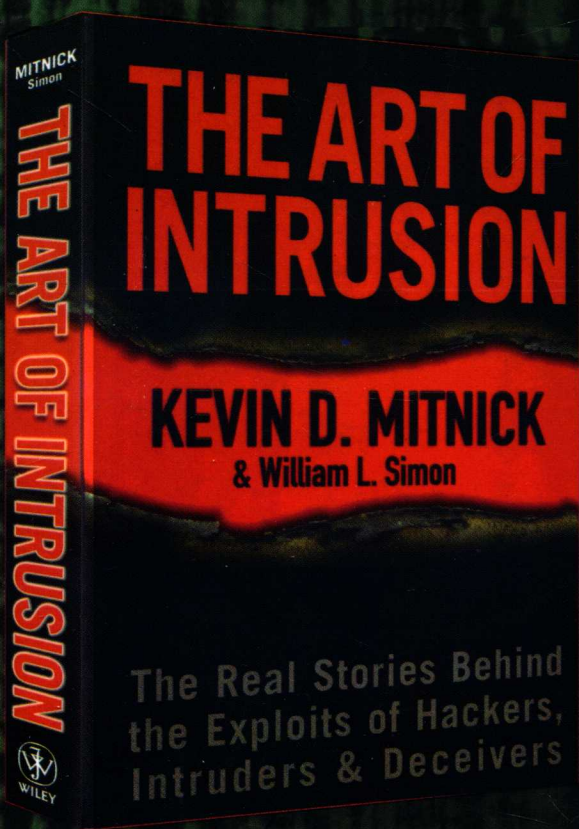


安全技术经典译丛

反入侵的艺术

——黑客入侵背后的真实故事



[美] Kevin D. Mitnick 著
William L. Simon
袁月杨 谢衡 译
潘爱民 审校



清华大学出版社

安全技术经典译丛

反入侵的艺术

——黑客入侵背后的真实故事

[美] Kevin D. Mitnick 著
William L. Simon 著
袁月杨 谢 衡 译

清华大学出版社

北 京

Kevin D. Mitnick, William L. Simon

The Art of Intrusion: the Real Stories Behind the Exploits of Hackers, Intruders and Deceivers
EISBN: 978-0-7645-6959-3

Copyright © 2005 by Kevin D. Mitnick & William L. Simon
All Rights Reserved. This translation published under license.

本书中文简体字版由 Wiley Publishing, Inc. 授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

北京市版权局著作权合同登记号 图字：01-2014-3256

Copies of this book sold without a Wiley sticker on the cover are unauthorized and illegal.

本书封面贴有 Wiley 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目(CIP)数据

反入侵的艺术——黑客入侵背后的真实故事/(美) 米特尼克(Mitnick, K. D.), (美) 西蒙(Simon, W. L.) 著; 袁月杨, 谢衡 译. —北京: 清华大学出版社, 2014
(安全技术经典译丛)

书名原文: The Art of Intrusion: the Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

ISBN 978-7-302-37358-2

I. ①反… II. ①米… ②西… ③袁… ④谢… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 159549 号

责任编辑: 王 军 韩宏志

装帧设计: 牛静敏

责任校对: 邱晓玉

责任印制: 宋 林

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: 三河市金元印装有限公司

经 销: 全国新华书店

开 本: 170mm×230mm 印 张: 16.25 字 数: 300 千字

版 次: 2014 年 9 月第 1 版 印 次: 2014 年 9 月第 1 次印刷

印 数: 1~4000

定 价: 49.80 元

译者序

Kevin D. Mitnick(凯文·米特尼克)曾是全球头号电脑黑客，其传奇黑客生涯是无人可比的；那时的他免费乘车、盗打电话，并驾轻就熟地出没于世界上最大几家公司的计算机系统。他自身的经历令人着迷，引人遐想。现在他将所采访的多个黑客的入侵公司、政府和组织的故事记录下来，并进行专业分析，与读者分享。书中涉及的人员包括在校学生、监狱囚犯、公司安全官员乃至政府执法人员等，事实上，其中多个故事的主角都将米特尼克奉为宗师。读者阅读本书时，总可将故事情节与自己所处的环境结合起来，体会到原来我们自己所用的计算机系统和物理安全措施就有不少安全漏洞。

作者的前一部著作 *The Art of Deception*(《反欺骗的艺术》)已经成为一本畅销书，其中阐述的一些技术手段和社会工程学知识已成为公司、政府以及国防信息安全等领域研究的热点，大学教授们经常引用这本书中的案例来充实现有理论。作为《反欺骗的艺术》的姊妹篇，本书所阐述的则是其他人的故事，我想，也只有作者这样的前黑客高手才可能采访到那些入侵者，让他们说出埋藏于心底多年的隐秘故事吧。

翻译本书时，我们时常感叹大千世界，无奇不有，这些黑客们所利用的技术、耐心和对社会工程学的娴熟运用常让我们叹为观止，拍案叫绝。

书中的故事和入侵过程引人入胜，匪夷所思。但为了防止有人模仿，作者有意在部分技术细节上对原过程进行了篡改，但这并不影响我们对本书所阐述的精髓的理解。

找一个舒适的场所，泡一杯龙井，慢慢品尝和感悟其中的美妙滋味吧！

译者

前 言

道高一尺，魔高一丈，聪明的黑客会利用黑客手段非法入侵我们公司的安全站点或个人系统。

另一方面，我们可以将黑客行为编成故事，让读者真切地了解黑客的入侵伎俩，做到知己知彼，有效地做好防范工作。由于这些故事让我和我的合作者 Simon 深信不疑，因此我就把这些故事都收集在本书中。

当我们为此书做采访时，也面临着一个颇为有趣的挑战，我们总是时不时地与被采访者做着斗智斗勇的游戏。对大多数记者和作家来说，确保故事的真实性是一件相当困难的事情：故事里的那个人真的是我们认为的那个人吗？这个人现在或曾经真的在他或她所说的那个机构工作过吗？这个人真的就职于他或她所说的那个工作岗位了吗？这个人有文件支持他的故事，我能证实这些文件的有效性吗？那些著名人士会相信这些故事，哪怕只是其中一部分吗？

核对黑客们的真诚比较棘手。在这本书里出现的大多数故事的主人公，并非那些已经锒铛入狱者，一旦他们的真实身份被揭示，他们将面临重罪指控。因此，故事里要求真实姓名，或者期待提供证据本身就是有争议的问题。

这些黑客向我讲述他们的故事是因为他们相信我。他们清楚我也曾是一名黑客，他们相信我不会出卖他们而使他们处于困境。然而，尽管存在风险，但许多黑客确实提供了一些有争议的证据。

尽管如此，有可能——事实上，很可能——一些黑客夸大了他们故事的细节以使故事更有说服力。或完全捏造故事，但其周围已出现的有力证据给他们敲响了“真相之铃”。

正因为存在这样的风险，所以我们一直在努力追求高度的可靠性。在采访过程中，我对每个技术细节提出质疑，对故事中任何不太合理的地方都要求他们清楚地解释，有时继续跟进，分析故事前后是否保持一致，或者看看他们第二次讲述时是否有差异。或者，如果此人被问及故事中被省略的难实现的步骤而“无法回忆”；或者，如果此人不太清楚自己先前声称做过的事情或无法解释他是如何从

地点 A 到地点 B。

除了有特殊说明外，本书中的每个故事都通过了我的“嗅觉检验”，我的合著者和我就此书中每一个故事的可信度都达成了一致。然而，为了保护黑客和受害者，我们常改动一些细节。在好几个故事里，我们虚拟了公司，修改了名称、行业和目标组织地点。从某种意义上讲，为了保护受害者的身份并防止模仿犯罪，我们给出了一些误导信息。但是，故事的性质和基本点还是准确的。

同时，由于软件开发和硬件厂商通过开发新产品和进行版本升级来不断修补安全性漏洞，因此在本书描述的事迹较少仍能产生作用。这样可能导致自以为是的读者认为不需要关注黑客，随着致命缺陷的揭露及纠正，读者和黑客所属公司没必要担心这些。但这些故事，无论是 6 个月前还是 6 年前发生的故事，都给人留下了深刻的教训，即黑客们每天都在发现新的脆弱点。阅读本书不是学习专业产品中的具体缺陷，而是要改变读者的态度，使之获得新的决心。

本书中有些故事令人震惊，有些故事开阔视野，有些故事使你为黑客的灵感而发笑。如果你是一位 IT 或安全专业人士，就能从每个故事中吸取教训以帮助你的公司加固安全。如果你并非技术人员，而只是对有关犯罪、胆大、冒险和公正朴实的故事感兴趣，那么你也可以从本书中获得乐趣。

致 谢

Kevin Mitnick

谨以此书献给我亲爱的家人和亲密的朋友，并且特别要感谢的是那些讲述故事的“黑帽”和“白帽”黑客们，他们使本书得以完成，并使我们从中受到教育和得到乐趣。

《入侵的艺术》这本书比我们写的上一部作品《欺骗的艺术》更具有挑战性，以往运用我们共有的创造才能构思一些奇闻佚事以说明社会管理的危害性，以及能够采取什么措施来缓解这些危险，与之相反，写本书时，我和 Simon 在很大程度上依靠采访以前的黑客、电话线路窃听者以及现已转变为安全专家的前黑客们，我们想写一本集犯罪悬疑和开拓视野于一体的书，从而帮助企业保护好其有价值的信息和计算机资源，我们坚信，通过揭露入侵网络和系统的黑客们的常用方法和技巧，很大程度上可以引导大众妥善应对技术性对手带来的风险和威胁。

我非常有幸与畅销书作家 Simon 一起致力于这本新书的写作，Simon 具有一个作家所拥有的卓越能力，能把黑客们提供的信息以通俗易懂的风格和方式表达出来，以至于祖母辈的老人都能看懂，更重要的是，Simon 已经不仅是我工作上的搭档，更是在整个写作过程中一直支持我的一位忠诚的朋友。虽然在写作过程中我们遇到过挫折并产生过分歧，但我们总能解决好这些问题并让双方都满意。大约两年后，政府的某些限制将会解除，我将可以完成和发表 *The Untold Story of Kevin Mitnick*。我期待着能和他在这个项目上继续合作。

Simon 的漂亮妻子 Argne Simon 的热心令我备感温暖，我感谢她过去三年里表现出的爱心、善良和大方。唯一遗憾是没能享用到她高超的烹饪技术，现在这本书终于完成了，也许我可以恳求她为我们做一顿庆功宴了！

由于我一直专注于本书的写作，一直没能花时间陪我的家人和朋友，我差不多成了一个工作狂，长期过着敲着键盘探索黑暗空间角落的日子。

我要感谢我深爱的女友 Darci Wood 和她那酷爱游戏的女儿 Briannah，她们对

这项耗时的工作表现出极大的耐心和支持，谢谢你们，宝贝！谢谢你们在我完成这项工作以及其他挑战性工作时对我的奉献和支持。

如果没有家人的支持和爱，这本书是不可能完成的。我的母亲和我的祖母在生活上给予我无私的爱和支持，我很幸运能被这样一位富有爱心和奉献精神的母亲所哺育，我也一直视母亲为最好的朋友。我的祖母就像我母亲一样，给予我只有母亲才能付出的养育和爱，她对于我的事业给予了非常大的帮助。有时我的事情和她自己的计划相冲突，但在任何情况下她总是优先考虑我的事情，哪怕这样做会为她带来不便。谢谢你，在我需要你的任何时候，你总是帮助我完成这项工作！她们极富爱心和同情心，总是教育我关心他人，对不幸的人伸出援手，通过学习她们付出和关心的方式，在某种意义上，我也紧跟上了她们的步伐。在写书过程中，我总是以工作和交稿期限为借口推迟了许多去探访她们的机会，我希望她们能够原谅我把她们放在了次要位置上。如果没有她们源源不断给予的爱护和支持，这本书就不可能完成，我将永远把这份爱深藏在心中。

我多么希望我的父亲 Alan Mitnick 和哥哥 Adam Mitnick 活得长久些，能和我一起打开香槟庆祝我的第二本书首次在书店上架。作为一名业务员和老板，我的父亲教我认识了许多美好的东西，我将终生铭记在心。

妈妈已故的男友 Sweve Knittle，在过去 12 年里，一直充当着父亲的角色，当我知道你总在我无法照顾母亲时照顾着她，我得到了莫大的安慰。你的去世深深地影响了我的家庭，我们怀念你的乐观幽默、爽朗笑声以及对家庭付出的爱。愿你安息吧！

我的婶婶 Chickie Leventhal 永远在我心中占据着特殊位置，过去数年里，我们家庭关系得到加强，彼此间的交流也很好，每当我需要建议或者需要一个地方停留时，她总给予我爱护和支持，在我全身心投入写书期间，我错过了很多机会去参加她、表妹 Mitch Leventhal 和男友 Robert Berkowitz 博士的家庭聚会。

我的朋友 Jack Biello 是一个充满爱心的人，他总是站出来为我说话，极力反对我在记者和政府检察官那里所受到的极不公平的待遇。在自由凯文运动中，他是一位重要人物，他同时也是一位作家，文笔非凡，擅长写有说服力的文章，揭露政府不让人们了解的真相。Jack 总为我挺身而出，毫不畏惧，和我一起准备演说稿和文章。在某些时候还充当我的媒体联络员。当我完成书稿《反欺骗的艺术》一书时，Jack 的去世使我非常失落和悲伤，虽然事隔两年，但 Jack 一直活在我心中。

我的密友 Caroline Bergerdn 一直非常支持我能在这部作品上取得成功。她很美丽，即将成为一名有前途的律师。她家住 Great White North，我和她是在维多利亚的一次演讲中认识的。我们很有缘。她发挥她的专长，校对、编辑、修正 Alex Kasper 和我举办的社会管理研讨会的一些事项。谢谢你，Caroline！

Alex Kasper 不仅是我最好的朋友，也是我的同事，目前我们正在举办为期一天或两天的研讨会，这是关于公司如何认识和防范社会管理袭击的研讨会。同样在洛杉矶 KFI 电台，我们一起主持了一档非常受欢迎的网络电台脱口秀节目“The Darkside of the Internet”。你是一位伟大的知己，谢谢你的宝贵意见和帮助，你超乎常人的善良和宽容一直积极地影响我，使我受益颇多。

Paul Dryman 是一位我们全家深交多年的朋友，是先父的好友。我父亲去世后，Paul 一直充当着父亲的角色。他总是很乐意帮助我，并和我交流想法。Paul，谢谢你这么多年来对父亲和我一如既往的无私友情。

Amy Gray 在过去三年里将我的演讲事务打理得井井有条。我不只欣赏和尊敬她的人格，而且高度评价她尊重人和礼貌待人的行为。你的支持和敬业使我成功地成为一名公众演说家和教练。非常感谢你不断的友情支持和对完美的追求。

在我和政府多年的对抗期间，律师 Gregory Vinson 一直是我智囊团中的一员。他为我写辩护书的日子，我们风雨同舟，一起经历了许多。目前，他是我的事务律师，每天不断地与我就新合同签订和新业务洽谈而辛勤地工作着。感谢你强有力的支持和辛勤的工作，特别是在紧急情况下获得了你的帮助！

Eric Corley(他的另一个名字是 Emmanuel Goldstein)是一位交往了十多年的密友，他一直积极地支持我。总是关心我的切身利益，当我被 Miramax 电影公司和一些记者丑化时，他总站出来为我公开辩护。当政府起诉我时，他也一直帮我走出困境，我无法用言语赞美你的好心、慷慨和友情。谢谢你，我忠诚而又值得信赖的朋友！

Steve Wozniak 和 Sharon Akers 长时间援助并帮助我走出困境。非常感谢你们为了支持我而频繁变更计划。有你们两个这样的朋友让我备感温暖。我希望，一旦这本书完稿，我们将有多一些时间聚会。Steve，我绝不会忘记那次你、Jeff Samuels 还有我一起开着你的越野车连夜赶到拉斯维加斯的 DEFCON 的历程，一路上我们轮流驾驶，那样我们就都可以通过 GPRS 无线连接方式用电子邮件与朋友聊天了。

我意识到，我要向很多人表示感谢，并对他们为我提供的爱心、友谊和支持

表示感激。但我无法一下子想起近年来所有遇到的慷慨相助之士的名字。可以说，我需要一个大容量的 U 盘来存储他们的名字，因为有这么多来自世界各地的人写信为我打气，给予支持。他们的鼓励对我意义重大，尤其在我最需要他们的时候。

我特别感谢我所有的支持者。他们站在我这一边，花费他们许多宝贵的时间和精力争取任何一个有可能倾听他们心声的人。对我受到的不公平待遇表示关切，为我受到那些企图从“Kevin Mitnick 神话”中牟利的人的中伤而感到愤怒。

衷心感谢那些出现在我职业生涯中用他们特殊的方式为我付出的人。David Fugate，他是 Waterside Productions 的员工，我的代理书商，在签订合同书前后多次因为我而被监禁。

非常感谢 John Wiley & Sons 给我写此书的机会，以及他们对我写出畅销书能力的信赖。我要感谢下面所有 Wiley 集团的人，他们使我梦想成真：Ellen Gerstein、Bob Ipsen 以及 Carol Long，他总是乐意回答我的问题并给予关注（我与他在 Wiley 签署了第一份合同，他当时是执行编辑）。还有 Emilie Herman 和 Kevin Shafer（技术编辑），他们和我构成一个团体，共同致力于完成这份工作。

我有很多与律师打交道的经历，但我希望在这里留一席之地向他们表达谢意，多年来，当与刑事司法制度发生不良互动时，他们对我嘘寒问暖，关怀之至，从言语上的问候直到深入案件中，我遇到了许多律师，他们与律师一贯的自我为中心的职业形象完全不一样，我尊重、钦佩、感谢这么多人毫无保留地给予我的慷慨支持和善意关心，他们每个人都值得用一段文字来感谢，至少我要提到他们所有人的名字：Greg Aclin、Fran Campbell、Lauren Colby、John Dusenbury、Sherman Ellison、Omar Figueroa、Jim French、Carolyn Hagin、Rob Hale、David Mahler、Ralph Peretz、Alvin Michaelson、Donald C. Randolph、Alan Rubin、Tony Serra、Skip Slaters、Richard Steingard、Honorable Robert Talcott、Barry Tarlow、John Yzurdiaga 和 Gregory Vinson。

其他家庭成员、朋友和生意合伙人也为我提供了建议和支持，在许多方面伸出援手，有必要认识和感谢他们。他们是 JJ Abrams、Sharon Akers、Matt “NullLink” Beckman、Alex “CriticalMass” Berta、Jack Biello、Serge、Susanne Birbrair、Paul Block、Jeff Bowler、Matt “404” Burke、Mark Burnett、Thomas Cannon、GraceAnn、Perry Chavez、Raoul Chiesa、Dale Coddington、Marcus Colombano、Avi Corfas、Ed Cummings、Jason “Cypher” Satterfield、Robert Davies、Dave Delancey、Reverend Digital、Oyvind Dossland、Sam Downing、John Draper、Ralph Echemendia、Ori Eisen、

Roy Eskapa、Alex Fielding、Erin Finn、Gary Fish、Fishnet Security、Lisa Flores、Brock Frank、Gregor Freund、Sean Gailey、Jinx 全体人员、Michael、Katie Gardner、Steve Gibson、Rop Gonggrijp、Jerry Greenblatt、Thomas Greene、Greg Grunberg、Dave Harrison、G. Mark Hardy、Larry Hawley、Leslie Herman、Michael Hess、Roadwired 全体人员、Jim Hill、Ken Holder、Rochell Hornbuckle、Andrew “Bunnie” Huang、Linda Hull、Steve Hunt、IDC 主要成员、Marco Ivaldi、Virgil Kasper、Stacey Kirkland、Erik Jan Koedijk、Lamo 一家、Leo、Jennifer Laporte、Pat Lawson、Candi Layman、Arnaud Le-hung、Karen Leventhal、Bob Levy、David、Mark Litchfield、CJ Little、Jonathan Littman、Mark Loveless、Lucky 225、Mark Maifrett、Lee Malis、Andy Marton、Lapo Masiero、Forrest McDonald、Kerry McElwee、Jim “GonZo” McAnally、Paul、Vicki Miller、Elliott Moore、Michael Morris、Vincent、Paul、Eileen Navarino、Patrick、Sarah Norton、John Nunes、Shawn Nunley、Janis Orsino、Tom Parker、Marco Plas、Kevin、Lauren Poulsen、Scott Press、Linda、Art Pryor、Pyr0、John Rafuse、Mike Roadancer、HOPE 2004 安全团队、RGB、Israel、Rachel Rosencrantz、Mark Ross、Bill Royle、William Royer、Joel “ch0l0man” Ruiz、Martyn Ruks、Ryan Russell、Brad Sagarin、Martin Sargent、Loriann Siminas、Te Smith、Dan Sokol、Trudy Spector、Matt Spergel、Gregory Spievack、Jim、Olivia Sumner、Douglas Thomas、Cathy Von、Ron Wetzal、Andrew Williams、Willem、Don David Wilson、Joey Wilson、Dave、Dianna Wykofka 以及 Labmistress.com 和《2600》杂志的所有朋友和支持者。

William L. Simon

在我们写《反欺骗的艺术》一书时，我和 Kevin Mitnick 结下了友谊，我们一起不断发现新的工作方法，同时加深了彼此间的友谊，所以我最先要感谢的就是他，在我们共同的第二次旅程中一位杰出的“旅途伴侣”！

Duid Fugate，我的 Waterside Productions 的经纪人，他首先把我和 Kevin 带到一起合作，挖掘出他的耐心和聪明才智，以寻求解决那些已出现的少见的不良状况。当情况日趋严峻时，每个作家应该有一位像朋友一样明智而又好心的经纪人。同样我不得不提及另一位多年的朋友——Bill Gladstone，Waterside Productions 的创始人和我的主要执行伙伴。Bill 是我成功写作生涯中的一位重要人物，我将永远感激他。

我的妻子 Arynne 用她的爱心和对完美的追求孜孜不倦地激励我，让我每天都

能有勇气重新开始。我无法用言语来表达对她的感激。她聪明并且直言不讳地指出我写作中的不足，这样使我的写作水平不断提高。有时我对她的建议反唇相讥，让她气愤不已，但她还是平息了愤怒，最终我也接受了她明智的建议并做了修改。

Mark Wilson 给予我很大的帮助。Emilie Herman 是一位资深编辑。接替 Emilie 工作的 Kevin Shafer 的力量也不能忽视。

到写第 16 本书时我已欠下了太多人情，他们一路上对我的帮助真可谓不小。这些人中，我特别要提到 Waterside 公司的 Kimberly Valentini 和 Maureen Maloney，以及 Josephine Rodriguez。Marianne Stuber 通常做快速转译工作(处理那些陌生的术语以及黑客俚语可不是件容易的事情)，Jessica Dudgeon 保持办公室工作有条不紊。Darci Wood 则帮助 Kevin 安排时间，以保证他能按时完成。

特别感谢女儿 Victoria 和儿子 Sheldon 对我的理解，同时感谢我的双胞胎外孙 Vincent 和 Elena，我相信一旦这本书稿完成，我就能经常和他们见面了。

Kevin 和我都十分感谢那些给我们提供故事的人，特别是其故事被我们采用的那些人。尽管风险很大，但他们仍然讲述了自己的故事。他们的身份一旦被暴露，很可能面临被气愤难平的人攻击的危险。有些人勇敢地讲出了他们的故事，虽然没有被采用，但他们确实是值得钦佩的。

目 录

第 1 章 赌场黑客轻取百万美金	1
1.1 研究	2
1.2 黑客技术日趋成熟	4
1.3 重写代码	6
1.4 重回赌场——进入实战	8
1.5 新方法	11
1.6 发起新一轮的攻击	12
1.7 落网	15
1.8 结局	17
1.9 启示	18
1.10 对策	19
1.11 小结	20
第 2 章 当恐怖分子来袭时	21
2.1 恐怖主义者投下诱饵	23
2.2 今晚的猎物：SIPRNET	26
2.3 令人担心的时刻来了	27
2.4 Comrade 被捕	28
2.5 调查 Khalid	30
2.5.1 恐怖组织 Harkatul-Mujahideen	32
2.5.2 9·11 以后	32
2.5.3 入侵白宫	33
2.5.4 结局	37
2.5.5 5 年以后	38
2.5.6 到底有多刺激	39
2.6 启示	40
2.7 对策	42
2.8 小结	44

第3章 来自德克萨斯监狱的入侵	45
3.1 监狱里：认识了计算机.....	45
3.2 不一样的联邦监狱.....	47
3.3 William 获取“城堡”钥匙.....	47
3.4 安全上网.....	49
3.5 解决方法.....	50
3.6 差点被抓.....	52
3.7 千钧一发.....	53
3.8 成长历程.....	54
3.9 重返自由世界.....	55
3.10 启示.....	57
3.11 对策.....	58
3.12 小结.....	61
第4章 警方与入侵黑客的较量	63
4.1 入侵电话系统.....	64
4.2 入侵法院计算机系统.....	65
4.3 旅馆来客.....	66
4.4 大门开启.....	67
4.5 守卫.....	69
4.6 处于监视之中.....	72
4.7 包围.....	74
4.8 过去.....	74
4.9 登上新闻节目.....	75
4.10 被捕.....	75
4.11 好运不再.....	76
4.12 入侵监禁所电话系统.....	77
4.13 打发时光.....	79
4.14 他们目前的工作状况.....	80
4.15 启示.....	80
4.16 对策.....	81
4.17 小结.....	82

第 5 章 黑客中的绿林好汉	83
5.1 援救	83
5.2 个人历史回顾	84
5.3 午夜会面	85
5.4 入侵美国电信巨头 MCI Worldcom	90
5.5 在微软公司内部	90
5.6 英雄, 但非圣人: 攻击《纽约时报》	91
5.7 Adrian 的过人之处	96
5.8 唾手可得的信息	98
5.9 这些日子	98
5.10 启示	100
5.11 对策	100
5.12 小结	103
第 6 章 渗透测试中的智慧与愚昧	105
6.1 寒冬	106
6.1.1 初次会晤	106
6.1.2 基本规则	107
6.1.3 攻击	108
6.1.4 灯火管制	111
6.1.5 语音信箱泄漏	112
6.1.6 最终结果	112
6.2 惊险游戏	113
6.2.1 结合的规则	114
6.2.2 计划	115
6.2.3 攻击	116
6.2.4 工作中的 IOphtCrack	117
6.2.5 访问	118
6.2.6 报警	119
6.2.7 幽灵	120
6.2.8 未遭遇挑战	121
6.2.9 暖手游戏	121
6.2.10 测试结束	122
6.3 回顾	123

6.4	启示	123
6.5	对策	124
6.6	小结	125
第7章	银行是否绝对可靠	127
7.1	遥远的爱沙尼亚	127
7.1.1	Perogie 银行	129
7.1.2	个人观点	130
7.2	远距离的银行黑客	131
7.2.1	黑客是学出来的, 不是天生的	131
7.2.2	入侵银行	133
7.2.3	你对瑞士银行账户感兴趣吗	135
7.2.4	结局	136
7.3	启示	136
7.4	对策	137
7.5	小结	138
第8章	知识产权并不安全	141
8.1	为时长达两年的黑客攻击	142
8.1.1	一颗探险之星	143
8.1.2	CEO 的计算机	146
8.1.3	入侵 CEO 的计算机	146
8.1.4	CEO 发现了黑客入侵	148
8.1.5	获取应用程序的访问权	149
8.1.6	被人察觉	151
8.1.7	返回敌方领地	152
8.1.8	此地不再留	152
8.2	Robert, 垃圾邮件发送者之友	153
8.2.1	获取邮件列表	154
8.2.2	色情作品盈利颇丰	155
8.2.3	Robert 是条汉子	156
8.2.4	软件的诱惑	157
8.2.5	发现服务器名称	158
8.2.6	Helpdesk.exe 的小帮助	159

8.2.7	黑客的锦囊妙计：“SQL 注入”攻击	161
8.2.8	备份数据的危险	165
8.2.9	口令观测	167
8.2.10	获取完整访问权限	167
8.2.11	把代码发回家	168
8.3	共享：一个破解者的世界	169
8.4	启示	172
8.5	对策	173
8.5.1	公司防火墙	173
8.5.2	个人防火墙	173
8.5.3	端口扫描	174
8.5.4	了解你的系统	174
8.5.5	事故应变和警告	175
8.5.6	检查应用程序中经过授权的改动	175
8.5.7	许可	175
8.5.8	口令	176
8.5.9	第三方软件	176
8.5.10	保护共享空间	177
8.5.11	避免 DNS 猜测	177
8.5.12	保护 Microsoft SQL 服务器	177
8.5.13	保护敏感文件	177
8.5.14	保护备份	178
8.5.15	免遭 MS SQL 注入攻击	178
8.5.16	利用 Microsoft VPN 服务	178
8.5.17	移除安装文件	179
8.5.18	重命名管理员账户	179
8.5.19	让 Windows 更健壮——避免存储某些凭证	179
8.5.20	深度防御	179
8.6	小结	180
第 9 章	人在大陆	183
9.1	伦敦的某个地方	183
9.1.1	潜入	184
9.1.2	映射网络	185