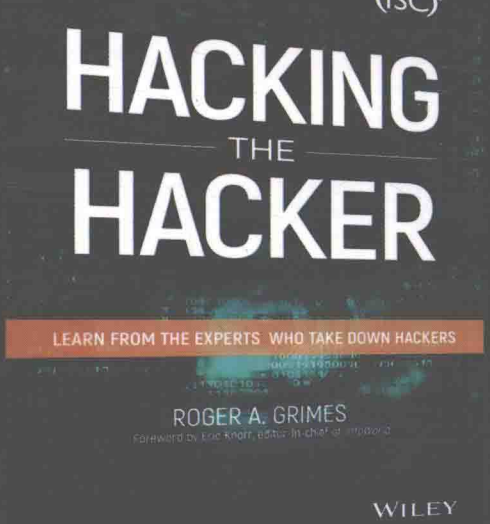
安全技术经典译丛

*InfoWorld*总编Eric Knorr作序推荐！

反黑客的艺术

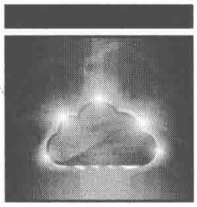
Hacking the Hacker:
Learn from the Experts Who Take Down Hackers



[美] 罗杰·格里姆斯 (Roger A. Grimes) 著
栾浩雷兵毛小飞 等译
北京爱思考科技有限公司 审

清华大学出版社

安全技术经典译丛



反黑客的艺术

[美] 罗杰·格里姆斯(Roger A. Grimes) 著
栾浩 雷兵 毛小飞 等译
北京爱思考科技有限公司 审

清华大学出版社
北京

Roger A. Grimes
Hacking the Hacker: Learn from the Experts Who Take Down Hackers
EISBN：978-1-119-39621-5

图书在版编目(CIP)数据

反黑客的艺术 / (美)罗杰 • 格里姆斯(Roger A. Grimes) 著；栾浩 等译. —北京：清华大学出版社，2019
(安全技术经典译丛)
书名原文：Hacking the Hacker: Learn From the Experts Who Take Down Hackers
ISBN 978-7-302-51526-5

Ⅰ. ①反…　Ⅱ. ①罗… ②栾…　Ⅲ. ①黑客—网络防御　Ⅳ. ①TP393.081

中国版本图书馆 CIP 数据核字(2018)第 254736 号

责任编辑：王　军　韩宏志
装帧设计：孔祥峰
责任校对：牛艳敏
责任印制：刘海龙

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：三河市龙大印装有限公司
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：10.375　　**字　　数**：279 千字
版　　次：2019 年 1 月第 1 版　　**印　　次**：2019 年 1 月第 1 次印刷
定　　价：98.00 元

产品编号：079455-01

译者序

本书主要介绍在安全行业具有影响力的一群国际知名道德黑客的人生历程。希望通过本书可让大家更好地了解“道德黑客”这个特殊群体：他们大多隐匿于网络世界，是技术高手，也是普通人。

“黑客”由英文单词“hacker”音译而来，狭义上指专门研究、发现计算机和网络漏洞的计算机爱好者，他们对计算机有着狂热的兴趣和执着的追求。道德黑客所做的不是恶意破坏，根据“开放源代码运动”领袖 Eric Raymond 的解释，“hacker”与“cracker”是分属两个不同世界的群体：“hacker”是有建设性的，而“cracker”则具有破坏性。

维基百科里“黑客”的定义是熟练的计算机专家，他们运用技术知识解决问题。虽然黑客可指任何熟练的计算机程序员，但“黑客”这个词承载了太多负面含义，让人联想到一群凭借自己的技术知识，利用漏洞攻击计算机系统，意在盗取客户信息、金钱或散布破坏性病毒的数字盗贼形象。

“hacker”的动词形式“hack”意为“劈、砍、辟出、开辟”，进一步引申为“干了一件非常漂亮的工作”。计算机黑客在自己熟悉的领域大显身手，个个都是编程高手。20 世纪 50 年代，无线电和

电子设备爱好者开始使用“黑客”一词，经过 60 年代麻省理工学院(MIT)铁路模型技术俱乐部(TMRC)的广泛使用而为人熟知。

1994 年，中国正式接入互联网。次年，“黑客”一词正式进入中国。网络上出现了《黑客入门教程系列》等文献，以道德黑客守则的形式传播黑客文件和黑客道德。最初的精神是“充分共享、充满激情、颠覆世界”，他们怀着乌托邦般纯真和美好的愿景。中国互联网的前身 CFIDO 就汇聚了诸多有理想、有道德底线、有技术追求和正义感的中国道德黑客。和现在不同，那时都依靠电话拨号方式接入网络，使用比 9600bps 还小的调制解调器，大家主要访问 BBS 站点，玩文字 mud 网络游戏，在原始网络中纵横驰骋。

1995—1996 年期间，中国各大中城市的互联网信息港已初具规模，中国互联网的第一代网管诞生，中国第一代的大众网民也开始走出 BBS，进入天地更广阔的 Internet。这两年是中国互联网初步成长时期，也是中国软件业蓬勃发展的时期。国内服务运营商开始实施优惠上网政策，互联网的发展进入普及阶段。

1997 年，中国道德黑客有了全球首个用于交流的中文黑客站点“绿色兵团”。希望“以兵团一般的纪律和规则，打造绿色和平的网络世界”。

1999 年中国互联网用户高速增长，同年电影《黑客帝国》热映，“黑客”一词在中国变得炙手可热。“安全焦点”“中国鹰派联盟”“中国黑客联盟”“小榕软件”“第八军团”“邪恶八进制”“黑客基地”“华夏黑客同盟”“中国红客联盟”也相继成立。

2011 年在上海举办的 COG 信息安全论坛上，中国道德黑客正式发布《COG 黑客自律公约》，阐述了道德黑客精神及文化精髓。很多人为践行道德黑客精神，为安全产业、社会乃至大众的福祉服务，转型成安全专家、企业的安全负责人。还有部分道德黑客创业打拼，建立网络安全帝国，通过安全服务继续实现理想，为大众服务。

(ISC)²作为国际知名的安全组织，一直关注并推动安全产业的发展。本书将揭示众多世界知名道德黑客的经历及经验总结。技术

工作者，特别是安全人员，阅读后会产生很多共鸣，拉近自己与世界知名道德黑客的距离。对于立志从事安全事业的未来道德黑客，此书将是一盏指路明灯。

北京爱思考科技有限公司(Beijing Athink Co., Ltd)特意组织力量将该书翻译出版，希望书中介绍的内容对读者深入了解道德黑客以及黑客世界能有所裨益。

这里衷心感谢本书的原作者和编辑们，是他们的支持和授权，才使这本书的中文版得以顺利出版；还要感谢(ISC)²中国办公室和清华大学出版社将本书引入中国，以飨广大安全行业的读者；更要感谢为这本书的出版和翻译工作付出大量艰辛劳动的各位译者，是他们的辛勤工作，才使中国读者得以近距离地了解世界知名黑客的传奇经历以及黑客道德和文化；最后感谢清华大学出版社的王军老师及编辑团队，他们在编辑过程中严格把关，提出详尽的修订建议，保证了本书的翻译质量。

最后，衷心希望广大读者从书中获益，并继续践行道德黑客精神、弘扬道德黑客文化，为中国的安全事业贡献力量。

译者简介

栾浩，现任融天下互联网科技(上海)有限公司首席技术官(CTO)及首席信息安全官(CISO)，持有 CISSP、CISA 和 ISO27001LA 等认证，担任本书翻译的技术负责人，负责统筹全书各项工作事务，并承担本书第 34、35、50 章的翻译工作。

雷兵，信息安全专家，持有 CCSP、CISSP、CISM、CISA 和 CEH 等认证，负责本书第 22、23、24 章的翻译工作以及全书部分章节的审校工作。

毛小飞，现任京东集团安全运营中心安全专家，持有 CISSP 和 ISO27001 等认证，负责本书第 14 章和第 28 章的翻译工作，以及全书的统稿和部分章节的审校工作。

姚凯，现任欧喜投资(中国)有限公司 IT 总监，持有 CISSP、CCSP、CSSLP、CISA 和 CEH 等认证，负责本书第 1~5 章的翻译，以及本书的通校工作。

王向宇，现任京东集团安全运营中心高级安全工程师。持有 CCSK、CISP、CISP-A 和软件开发安全师等认证。负责本书第 8 章和第 43 章的翻译工作，以及全书部分章节的审校工作。

顾伟，现任安进生物制药公司日本及亚太地区业务信息安全官，持有 CISSP、CCSP、CISA、CISM 和 CGEIT 等认证，负责本

书第 15~17 章的翻译工作。

赵锐，现任金融行业高级风控经理，持有 CCSK、CISM、CEH 和 PMP 等认证，承担本书第 21、25、48 章的翻译工作，并为本书撰写译者序。

吴潇，现任北京天融信网络安全技术有限公司专家级安全顾问，持有 CISSP、CISA、PMP 和 ISO27001 等认证，负责本书第 6、37、44 章的翻译工作。

张伟，担任北京初到科技有限公司 CEO 职务，持有 CISSP 和 ITIL(F)等认证，负责本书第 41、42、45、46、47 章的翻译工作。

蒋朝晖，现任花旗集团亚太区信息安全官，持有 CISSP 和 CISM 等认证，负责本书第 26 章和第 27 章的翻译工作。

周苏静，现任白墨子区块链安全实验室技术总监，持有 CISSP 等认证，负责本书第 12、32、36、38 章的翻译工作。

牛承伟，现任广州地铁集团有限公司基础架构主管，持有 CISP 等认证，负责本书第 30 章、第 39 章、序言和前言的翻译工作。

徐正伟，现任阿里巴巴集团安全运营专家。持有 ISO27001LA 等认证，负责本书第 18、19、20 章的翻译工作。

刘北水，现任中国赛宝实验室信息安全研究中心工程师，持有 CISSP、CompTIA 和 Security+等认证，负责本书第 29 章和第 33 章的翻译工作。

王威，现任上海市公安局安全领域工程师，持有 CISP 等认证，负责本书第 10、11、13 章的翻译工作。

马成明，现任北京微步在线科技有限公司华东区解决方案总监，持有 CISSP、CISA、CISM 和 CIPM 等认证。负责本书第 31、40、49 章的翻译工作。

危国洪，现任金融行业安全架构师，持有 CISSP 等认证，负责第 7 章和第 9 章的翻译工作。

还有多位安全专家在本书译校过程中给予了帮助，包括吕劼、廖勇、李继君、张东、洪恒艺、王瑞军、杨超、田方、赵欣、吴茜、赵沁泥、薛凯泽和樊开元等。

作者简介

罗杰·格里姆斯(Roger A. Grimes)于 1987 年进入安全领域，与恶意计算机黑客已经斗争了 30 多年。Roger 获得十几种计算机安全证书(包括 CISSP、CISA、MCSE、CEH 和 Security+)，甚至通过了与计算机安全无关的、极难的 CPA 考试。Roger 创立和更新了计算机安全教育课程，为数千名学生讲授攻防之道。Roger 经常在国际计算机安全会议上发表演讲。Roger 受雇对一些公司及其网站进行专业的渗透测试，每次都会在三小时内成功进入。Roger 独自撰写或参与撰写了 8 本关于计算机安全的书籍和近 1000 篇刊登在杂志上的文章。自 2005 年 8 月起，Roger 担任 *InfoWorld* 杂志的计算机安全专栏作家(http://www.infoworld.com/blog/security-adviser/)。Roger 担任全职的计算机安全顾问超过 20 年，为全球各类规模的公司提供如何阻止恶意黑客和恶意软件的建议。在漫长的工作经历中，Roger 认识到大部分恶意黑客不像大部分人想象的那么神奇，这些恶意黑客绝对没有大部分防卫者聪明。

致　谢

感谢 Jim Minatel 为这本我已构思了 10 年的书籍提供的指导，感谢 Kelly Talbot 编辑，Kelly 是我著书 15 年来遇到的最优秀编辑。Kelly 擅长在不改变作者原意的前提下修正问题。感谢 10 年之久的雇主——微软公司，这是我任职过的最佳公司。感谢 Bruce Schneier 的非正式指导。感谢 Brian Krebs 所做的调查性报道。感谢 Ross Greenberg、Bill Cheswick 以及其他将计算机安全知识写得妙趣横生的早期作者，你们是我的榜样，我将继续你们的事业。最后，我今天取得的成就离不开我家较好的作家——我的双胞胎哥哥 Richard Grimes，这 20 年里，哥哥一直鼓励我写作。另外，在此感谢每一位同行。

序　言

Roger A. Grimes 在计算机安全行业已经工作了 27 年，我有幸在 15 年前与 Roger 相识。Roger 是少数几个将安全理念融入骨髓的专业人士之一；他总能直接把握主题，另外，他拥有与坏人做斗争以及根除安全防御弱点的丰富经历，这些使得 Roger 成为唯一有资格撰写本书的人。

2005 年，Roger 以邮件方式写了一篇重量级文章，旨在批评一位安全作家的作品。这篇文章引起了我们的高度关注，于是立即邀请 Roger 为 *InfoWorld* 撰稿。此后一发不可收拾，Roger 迄今已为 *InfoWorld* 写了几百篇文章，所有文章都深入刻画了恶意黑客和防御者的心理，显示出 Roger 对安全主题的热爱。在 *InfoWorld* 每周的安全专栏中，Roger 尽情展现自己的过人天赋，总是关注实质性问题，而不是追逐短暂的威胁或过分炒作的新科技。很多机构一面倒地忽视基础，蜂拥追求时髦方案，而 Roger 则倾尽心力去说服安全防卫者和高管层去做正确的事情。

在本书中，Roger 介绍了一些在安全行业具有影响力的道德黑客。道德黑客通过不懈努力筑起一条坚固防线，以对付日益增多的攻击者。这些年来，攻击者的目标从破坏性损害转向偷盗珍贵知识

产权以及从金融机构和客户那里窃取数百万美元。我们欠了这些安全专家一笔巨债！在采访 Brian Krebs、Dorothy Denning 博士、Bruce Schneier 等专家的过程中，Roger 赞扬了他们的成就，写出一篇篇寓教于乐的短文。如果你对计算机安全感兴趣，或者是一位网络安全从业人员，本书将是你的良师益友。

InfoWorld 总编 Eric Knorr

前　言

此书旨在赞扬那些默默奉献的计算机安全防卫者。通过介绍全球最好的白帽黑客、防卫者、隐私保护者、教师和作家，希望大家读后会感激那些在幕后为我们今天的美好生活付出不懈努力的人们。如果没有这些人为我们保驾护航，那么计算机、互联网甚至是与之连接的所有设备都将失效。此书是对防卫者的赞美之书。

鼓励每位有意从事计算机工作的人士都考虑往计算机安全方向发展。也鼓励那些纠结于道德伦理的崭露头角的黑客从事计算机安全工作。通过打击恶意黑客及其开发的恶意软件，我过上了富裕的生活。我能以合乎道德和法律的方式，完成每个感兴趣的黑客攻击。成千上万的其他人也能做到这一点。在任意一个国家和地区，计算机安全都是最热门、收入最高的职业。我从这个职业收获颇丰，相信你也一样。

本书的大部分内容中会提供一章来概括一种具体的黑客操作风格，此后附上一个或多个在相应计算机安全防卫领域成就斐然的名人的小传。尝试选择各个行业传奇代表、杰出人物，甚至是只在小技术圈子内显露出卓越才华的人士。尝试选择美国和全球各地多个领域的学者、供应商、教师、管理人员、作家和自由从业者。希

望对计算机安全职业感兴趣的读者能怀着与这些名人一样的动机，帮助打造更安全的计算机世界。

为正确的事业奋斗！

目　录