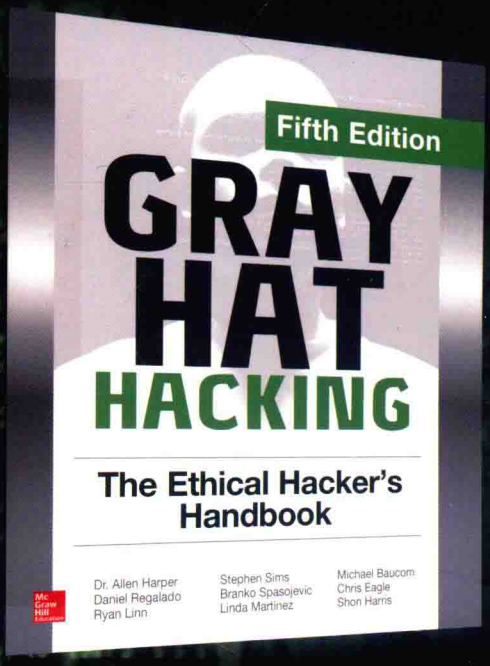
安全技术经典译丛

Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition

灰帽黑客（第5版）

正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术



艾伦·哈珀(Allen Harper)
[美] 丹尼尔·里加拉多(Daniel Regalado) 等著
赖安·林(Ryan Linn)
栾 浩 毛小飞 姚 凯 等译
网安世纪科技有限公司 审校

清华大学出版社

安全技术经典译丛

灰帽黑客

(第5版)

艾伦·哈珀(Allen Harper)
[美] 丹尼尔·里加拉多(Daniel Regalado) 等著
赖安·林(Ryan Linn)

栾 浩 毛小飞 姚 凯 等译

清华大学出版社

北 京

Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, Shon Harris
Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
EISBN：978-1-260-10841-5

图书在版编目(CIP)数据

灰帽黑客：第5版 / (美)艾伦·哈珀(Allen Harper)，(美)丹尼尔·里加拉多(Daniel Regalado)，(美)赖安·林(Ryan Linn) 等著；栾浩，毛小飞，姚凯 等译. —北京：清华大学出版社，2019
(安全技术经典译丛)
书名原文：Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
ISBN 978-7-302-52768-8

Ⅰ. ①灰… Ⅱ. ①艾… ②丹… ③赖… ④栾… ⑤毛… ⑥姚… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

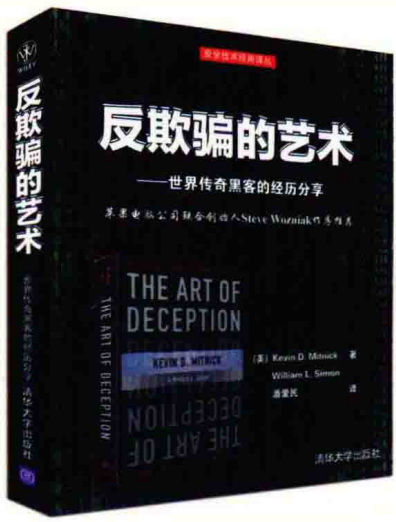
中国版本图书馆CIP数据核字(2019)第071024号

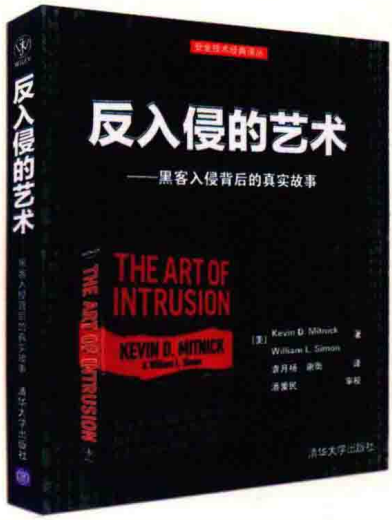
责任编辑：王　军
装帧设计：孔祥峰
责任校对：成凤进
责任印制：丛怀宇

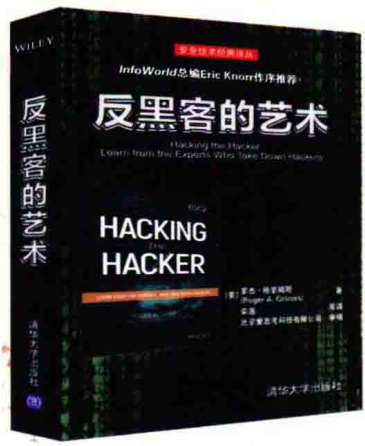
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市铭诚印务有限公司
经　　销：全国新华书店
开　　本：170mm×240mm　　印　　张：36.5　　字　　数：736千字
版　　次：2019年6月第1版　　印　　次：2019年6月第1次印刷
定　　价：128.00元

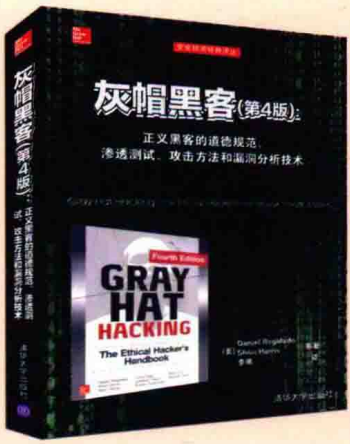
产品编号：081477-01

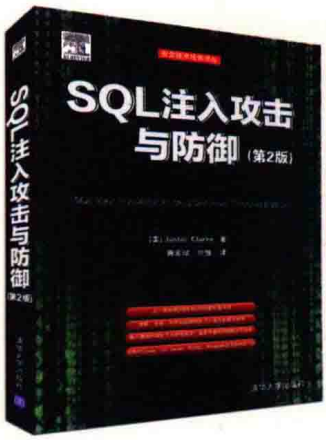
安全技术经典译丛

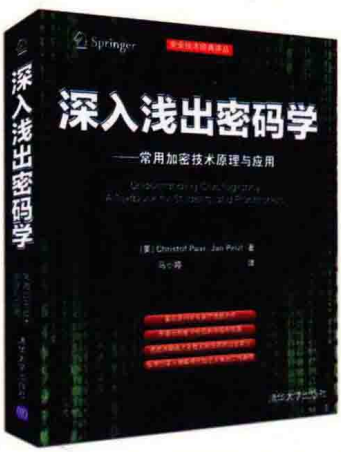

反欺骗的艺术
——世界传奇黑客的经历分享
THE ART OF DECEPTION
KEVIN D. MITNICK
[美] Kevin D. Mitnick 著
William L. Simon
清华大学出版社

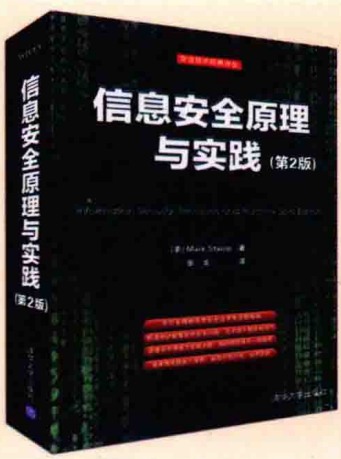

反入侵的艺术
——黑客入侵背后的真实故事
THE ART OF INTRUSION
KEVIN D. MITNICK
[美] Kevin D. Mitnick 著
William L. Simon
清华大学出版社

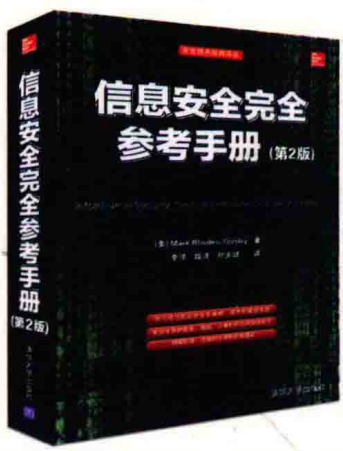

反黑客的艺术
InfoWorld总编Eric Knorr作序推荐
HACKING
HACKER
清华大学出版社


灰帽黑客(第4版)
正义黑客的道德规范
渗透测试、攻击方法和漏洞分析技术
GRAY
HAT
HACKING
The Ethical Hacker's Handbook
清华大学出版社

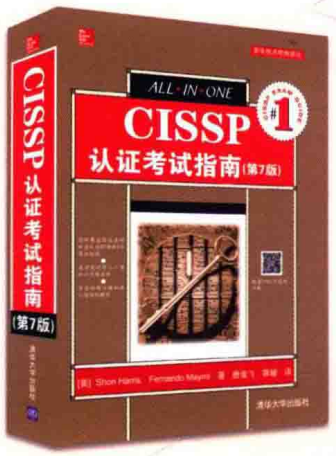

SQL注入攻击与防御(第2版)
清华大学出版社

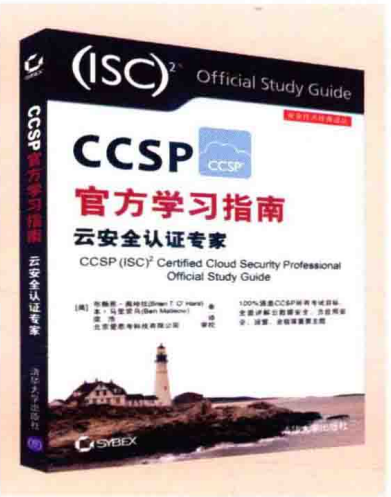

深入浅出密码学
——常用加密技术原理与应用
清华大学出版社

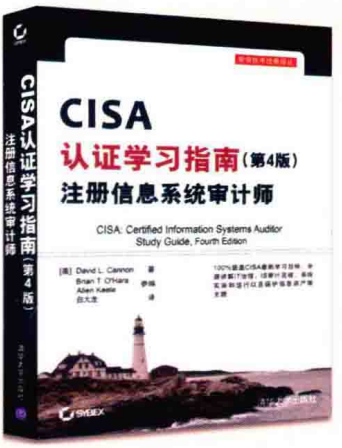

信息安全原理与实践(第2版)
清华大学出版社

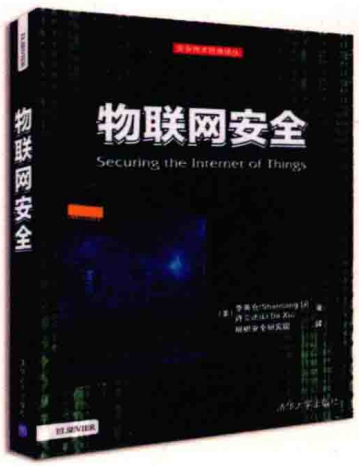

信息安全完全参考手册(第2版)
清华大学出版社

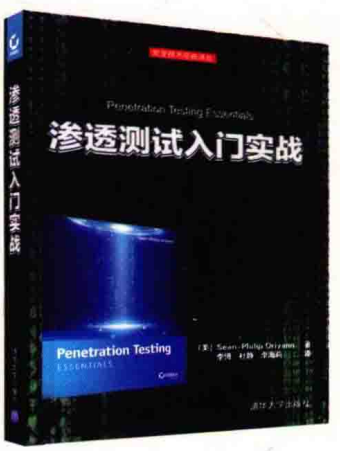
安全技术经典译丛

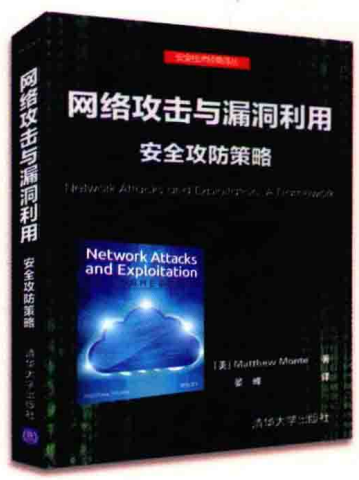


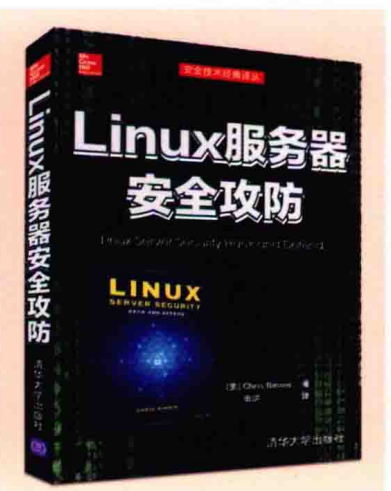


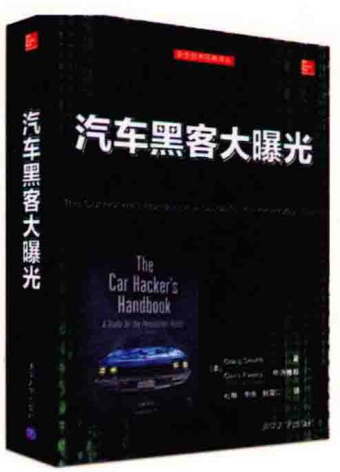












译 者 序

关注新闻的朋友可能知道，《焦点访谈》在2018年11月播放过一期节目，讲的是网络安全。节目中报道的一些事件触目惊心。对于广大企业来说，恶意攻击者尽管不是这种专业机构，但是攻击的后果也是非常严重的。典型的案例就是台积电因为勒索病毒的攻击，生产线全数停摆，预计损失高达17.4亿元人民币。从上面的案例可以发现，网络虚拟世界是一个没有硝烟的战场，时时刻刻有心怀恶意的人试图绕过公司的防护，期望获取不当收益。

对于网络安全面临的严峻形势，党和国家领导人有敏锐的洞察。习近平总书记主持召开了网络安全和信息化工作座谈会并对网络安全做出重要指示。习近平总书记指出："第一，树立正确的网络安全观。理念决定行动。当今的网络安全，有几个主要特点。一是网络安全是整体的而不是割裂的。在信息时代，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。二是网络安全是动态的而不是静态的。信息技术变化越来越快，过去分散独立的网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念。三是网络安全是开放的而不是封闭的。只有立足开放环境，加强对外交流、合作、互动、博弈，吸收先进技术，网络安全水平才会不断提高。四是网络安全是相对的而不是绝对的。没有绝对安全，要立足基本国情保安全，避免不计成本追求绝对安全，那样不仅会背上沉重负担，甚至可能顾此失彼。五是网络安全是共同的而不是孤立的。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。"

作为一名网络安全从业人员，对于网络安全我们有着切身体会。必须认识到，世界上没有绝对安全的系统。首先，计算机技术飞速发展，过去安全的手段在今天强大且廉价的计算能力之下，节节败退。其次，所有的系统都是由人开发的，开发过程中不可避免存在逻辑、思维和技术上的疏漏，因此系统漏洞不可避免。最后，随着新技术的出现，新的攻击手段层出不穷，例如Mirai僵尸网络感染数以千万计的物联网设备，发起有史以来最大规模的DDoS攻击。对于Mirai在还没有出现行之有效的应对手段之前，攻击手段又一次升级了——BrickerBot又已经开始发动PDoS攻击。

《孙子兵法》说道，"知彼知己，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必败。"企业的网络安全建设往往从自身出发，关注内部建设，试

图关起门，高筑墙，希望通过这样的方式抵御攻击。这种做法也就是只能做到知己，甚至有时连这一点也做不到。在网络安全的攻防中，最多只是与不知名的对手打个平手。为了在网络防御战中战胜对手，我们在知己的同时还要知彼，了解黑客的攻击手段和方法。鉴于此，为了“加强对外交流、合作、互动、博弈，吸收先进技术”，我们引进并翻译了《灰帽黑客(第5版)》，希望通过本书，让广大计算机从业人员，尤其是安全从业者，能够对计算机攻击方法有清晰的认识，从而在日常的运维及开发中加强安全意识，提升网络防御能力。

《灰帽黑客(第5版)》在漏洞原理、代码调优、内存数据提取的技巧、动态调试、静态分析等各个方面，结合各种实验，指导读者构造漏洞代码，亲自动手来完成对漏洞的利用。难能可贵的是，漏洞代码量非常少，对初学者来说很容易理解，这是市面上大部分技术书籍所不具备的优点。作为一本经典图书，本书追随计算机技术的发展，一直在更新。但不可否认，相对于技术的发展，书本的内容存在滞后。但本书向广大读者介绍了计算机攻击技术的基本原理和运用，而这部分变化相对较小。广大读者在掌握本书内容的基础上，可参考其他资料，进一步提升自身能力。

必须强调指出，本书介绍的技术既可用于提高网络防御，也可用于进行网络攻击。广大读者必须恪守道德准则，抵制各种诱惑，坚守“未经授权，处理别人的计算机和数据就是犯罪行为”这一基本信条。在安全界，素有“白帽”“黑帽”“灰帽”黑客之说。黑帽黑客是指那些造成破坏的黑客；而白帽黑客则研究安全，以建设安全的网络为己任；灰帽黑客发现漏洞却不公开，而是与供应商一起合作来修复漏洞。我们希望大家都成为灰帽和白帽黑客，将学到的技术用于正义的事业。

本书从2018年4月初开始，经过近8个月的艰苦努力，才全部完成翻译。在翻译过程中译者力求忠于原著，尽可能传达作者的原意。在此，非常感谢栾浩先生，正是在他的努力下，这些译者才能聚集到一起，完成这项工作。同时，栾浩先生投入了大量的时间和精力，组织翻译工作，把控进度和质量。没有他的工作，翻译工作不能这么顺利地完成。同时，也要感谢姚凯先生，他全程参与文稿的翻译和校对，投入大量业余时间对文稿进行了多轮校对，提出大量宝贵意见，保证了全书的质量。同时感谢清华大学出版社和编辑的严格把关，正是因为他们的辛勤付出和繁重的幕后工作，才有了本书的出版。

感谢网安科技有限公司组织的安全技术资源，以及对本书翻译和校对工作给予的大力支持。

本书涉及内容广泛，立意精深。因为能力局限，在翻译中难免有错误或不妥之处，恳请广大读者朋友不吝指正，不胜感激。

从业人员对本书的赞誉

《灰帽黑客(第5版)》一如既往地呈现大量攻击性IT安全原则的最新知识精髓。9位作者都是备受尊崇的信息安全大师，将与读者共享突破安全机制的技术经验和专长。

本书第III部分由Stephen Sims撰写，浓墨重彩地描述最新漏洞攻击程序的编写方式。第14章使用主流Web浏览器中的最新漏洞，披露如何为“与栈相关的内存损坏”编写漏洞攻击程序，从而绕过内存保护。

对于有志于从事信息安全的人士而言，本书堪称一座熠熠生辉的资源宝库！

—Peter Van Eeckhoutte
Corelan Team (@corelanc0d3r)

《灰帽黑客(第5版)》是我苦苦追寻的至宝，我总是毫不犹豫地及时购买最新版本。网络安全领域在不断发展，为适应新威胁，信息安全从业人员必须掌握新术语和概念，了解最新的漏洞攻击技术，知识体系将变得十分庞大。本书作者都是各自领域的顶尖专家，将引领我们紧紧跟随安全趋势，书中介绍的红队操作、Bug赏金计划、PowerShell技术以及物联网和嵌入式设备都是我们必须掌握的新知识点。

—Chris Gates
Uber高级安全工程师

攻击技术数量空前，控制和保护机制也达到前所未有的高度。现代操作系统和应用程序在不断进步，对黑客攻击的防范能力令人印象深刻，但条件成熟时，黑客仍不时得手。本书呈现大量最新技术，分步详解漏洞，分析如何绕过ASLR和DEP控制。在大量实例的引导下，你将对最新的黑客攻击技术有更深刻的理解。

—James Lyne
Sophos全球安全顾问兼SANS Institute研发总监

纪念 Shon Harris

在本书前几个版本中，我都撰文怀念我的朋友、导师以及我最信赖的人Shon Harris。我从美国海军陆战队退役并开启新职业时，Shon是我的指路人，在同Shon一起工作的日子里，我们彼此合作愉快。长话短说，如果当初没有Shon Harris，就不会有本书；若不是Shon一路提携，我的职业生涯也无法取得卓越成就。我一直非常想念她，我谨代表本书其他作者说：我们爱你，你永远活在我们心中。如果你不了解Shon，你应当通过本书以及其他书籍阅读她的感人事迹。我们的头脑中都有Shon的鲜活记忆，一直因为有她这样的朋友而自豪，并愿意将她的故事讲给大家听。Shon是一个充满魅力的人，声誉斐然，赐予我们善意和慷慨！我们深深地怀念她。谨以本书表达对她的敬意和怀念之情。

——Allen Harper
本书第一作者，Shon Harris的朋友

谢谢母亲的辛勤哺育和精心培养，帮助我提高文字水平，使我成为一名作家。

——Ryan Linn

感谢爱妻LeAnne和女儿Audrey，谢谢你们的一贯支持！

——Stephen Sims

谢谢爱女Elysia无条件给予的关爱和支持，你在多个方面鼓励我前进，我也永远是你的坚强后盾和支持者。

——Linda Martinez

谢谢亲友们无尽的支持和帮助，让我的生活甜蜜幸福！

——Branko Spasojevic

感谢女儿Tiernan的支持，你不断提醒我享受生活并每天学习。希望你未来成为出色的人。

——Michael Baucom

感谢儿子Aaron带给我的爱，尽管我花了大量时间从事写作，也感谢我们在一起时共同分享的快乐。

——Chris Eagle

致　谢

本书所有作者都想表达对麦格劳-希尔教育集团(McGraw-Hill Education)的编辑们的谢意。尤其要感谢Wendy Rinaldi和Claire Yee，正是你们使我们步入了正轨，并在整个过程中给予了巨大帮助。你们崇高的职业精神和忘我奉献提高了出版社的信誉，感谢你们对这个项目的重要贡献！

Allen Harper：感谢爱妻Corann和两个美丽活泼的女儿Haley与Madison。感谢你们在我转行时给予的支持和理解。

我深深地爱着你们，Haley与Madison一天天地长大了，出落得美丽端庄，我备感自豪。感谢前雇主和目前的雇主。感谢Tangible安全公司的朋友们对我的帮助，让我过上更幸福的生活。谢谢利伯缇大学的师生们，有幸在这些年与你们共事，我校一定会培养出大量优秀人才！

Branko Spasojevic：感谢各位家庭成员——Sanja、Sandra、Ana Marija、Magdalena、Ilinka、Jevrem、Olga、Dragisa、Marija和Branislav，感谢你们的支持。生活在这样的书香门第，我备感荣幸。

还感谢所有乐于免费分享知识惠及他人的朋友们。需要特别提及的是Ante Gulam、Antonio、Cedric、Clement、Domagoj、Drazen、Goran、Keith、Luka、Leon、Matko、Santiago、Tory以及TAG、Zynamics、D&R和Orca的各位人士。

Ryan Linn：感谢Heather的支持、鼓励和建议，以及家人和朋友们的支持。这段时间因忙于写作而疏于与你们交流，感谢你们的长期忍耐。

感谢Ed Skoudis，若没有你的推动，我不可能完成这么棒的事情！还有HD、Egypt、Nate、Shawn以及其他所有在我最需要的时候伸出援手，提供代码协助、指导及支持的朋友和家人。

Stephen Sims：感谢我的妻子LeAnne和女儿Audrey，感谢你们一直以来对于我花费大量时间从事研究、写作、工作、教学及差旅的支持。

也要感谢父母George和Mary，以及妹妹Lisa，感谢你们的帮助。最后特别感谢通过论文、演讲和工具对社区建设贡献良多的那些才华横溢的安全研究者们。

Chris Eagle：感谢妻子Kristen的鼎力支持。没有你的支持，我将一事无成。

Linda Martinez：谢谢勤勉的父母，你们就是我的光辉榜样。感谢女儿Elysia多年来的支持，使我能投入事业，追逐梦想。

诚挚地感谢我的朋友以及一些行业精英，如Allen、Zack、Rob、Ryan、Bill和Shon。

Michael Baucom：感谢妻子Bridget和女儿Tiernan，为支持我的事业，你们默默付出了很多。

谢谢父母的爱和支持，你们给我灌输了做人的道理，培育了我的上进心，使我在事业方面取得了今天的成就。感谢美国海军陆战队给予我克服一切困难的信心。最后感谢同事兼好友Allen Harper。这个卓越的团队让我在工作中如鱼得水。

我们所有作者还要集体感谢Hex-Rays，感谢你们慷慨地提供了IDA Pro工具！

技术编辑简介

Heather Linn拥有逾20年的安全领域工作经验，曾在公司安全、渗透测试、威胁猎杀团队工作。Heather为Metasploit等开源框架做出贡献，曾在全球讲授取证、渗透测试和信息安全等课程，并为这些课程贡献资料。

Heather曾在多个技术会议上发表演讲，包括BSides、区域ISSA分会，并向信息安全领域的新生授课，帮助学生们了解现在，展望未来。

作者简介

Allen Harper博士，CISSP。Allen曾担任美国海军陆战队(Marine Corps)军官，2007年，在伊拉克之旅结束后退役。Allen拥有30年以上的IT/安全经验。Allen从Capella大学获得IT博士学位，研究方向是信息保障和安全；从海军研究生院(NPS)获得计算机科学硕士学位，从北卡罗来纳州大学获得计算机工程学士学位。Allen负责为Honeynet项目指导开发名为roo的第三代蜜墙CD-ROM。Allen曾担任多家《财富》500强公司和政府机构的安全顾问。Allen对物联网、逆向工程、漏洞发现以及各种形式的道德黑客攻击感兴趣。Allen是N2 Net Security有限公司的创始人，曾担任Tangible安全公司的执行副总裁和首席道德黑客。Allen目前担任利伯缇大学(位于弗吉尼亚州林奇堡市)网络卓越中心的执行总监。

Daniel Regalado(又名Danux)是一名墨西哥裔的安全研究员，在安全领域拥有16年以上的丰富经验，曾参与恶意软件、零日攻击、ATM、物联网设备、静脉注射泵和汽车信息娱乐系统的剖析和渗透测试。Daniel曾在FireEye和赛门铁克(Symantec)等知名公司工作，目前担任Zingbox的首席安全研究员。Daniel曾分析针对全球银行ATM的恶意软件攻击，获得多项发明，并因此成名，最著名的发明有Ploutus、Padpin和Ripper。

Ryan Linn在安全领域积累了逾20年的经验。曾担任系统编程人员、公司安全人员，还领导过全球网络安全咨询工作。Ryan参与过多个开源项目，包括Metasploit和Browser Exploitation Framework (BeEF)等。Ryan的推特账号是@sussurro，曾在多个安全会议(包括Black Hat、DEFCON)上发表研究报告，并为全球机构提供攻击和取证技术方面的培训。

Stephen Sims是一位业内专家，在信息技术和安全领域拥有逾15年的经验。Stephen目前在旧金山担任顾问，提供逆向工程、漏洞攻击程序开发、威胁建模和渗透测试方面的咨询。Stephen从诺威治大学获得信息保障硕士学位，是SANS机构的高级讲师、课程作者和研究员，编写高级漏洞攻击程序和渗透测试课程。Stephen曾在多个重要的技术会议上发表演讲，如RSA、 BSides、OWASP AppSec、ThaiCERT和AISA等。Stephen的推特账号是@Steph3nSims。

Branko Spasojevic是谷歌检测和响应团队的安全工程师。他曾在赛门铁克担任逆向工程师，并分析过各类威胁和APT组。

Linda Martinez是Tangible安全公司商业服务交付部门的首席信息安全官兼副总

裁。Linda是一位老道的信息安全执行官和业内专家，具有18年以上的管理技术团队、开拓技术业务范围以及为客户提供优质咨询服务的经验。Linda负责管理Tangible安全公司商业服务交付部门，业务范围包括：渗透测试(红队和紫队操作)，硬件攻击，产品和供应链安全，治理、风险管理和合规，应急响应和数字取证。身为首席信息安全官，Linda还为多家公司提供专家级指导。此前，Linda曾担任N2 Net Security的运营副总裁，曾参与创立信息安全研究和咨询公司Executive Instruments，并担任首席运营官。

Michael Baucom目前担任Tangible安全公司Tangible实验室的副总裁，曾参与多个项目，包括软件安全评估、SDLC咨询、工具开发和渗透测试。此前，Michael曾在美国海军陆战队担任地面无线电维修员。另外，Michael曾在IBM、Motorola和Broadcom担任多个职位，包括测试工程师、设备驱动程序开发人员以及嵌入式系统软件开发人员。Michael还担任Black Hat培训师，为本书提供技术建议，曾在多个技术会议上发表演讲。Michael目前的研究方向是渗透测试活动的自动化、嵌入式系统安全和手机安全。

Chris Eagle是位于加州蒙特利尔的海军研究生院(Naval Postgraduate School，NPS)计算机科学系的高级讲师。作为一位具有30年以上经验的计算机工程师及科学家，他曾撰写多本书籍，曾担任DARPA的Cyber Grand Challenge的首席架构师，经常在安全会议上发表演讲，为安全社区贡献了多个流行的开源工具。

Shon Harris(已故)令人无限怀念。Shon是Logical Security公司的总裁、一位安全顾问，曾担任美国空军信息战(U.S. Air Force Information Warfare)部队的工程师，也是一名作家、教育工作者。Shon撰写了畅销全球的《CISSP认证考试指南》(最新版本是第8版)以及其他多本著作。Shon曾为来自多个不同行业的各类公司提供咨询服务，也曾为广泛的客户讲授计算机和信息安全课程，这些客户包括RSA、Department of Defense、Department of Energy、West Point、National Security Agency (NSA)、Bank of America、Defense Information Systems Agency (DISA)和BMC等。Shon被*Information Security Magazine*评为信息安全领域25位最杰出的女性精英之一。

免责声明：本书中发表的内容均属作者个人观点，并不代表美国政府或这里提及的其他任何公司。

译者简介

栾浩，获得上海大学项目管理专业管理学学士学位，持有CISSP、CISA、CCSK、ISO 27001 LA和BS 25999 LA等认证，现任融天下互联网科技(上海)有限公司CTO及CISO职务，负责金融科技研发、业务安全及反舞弊、信息安全、数据安全和风控审计等工作，2015—2019年度(ISC)²上海分会理事。栾浩先生担任本书翻译工作的总技术负责人，负责统筹全书各项工作事务，并承担第1~10章的翻译工作，以及全书的校对、定稿工作。

毛小飞，毕业于湘潭大学计算机系，持有CISSP和ISO 27001等认证。现任京东集团企业信息化部安全技术负责人，负责渗透测试、病毒分析、安全产品开发和应急响应等工作。毛小飞先生负责本书第11~13章的翻译工作以及部分章节的校对工作。

姚凯，获得中欧国际工商管理学院MBA管理学硕士学位，持有CISSP、DPO、CISM、IAPP-FIP、CISP和CISA等认证。现任欧喜投资(中国)有限公司IT总监，全面负责IT及安全工作。姚凯先生负责第14~20章的翻译工作，以及部分章节的校对、统稿及定稿工作，并为本书撰写了译者序。

雷兵，获得同济大学海洋地质专业理学硕士学位，持有CISSP、CCSP、CISM、CISA和CEH等安全认证。现任安全专家，负责大数据相关安全工作。雷兵先生负责本书第21~23章的翻译工作，以及部分章节的统稿、校对及定稿工作。

王向宇，获得安徽科技学院网络工程专业工学学士学位，持有CCSK、CISP、CISP-A和软件开发安全师等认证，现任京东集团企业信息化部高级安全工程师，负责日常安全事件处置与应急、数据安全、安全监控平台开发与运营、云平台安全和软件开发安全等工作。王向宇先生负责本书第24和25章的翻译工作，以及部分章节的校对工作。

付晓洋，获得卡内基梅隆大学信息系统管理硕士学位。现任聚思鸿信息技术服务有限公司高级软件工程师，负责软件产品的技术设计、开发以及代码安全加固工作。付晓洋先生负责本书涉及开发及代码的章节的校对工作。

吴薇，获得北京邮电大学信息与计算科学专业理学学士学位，持有CISP、CCSE和RHCE等证书。现任中国航空结算有限责任公司高级网络工程师，负责网络架构设计、安全运营等工作，被授予中央企业技术能手、全国民航技术能手等多项荣誉称号。吴薇女士负责本书的全书校对工作。

邵德强，获得北京航空航天大学计算机科学与技术专业工学学士学位，持有

CISA、ISO 27001和CISP等认证。现任包商银行股份有限公司数据安全管理岗，负责公司的数据安全体系建设、系统与数据安全项目管控以及数据安全审计与合规等工作。邵德强先生负责本书部分章节的校对工作。

在本书的翻译及校对过程中，还有多位安全专家给予了帮助，包括卡巴斯基吕劼先生、廖勇博士、京东集团李继君先生以及顺丰集团张东先生等。最后，感谢(ISC)² 上海分会诸位技术专家对本书翻译过程的大力支持！