Mc Graw Hill Education

网络安全机密与解决方案

Network Security Secrets & Solutions

HACKING EXPOSED

"像所有经典著作一样，本书经受住了时间的考验：还是那么一语中的，还是那么一针见血，还是那么必不可少。第5版必将成为现代计算机网络和计算机系统安全专业人士的Bible。"

——Peiter Mudge Zatke
前白宫国会顾问，L0phtCrack的作者
@stake和Intrusic的奠基人

第5版

黑客大曝光

[美] Stuart McClure　Joel Scambray　George Kurtz　著
王吉军　张玉亭　周维续　译

Mc Graw Hill
清华大学出版社

网络安全机密与解决方案

黑客大曝光

（第5版）

【美】Stuart McClure, Joel Scambray
George Kurtz 著
王吉军 张玉亭 周维续 译

清华大学出版社 McGraw Hill Education

Stuart McClure，Joel Scambray，George Kurtz
Hacking Exposed Fifth Edition:Network Security Secrets & Solutions
EISBN 0-07-226081-5

图书在版编目（CIP）数据

黑客大曝光：网络安全机密与解决方案：第 5 版/
（美）麦克卢尔（McClure, S.），斯卡姆布智（Scambray, J.），
库尔茨（Kurtz, G.）著；王吉军，张玉亭，周维续译，－5 版，
－北京：清华大学出版社，2006
书名原文：Hacking Exposed Fifth Edition : Network Security Secrets & Solutions
ISBN 7-302-12259-8

Ⅰ. 黑…　Ⅱ. ①麦…②斯…③库…④王…⑤张…⑥周…
Ⅲ.计算机网络—安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 152394 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：刘秀青　陈洁
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：**43.75　　**字数：**956 千字
版　　次：2006 年 4 月第 1 版　　2006 年 4 月第 1 次印刷
书　　号：7-302-12259-8/TP・7882
印　　数：0 001~4 000
定　　价：78.00 元

内 容 提 要

《黑客大曝光》一书享誉全美，被信息安全界奉为圣经，号称信息安全第一书。作者独创“黑客大曝光方法学”，从攻防两方面系统阐述了最常见的黑客入侵手段及对应的防御策略。

作者秉承前 4 版的一贯写作风格，开篇即以“踩点”、“扫描”、“查点”三部曲，拉开黑客入侵的序幕。之后，作者拨冗去繁，从系统、网络、软件三个方面对黑客攻击惯用手段进行剖析：“系统攻击”篇针对 Windows、UNIX 系统攻击给出精辟分析，并覆盖最新热门主题远程连接和 VoIP 攻击；“网络攻击”篇全面展示无线攻击技术和手段、防火墙攻击和拒绝服务攻击；“软件攻击”篇则引入全新概念——应用程序代码攻击，详细解释源代码泄露、Web 应用程序攻击等最新黑客技术手段。全书结合多个生动案例，环环相扣，引人入胜，读者如临其境。

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，是信息系统安防人士的宝典，也可作为信息安全相关专业的教材教辅用书。

献给我的家人，你们的爱和宽容时时提醒我自己是多么幸福。

——Stuart

献给所有为美国利益而战的勇士们。

——Joel

献给我最爱的妻子 Anna 和儿子 Alex，是你们给予我灵感、指引和永恒的支持。献给我的母亲，是您帮助我锤炼了性格，教我如何战胜逆境。

——George

译者推荐

信息和网络安全技术经过近十年来的发展，在广度和深度上已经有了很大的进步，其中一个重要的研究趋势就是注重攻、防结合，追求动态安全。反映在信息安全技术的研究上，形成了两个完全不同的角度和方向。一个角度是从正面防御的方面考虑，研究加密、鉴别和认证、授权和访问控制等等；另一个角度是从反面攻击的方面考虑，研究漏洞扫描评估、入侵检测、紧急响应、防病毒等等。不管从事哪方面研究，以平和的心态、深入地了解另一方面的思路和方法是相当有益的。

然而，与此相关的信息安全研究著作和书籍却大多数都是从防御的角度论述的。从学习信息安全知识的角度看，我们不仅需要了解防御方面的技术，也需要深入了解检测和响应环节的技术。信息安全技术与应用的实践证明：最大的不安全就是自以为安全。安全策略的制定、安全技术的采用和安全保障的获得很大程度上要取决于对安全威胁的把握。因为信息安全工作具有很强的对抗性，威胁时刻存在；各种各样的安全问题常常会掩盖在表面的平静之下。“隐患险于明火”、“知己知彼、百战不殆”等古训对于网络空间的安全防御依然教益匪浅。对于潜在威胁的了解，对于攻击者手法的洞悉，对于自身脆弱性的意识，都是自身安全的前提。

《黑客大曝光》是近年出版的一本从攻击角度论述信息安全的畅销书。它用类似《简氏百科全书》的方式，将网络黑客年的技法和兵器一一罗列，细加盘点。作者告诉你 UNIX 的配置是如何被篡改的，Windows NT 的注册密钥是怎样被窃换的，可以对 NetWare 的设置做些什么手脚等。作者虽然无意批评现实主流厂商的产品，但却毫不隐讳地指出了众多产品的缺陷与不足。尤其值得一提的是，作者从攻防兼备的角度，将纷繁复杂、似是而非的攻防思路解释、分析

得明明白白。相对于第 1 版而言，本版在内容上做了及时更新，在“蜜罐”和 Windows 2000 公开安全漏洞方面，在邮件病毒、分布式拒绝服务攻击与路由协议有关的攻击方面，增添了不少精彩的内容。

黑客入侵技术不会因为我们不去了解它而不复存在；黑客们也不会因为我们不去学习、不去掌握抗击技术和工具而放弃对“手无寸铁”者的攻击。网络安全的保卫者力争不要落在犯罪分子后面。我们需要在知识的获取上与黑客比速度，如果能够先于攻击者之前了解这些知识，那么我们的安全就会更加有保障。他山之石，可以攻玉。从这个意义上讲，《黑客大曝光》是一本很好的、生动的、鲜活的教材，我们乐意将它推荐给广大的信息安全从业人员学习和参考。

译 者

2006 年 2 月

序　言

因特网是一个脆弱的生态系统，没有什么人能够确保赢得胜利。作为一家全球性的信息安全技术公司的总裁，我曾经亲眼目睹Nimda、Blaster和Fun Love等蠕虫像纳粹德国发动的闪电战那样洗劫了无数的公司。在这类攻击活动刚爆发时的关键而又混乱的几个小时里，全世界的信息安全专家都在争分夺秒地分析有关代码。在攻击爆发时，企业的信息安全人员和软件厂商的研究团队紧急行动起来，每一条尚可信赖的通信通道都充斥着仍在安全地带和已经蒙受不幸的人所发出的消息。

对于我们这些身处旋涡中心的人来说，整个过程既紧张刺激又有一丝担忧和害怕。在最初的几分钟里，我们每个人都在担心能否阻止这场灾难。还好，到目前为止，所有的攻击活动在几个小时之后都无一例外地得到了控制，而人们的注意力也开始转向收拾残局和防范类似攻击手段的变体。在一个星期之内，信息安全团队找出了问题的根源并提出了最终的解决方案，大家走出机房喝点儿啤酒庆祝一下，然后回家美美睡上一觉。

到目前为止，正义者赢得了每一场胜利，战局也似乎在按照我们所预期的方向发展。身边的非技术型业务总裁已经变得习惯于赢得这种网络世界的胜利。他们对自己的信息安全团队非常有信心，毫不吝啬地在他们身上花费大笔的金钱。有不少人认为已经取得的胜利将一直延续下去——还有什么可以阻止我们继续“赢”下去呢？但偶尔也会有几个有远见的执行官自问：“我该如何向董事会成员解释未来的风险？我们真的能继续把这类损失控制在最低限度吗？”

我有时会向这些执行官推荐由Weaver、Paxson和Staniford撰写的分析文章“How to Own the Internet in Your Spare Time”（如何在你们的业余时间里主宰因特网）。这篇文章的结论是“编写得更巧妙的计算机蠕虫有可能在几分钟甚至几十秒钟内传播开来，而其控制、修改和演变方式或许会有无穷多种可能性，它们将对各种网站和网络构成永远的潜在威胁”。我们真的不清楚未来会遇到哪些风险，因为黑客技术和黑客组织正在以惊人的速度发展。我们能够采取的最佳措施是深入了解这种风险并确保投资能够减少这种风险。

有了这种清醒的认识，下一个问题就是，最需要做哪些事情才能继续赢下去？作为一名供应商方面的总裁，我会因为我本人追求最新技术的情结而向执行官推荐下面这句话：

第一，我们需要继续投资我们的技术人员；第二，我们需要了解哪些东西对各项业务的正常运转是必不可少的。

我的推荐答案提到了两个需要，而你们手里的这本书解决了第一个需要并为第二个需要做好了准备。熟悉各种潜在的攻击机制是非常关键的，《黑客大曝光》第5版可以说是这方面的权威著作。潜在的安防漏洞和攻击手段可能千变万化，本书前几个版本的读者可以从这本书里发现关于各种新型攻击手段的新见解。我想利用这个机会向企业的技术经理提出这样一个建议：每年至少要带领你手下的技术人员参加一个这类内容的技能培训并通过集体讨论和实际应用等方式不断地强化这方面的知识和技能。

至于将为技术人员学习本书而支付金钱的业务经理，我的建议是一定要大力支持这种学习，因为这可以让技术团队的知识技能水平得到难以置信的提高。企业的技术团队必须了解信息攻防战的全貌，这包括各种安防漏洞、各种攻击机制、本企业的信息安防漏洞一览表、本企业需要保护的信息资产的商业价值，等等。只有把所有这些因素汇集在一起，企业才能以一种让董事会满意的方式管理好自己的风险并在日常工作中真正做好防范黑客攻击的准备工作。据我所知，其他类别的IT专著都没有像本书这样全面地对防范黑客攻击所需的技术知识、信息资产的商业价值以及企业的组织结构做出论述。

现代的信息安全技术，尤其是入侵防御技术，对企业建立自己的信息安全防线有巨大的帮助作用。如果没有一套制度化的策略和流程以及相应的技术支持，就不可能在“噩梦成真”的时候做出正确的响应。但是，如果在人才方面没有厚实的储备，技术再先进、策略和流程再细致，也不能发挥其真正的价值；而经过培训的信息安全专家无疑是这种人才基础的柱石。据我所知，过去发生的网络攻击活动从未导致过人员生命或健康的损失。但因特网这个生态系统每天都在进化，如果不出所料，经由因特网传输的VoIP将在几年之内成为人们进行语音通信的主要手段。网络技术的发展使得人们对网络的依赖程度日益增加，这种依赖反过来又进一步促进了网络技术的发展，但是，网络技术的发展也提高了网络的威胁和风险程度。也许过不了多久，你们拨打的911求助电话或在某个寒冷的冬夜拨打的暖气报修电话能否接通就要看因特网的脸色了。

很明显，人们对网络的依赖程度在一天天增加，而来自网络的威胁和风险对人们日常生活的潜在影响也在一天天变大。如果你想获得足够的技术技能和商业头脑来确保企业的安全运转，就应该把《黑客大曝光》第5版作为必读书籍。熟悉并掌握这本书里的知识和技能是我们大家打赢未来每一场信息攻防战的第一步。

McAfee 公司总裁 Gene Hodges

前　言

不患无知，独患失察

回顾《黑客大曝光》第一版面世时的1999年，每个人都在“.com”世界里寻找着自己的立足之地并梦想自己有朝一日能够成为一家举世瞩目的IPO。那是一段美好的时光，各种各样的新技术如雨后春笋般涌现出来。但我们也知道，那段先建立一家“.com”公司，然后在12个月内把它变成一家股票上市公司的好时光已经一去不复返了。这不仅是因为资本市场本身发生了戏剧性的变化，信息安全因素也在其中扮演了重要角色。如果你到现在还不明白信息安全不是一种奢侈而是一种必要的话，我敢说你在过去的5年里不是穴居在某个岩洞的深处，就是你到现在还沉浸在你的“.com”股票还值点儿钱的旧日美好时光里不能自拔。

从产生编写《黑客大曝光》一书的想法开始，我们的目标一直是教育和警醒世人。有些人可能会批评我们“教育和警醒了许多坏家伙”，但那绝不是我们的初衷——那些坏家伙早就知道书里给出的东西。事实上，你们当中的许多人也早已知道黑客用来从事罪恶勾当的技术，而我们认为让更多的正义者知道这些技术只能是一件更好的事情。正如笔者经常说的那样，信息安全工作不是一件非常困难的事情，接受过这方面的教育培训并能随时保持高度警惕的任何人都可以胜任这项工作。

因此，《黑客大曝光》第5版里的关键词就是“警惕”。不管你是一位家庭用户还是某个世界100强公司的信息安全团队成员，都需要保持高度警惕。

不要因为同情心而丧失了应有的警惕性。无论是从你的个人生活还是事业发展的角度讲，密切关注信息安全技术的发展都将给你带来物超所值的回报。千万不要让自己在信息高速公路上成为各种“流弹”的下一个牺牲品！

第5版新增内容

之所以要编写《黑客大曝光》第5版，是因为不断涌现的新技术带来了一些新的安全威胁。信息安全领域里的各种挑战与信息技术的发展变化亦步亦趋：当技术的复杂程度呈指数级增长时，随之而来的安全问题也在以同样的比例增加。根据你个人的立场，这可能是一个好消息，也可能是一个坏消息。此外，可以用来绕过现有信息安全机制的新技术、新工具和新攻击手段正以一种让人应接不暇的速度涌现。你尽可以把信息攻防技术的此消彼长看作是一场“猫和老鼠”的游戏，但绝不能对这种利害冲突视若无睹。在这本书里，我们将延续《黑客大曝光》前几版的传统，把目前最新的信息攻防技术和技巧呈现给大家。

新增内容

下面是《黑客大曝光》第5版新增部分内容：

- 针对UNIX系统的最新信息攻防技术。
- 新增加的“攻击应用程序代码”一章对软件编程缺陷的产生过程以及如何防止它们有害传播的最佳应对措施进行了探讨。
- 新出现的Windows攻击手段以及相应的防范措施，其中包括利用RPCSS（Blaster蠕虫）、LSASS（Sasser蠕虫）和PCT（Download.ject病毒）缓冲区溢出漏洞的新型攻击手段。
- 全面改写的“拒绝服务攻击”一章，增加了对大规模分布式拒绝服务攻击及其防范措施的讨论。
- 介绍了一些新出现的Web黑客工具和技术，包括HTTP响应分割和几种新的自动化漏洞扫描工具。
- 全面改写的“攻击因特网用户”一章，对最新的IE浏览器攻击技术、在线服务的信息安全问题、网络欺诈等“社交工程”类攻击手段以及针对Windows平台的rootkit等黑色软件的最新发展动向进行了介绍和分析。
- 新增加了对无线网络攻击技术的介绍。
- 新增加了关于VoIP等远程连接攻击技术的内容。
- 新增加了关于Web和电子邮件客户端软件最新攻击技术的讨论，其中包括最新的IE浏览器攻击手段、网络欺诈活动、间谍软件、rootkits、“机器人”软件等。
- 黑客们利用Google搜索引擎作为情报收集工具的新方法。
- 经过改写的“查点”一章增加了如何利用因特网上的各种数据库收集情报的讨论。

- 全新的“案例研究”可以让大家及时了解最近出现的有关Google、无线网络和Mac OS X操作系统的攻击手段。

本书内容的基本结构

本书沿用了《黑客大曝光》以往的一贯设计风格。

这个图标代表攻击手段

这个图标可以帮助读者快速查找到特定的穿刺工具和具体操作步骤。在介绍完每一种攻击手段之后，我们会立刻给出针对这种攻击手段的防范措施并用下面这个图标加以突出。

这个图标代表防范措施

这个图标可以帮助读者快速查找到修补安防漏洞和挫败攻击者的具体措施和操作步骤。

- 在查阅书中代码清单时，请特别注意我们用**黑体字**强调的用户输入内容。
- 我们对书中介绍的每一种攻击手段都从三个方面进行了风险评级：

流行度：	*利用这种手段对实际目标进行攻击的频率：1代表最少见，10代表最常见。*
简单度：	*使用这种攻击手段所需的技能：10代表需要的技能最少，1则代表只有资深安全人员才能实施。*
影响力：	*攻击得手时可能造成的损失大小：1代表目标系统上的信息损失程度最小，10代表黑客能攻破超级用户账户或造成与此种情况相当的损失。*
风险率：	*前三个数字的平均值（舍入为与之最接近的整数），这个数值给出了这种攻击手段的总体危害程度。*

致读者

我们编写《黑客大曝光》一书的最初目的只是为了对几位作者所知道的黑客攻击手段进行收集整理并向渴望获得信息安全知识的人们提供相应的防范措施，但没有想到它会拥有这么多的读者并被翻译成20多种文字。《黑客大曝光》及其后续版本的受欢迎程度大大超出了我们当初的预想。几位作者经常在世界各地旅行，而每当我们在旅途中听到人们说起“是的，我有一本信息安全方面的圣经——《黑客大曝光》”时，就会觉得自己的付出得到了超值回报。

自从《黑客大曝光》第1版面世之后，有许多与之风格类似的书籍也出现在书店的货架上。你们或许读过信息安全方面的其他书籍并有自己的认识，但我们认为我们的写作风

格是最为简明、实用和准确的：把关于黑客技术、工具和相关对策的最新信息及时准确地提供给读者，帮助他们保护自己的信息资产。我们在这本书里仍然延续了这一风格。如果这是你第一次接触《黑客大曝光》，欢迎；如果你是这本书的长期读者，我们希望你能像喜欢前几个版本那样喜欢本书。法国思想家弗朗西斯·培根爵士曾经说过：知识就是力量。但知识的力量应该用来造福于人类而不是危害他人，我们衷心希望本书能够帮助各位赢得信息攻防战的胜利并给网络世界带来和平与安定。

致　　谢

首先，我们要衷心感谢各位勤恳和热心的Foundstone公司同事们的大力帮助。没有他们的不倦努力和严格把关，就没有读者手里的这本《黑客大曝光》第5版。我们还要感谢微软公司的同行们，其中包括微软的MSN Security、SBTU、TwC、Corporate Security、PSS、Office等项目团队以及向我们提供其他帮助和鼓励的人们。

我们还要特别感谢McGraw-Hill/Osborne出版公司为了这本书而不知疲倦的编辑和出版人员，其中包括Jane Brownlow、Emily Wolman、LeeAnn Pickrell、James Kussow和Jessica Wilson。

最后，我们还要向本书第 1 版、第 2 版、第 3 版和第 4 版的全体读者致以衷心的感谢。你们的无尽支持既是我们不断钻研最新信息安全技术的动力，也是我们揭秘最新黑客技术的目的。

作者简介

Stuart McClure

Stuart McClure 是 McAfee 公司风险管理类产品的研发副总裁，主要负责制定 McAfee Foundstone 系列风险化解和管理解决方案的产品研发和市场营销战略。McAfee 公司的 Foundstone 系列产品每年可以帮助那些受到黑客攻击、感染计算机病毒、蠕虫和黑色软件的用户挽回数百万计的经济损失。在加盟 McAfee 公司之前，Stuart 是 Foundstone 公司的创始人、总裁和首席技术执行官，该公司于 2004 年 10 月被 McAfee 公司收购。

Stuart 对各种安防产品有着全面深入的了解，是当今信息安全领域公认的权威之一。Stuart 给 McAfee Foundstone 公司带来了多年积累的技术和领导艺术，他在技术、实际操作和财务管理方面都有着很深厚的经验。在 Foundstone 公司，Stuart 既是产品规划和发展策略方面的领路人，也是所有技术开发、技术支持以及项目实施工作的具体领导者。在 Stuart 的带领下，Foundstone 公司自 1999 年成立以来每年的业绩增长率都超过了 100%。

在 1999 年，他牵头编写了有史以来最畅销的计算机信息安全类书籍——*Hacking Exposed: Network Security Secrets and Solutions*[1]，该书迄今已销售了 50 万册。此外，Stuart 还是 *Hacking Exposed: Windows 2000*（McGraw-Hill / Osborne 出版公司，2001 年）和 *Web Hacking: Attacks and Defense*（Addison-Wesley 出版公司，2002 年）的作者之一。

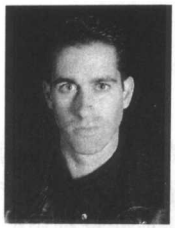
在加入 Foundstone 公司之前，Stuart 曾在 Ernst & Young 咨询公司的 National Security Profiling Team（国家信息安防支持团队）担任过多种与信息安全和 IT 有关的领导职务，他还在 InfoWorld 杂志的测试中心担任过两年的行业分析师，在加利福尼亚州政府和地方政府担任过五年的 IT 部门主管，有两年自营一家 IT 咨询公司，还有两年在科罗拉多州立大学负责 IT 事务。

Stuart 拥有科罗拉多州立大学的心理学和哲学学士学位，同时他还学习了大量的计算机科学与应用专业的课程，后来又陆续获得了包括 ISC2 机构的 CISSP、Novell 公司的 CNE 以及 Check Point 公司的 CCSE 在内的多个证书。

---

1 编者注：本文中提到的 Hacking Exposed:Network Security Secrets and Solutions、Hacking Exposed: Windows 2000、Hacking Exposed:Web Applications、Hacking Linux Exposed 等书均已由科海培中公司与清华大学出版社联合出版。

Joel Scambray



Joel Scambray 是微软公司 MSN 网站的高级安全主管，他每天都会遇到很多臭名昭著的因特网“居民”——从垃圾邮件制造者到恶意的攻击者。很多人是通过他编写的 *Hacking Exposed: Network Security Secrets & Solutions* 一书知道他的，这本书是世界上最畅销的因特网安全书籍之一。他还是 *Hacking Exposed: Web Applications* 一书的主要作者之一。

在 2002 年 8 月加入微软公司之前，Joel 曾帮助一家提供信息安全服务的新公司 Foundstone 赢得了业界公认的领导地位。他还担任过 Ernst & Young 咨询公司的经理、Microsoft TechNet 网站的安全专栏作家、InfoWorld 杂志的主编以及一家大型商业房地产公司的 IT 总监。Joel 还在很多场合做过信息安全方面的演讲，包括 CERT、The Computer Security Institute（CSI，计算机安全技术学院）、ISSA、ISACA、SANS、各种私营企业以及 FBI 和 RCMP 等政府机构。Joel 在 1999 年就获得了 CISSP 证书。

Joel Scambray 的联系方法：joel@winhackingexposed.com

George Kurtz

George Kurtz 是 McAfee 公司的风险管理部副总裁，主要负责制定 McAfee Foundstone 系列风险化解和管理解决方案的产品研发和市场营销策略，那些产品可以帮助用户保护自己的 IT 资产和优化其业务的可持续发展。在加盟 McAfee 公司之前，George 是 Foundstone 公司的 CEO，该公司于 2004 年 10 月被 McAfee 公司收购。

George 利用自己的商业远见和技术天份为 Foundstone 公司制定了发展战略，使该公司在众多的信息安全解决方案提供商中脱颖而出。在 1999 年与其他人合伙创办 Foundstone 公司之后，George 以自己的远见和企业家精神吸引了一大批世界一流的人才加入该公司的管理团队，并把 Foundstone 经营成一家最成功和最主要的私营信息安全公司。在担任 Foundstone 公司首席执行官期间，George 成功地募集到了超过 2000 万美元的风险投资，与多家世界级大公司建立了战略合作伙伴关系，并于 2004 年把 Foundstone 公司出售给了 McAfee 公司。他被评为全美发展最快的 50 家公司的领导者和技术创新先锋之一，南加利福尼亚州软件行业协会把他选为 2003 年度软件企业家之一。

在合伙创办 Foundstone 公司之前，George 是 Ernst & Young 咨询公司信息安全服务部门的全美总经理。在加入 Ernst & Young 公司之前，George 是 Pricewaterhouse Coopers 公司负责全球因特网信息安全测试项目研发工作的经理。

作为一名国际公认的信息安全专家和企业家，George 经常在该领域的各年会上发表演讲，他的言论经常出现在众多顶级刊物和公共媒体上，其中包括 ***Wall Street Journal***（华尔

街邮报）、*Time*（时代杂志）、*Los Angeles Times*（洛杉矶时报）、*USA Today*（今日美国杂志）、CNN 电视台等。他是畅销书 *Hacking Exposed: Network Security Secrets & Solutions* 和 *Hacking Linux Exposed*（McGraw-Hill/Os-borne 出版公司，2002 年）的合著作者之一，并经常在信息安全领域的权威刊物上发表文章。

George 拥有信息安全行业的多项证书，包括 Certified Information Systems Security Professional（CISSP）、Certified Information Systems Auditor（CISA）和 Certified Public Accountant（CPA）证书。George 毕业于塞顿霍尔大学，在那里获得了财务专业的学士学位。

其他作者简介

Stephan Barnes 是 McAfee 公司旗下 Foundstone Professional Services 咨询业务部门的现任销售主管，而他本人是信息安全业的著名人物之一。Stephan 在信息安全领域已有 20 多年的从业经验，主要研究方向是密集拨号、调制解调器、PBX 和语音邮件等安全技术。所有这些技术都是评估一家现代企业对外安全现状的重要组成部分。Stephan 的从业经历包括为一家军事承包商和美国国防部（Department of Defense，DoD）工作，为各种财务、电讯、保险、制造、营销、公共事业和高科技公司进行了数百次穿刺测试和咨询。Stephan 经常在与信息安全有关的学术会议和组织机构发表演讲。他的网名 M4phr1k 已经使用了 20 多年，他还建立了一个专门讨论密集拨号技术和其他相关话题的个人站点 http://www.m4phr1k.com。

Michael Davis 目前是 Foundstone 公司的一名研究人员。他是活跃的入侵检测系统开发者和部署者，著名的入侵检测系统软件 Snort 就有他的功劳。Michael 还是 Honeynet 项目的成员之一，他在那里负责为基于 Windows 的“密网”开发数据和网络控制机制。

Nicolas Fischbach 是 COLT Telecom 公司欧洲网络安全工程团队的高级经理之一，该公司是一家业界领先的泛欧洲端到端通讯服务提供商。他拥有网络和分布式计算的工学学位，是人们公认的网站安全和 DoS 攻击化解方面的权威。Nicolas 是为法语用户提供计算机和网络安全服务的 Sécurité.Org 网站、非正式安防研究团队 eXperts 和 mystique 组织以及 Honeynet 项目法国分部的合伙创办人之一。他参加过无数的计算机技术和信息安全技术会议，在许多大专院校开设了网络建设和信息安全课程；还经常在法语信息安全技术杂志 *MISC* 上发表文章。有关 Nicolas 的更多信息和联系方法，见他的个人主页 http://www.security.org/nico。

James C. Foster（CISSP，CCSE）是 Foundstone 公司 FASL Research & Development and Threat Intelligence 部门的经理，他领导的研发团队主要负责为 FoundScan 系列产品开发