围内部署使用，使客户详细了解安全状况及其政策遵循状态（compliance posture）。OUTSCAN 是欧洲部署使用最广的 On-Demand（按需）安全解决方案，去年为 1000 多名顾客提供扫描服务。

致　谢

在此特别感谢 Jonathan Bokovza、Šarunas Grigaliunas 和 Harald Welte 他们及时的、无微不至的帮助，也感谢 Jane Brownlow、Jennifer Housh 和 LeeAnn Pickrell。

引言

GNU-Linux 是世界上顶级黑客的乐园，也是他们一个可以发挥无限想象的玩具，与我们小时候玩的一盒积木或是一袋橡皮泥没有什么不同。不管是一名艺术家还是一名科学家，玩出花样的可能性是无穷的。想利用计算机执行、编译、生成的任何东西，只受限于你的创造力。这就是 Linux 迷人的地方。

很多人简单地称它为 Linux，而不是它的全名——GNU-Linux，这就像人们常常称呼好友的昵称，而不是全名一样。也许正是因为读者可以用该操作系统通过其源代码来实现任何项目，才有了这种亲密关系；又或者是来源于加入某个社群的经验。不管如何获得，人人都可以受益于与一台机器的交流，这实在应归功于 Linux 的透明性和开放性。

尽管在 Internet 不是上占优势的操作系统，Linux 仍然相当流行。考虑到绝大多数提供 Web 服务、Email 服务，以及域名解析服务的服务器都依赖于 Linux 的开源代码。这给我们带来了困扰，如此开放的系统能做到适当的安全吗？

难点就在于如何保护它。你认为应该如何去保护这样开源的系统呢？它所有设计的组件都是一点一点地编译、再编译，然后再配置加上去的。不同机器也不会完全一样。两个完全一样的系统是不可能存在的。那么，我们将如何一点一点地实现对所有这些系统的保护呢？

《Linux 黑客大曝光》第三版是基于 ISECOM 的研究成果写成的。ISECOM 是一个开放的安全研究组织，以提高系统安全意识为己任。ISECOM 在全世界已经有成千上万的成员，提供了大量与保安、安全及隐私有关的方法和架构。ISECOM 通过广泛的合作和不断地复审，努力追求最高质量的研究成果——如同本书的写作。由众多热心安全和专业人士合作去编写一本现实的、可实践的、真正抓住 Linux 精髓的著作。只有通过这种方法，才能找到全方位地巩固 Linux 系统安全的方法。