网络安全机密与解决方案

Network Security Secrets & Solutions

HACKING EXPOSED

黑客大曝光

第2版

【美】Joel Scambray,Stuart McClure
George Kurtz 著
钟向群 杨继张 译
吴世忠 审校

清华大学出版社
McGraw Hill Education

网络安全机密与解决方案

黑客大曝光

（第2版）

【美】Joel Scambray,Stuart McClure
George Kurtz 著
钟向群 杨继张 译
吴世忠 审校

清华大学出版社 McGraw-Hill Education

(京)新登字 158 号
著作权合同登记号：01-2001-3276

内容提要

全书从攻击者和防御者的不同角度系统阐述了计算机和网络的入侵手段及相应防御措施。

本书的第 1 版在美国是畅销书，销量已超过 10 万册。自第 1 版畅销后，又有许多崭新的工具和技术出现，第 2 版在第 1 版的基础上增加了近一倍的新内容，包括探讨了 Windows 2000 的系统攻击与防御、对因特网用户的攻击与防御；介绍了新的后门和侦破技术，新的分布式拒绝服务攻击(DDoS)的工具和技巧以及新的网络分析工具。

全书注重案例分析，讲解了很多具体攻击的过程，更重要的是将几乎所有讨论过的攻击手段都提供了相应的对策。

本书是安全漏洞的宝典，是负责安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的重要参考书。

书　名：黑客大曝光：网络安全机密与解决方案(第 2 版)
作　者：Joel Scambray,Stuart McClure,George Kurtz
译　者：钟向群　杨继张
出版者：清华大学出版社(北京清华大学校内，邮编 100084)
印刷者：北京门头沟胶印厂
发　行：新华书店总店北京科技发行所
开　本：异 16　印张：46.75　　字数：858 千字
版　次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
印　数：0001～5000
书　号：ISBN 7-302-05026-0/TP.2932
定　价：69.00 元

院士推荐

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护方面的技术，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、是似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和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。

中国工程院院士 何德全

谨以此书献给我的父母和先辈，是他们给了我生命；献给我的妻子，是她给予我持续的鼓励；也献给我的孩子们，是她们赋予了此书奇异与灵性。

-- Joel Scambray

本书献给我的妻子与孩子；要不是她们坚定的支持与爱，我的一生就几乎没什么值得一提；也献给我的父母，他们给予我的自信心令我感激不尽。

-- Stuart McClure

本书献给我亲爱的妻子 Anna。要不是她的理解、支持和不懈的努力，我不可能完成这本书。我还要感谢我的全体家庭成员，当最后期限眼看就要逾越时，她们帮我“挤占时间”。

-- George Kurtz

本书献给追求真理的人们，他们仍在坚持不懈地从桎梏与训诫中寻求自由。

-- 全体作者

关于作者

Joel Scambray

Joel Scambray是Foundstone公司(http://www.foundstone.com)的主要负责人之一，Foundstone公司向各种机构(从幸福500到新兴的公司)提供信息系统安全咨询服务。他对各种安全技术均有丰富的实战经验；为各种应用程序和产品设计和分析了安全体系结构。Scambray先生在微软的TechNet站点每月“安全问答”中担任专栏答题(http://www.microsoft.com/technet/security)，并且在InfoWorld杂志(http://www.infoworld.com/security)的“安全观察”专栏中发表过许多的安全技术产品分析文章。他曾在Ernst&Young LLP公司的电子安全解决小组中担任主管，是InfoWorld的测试中心高级分析员；也曾任一家大房地产公司的IT主管。Scambray先生是认证的信息系统安全专家(CISSP，Certified Information Systems Security Professional)以及认证的Checkpoint安全工程师(CCSE，Certified Checkpoint Security Engineer)。

读者可通过电子邮件joel@hackingexposed.com 与Joel Scambray联系。

Stuart McClure

Stuart McClure是Foundstone公司(http://www.foundstone.com)的总裁兼CTO，他有十多年的IT和安全经验。McClure先生擅长安全评估、防火墙评测、电子商务应用评测、主机系统评测以及PKI技术、攻击检测、事件响应等。他担任了两年多的InfoWorld杂志“安全观察”专栏的作者之一，该专栏主要讨论各种安全问题、系统脆弱性以及安全技术开发等。在过去的四年中，他与五大安全咨询公司及InfoWorld测试中心一起评测了数以千计的网络与安全的硬软件产品。在此之前，McClure先生花了七年多的时间管理和保障公司、学院及政府机关的网络与系统，这些系统涉及了Cisco，Novell，Solaris，AIX，AS/400，Windows NT以及Linux等多种产品和平台。

读者可通过电子邮件stuart@hackingexposed.com 与Stuart McClure联系。

George Kurtz

George Kurtz是Foundstone公司(http://www.foundstone.com)的CEO，该公司是一个非常优秀和前沿的安全咨询与培训组织。Kurtz先生是国际知名的安全专家，在他的安全顾问生涯中已进行了数以百计的与防火墙、网络及电子商务相关的安全评估。Kurtz先生在入侵检测、防火墙技术、事件响应进程以及远程访问方案等方面有丰富的经验。他还是许多安全会议的专门发言人，其言论在很多著名出版物中被引用，包括“华尔街日报”(The Wall Street Journal)、“信息世界”(Info World)、“今日美国”(USA Today)等。Kurtz先生还经常被邀请在安全事件中发表评论；也是各大电视台(包括CNN，CNBC，NBC及ABC等)的常客。

读者可通过电子邮件george@hackingexposed.com与George Kurtz联系。

关于技术评阅者

Saumil Shah

Saumil Shah 先生为 Foundstone 公司的客户提供信息安全的咨询服务，其专长为道德黑客技术(ethical hacking)与安全体系结构。他获得了认证的信息系统安全专家(CISSP)资格。Shah 先生有六年多的系统管理、网络体系以及异种平台集成及信息安全经验。他为 IT 领域中的许多著名公司做过大量的道德黑客防范训练。在加入 Foundstone 公司之前，Shah 先生与 Ernst&Young 公司的高级顾问负责其道德黑客防范及安全体系解决方案。Shah 先生也是 Tata McGraw-Hill India 出版社出版的《The Anti-Virus Book》一书的作者，也曾是印弟安那管理研究所的研究助理。

读者可通过电子邮件 saumil.shah@foundstone.com 与 Saumil Shah 联系。

Victor Robert "Bob" Garza

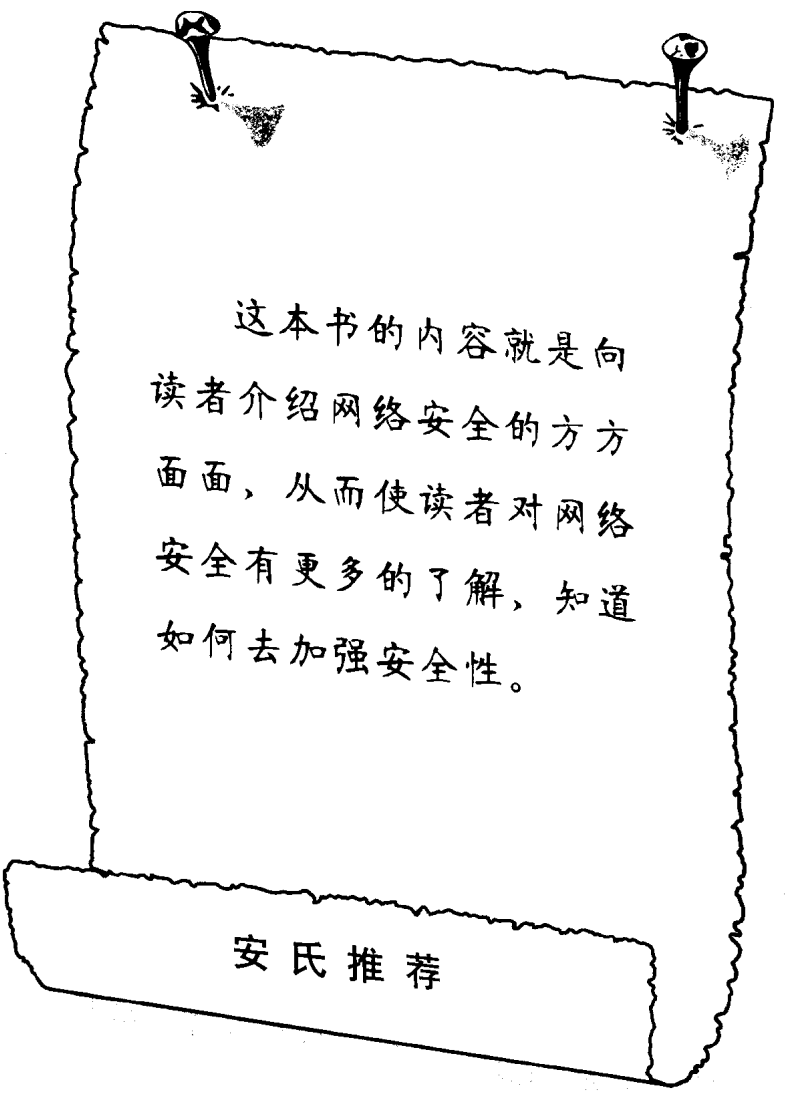
Bob Garza 是硅谷一跨国公司的高级 IT 网络工程师，主要负责超过 2 万 5 千多台主机的网络的运行支持、网络管理及安全工作。他在计算机行业中有超过 20 年的工作经验，是"傻瓜"(For Dummies)系列丛书的作者。Garza 先生在过去九年中还为 InfoWorld 和 Federal Computer Week 撰写过网络和安全产品的回顾文章。Garza 先生是电信管理的硕士及信息系统管理的学士。

Eric Schultze

Eric Schultze 近九年来一直在信息技术与安全领域中工作，大部分时间关注于微软技术与平台的评估及相关安全性。他也是 NetWorld Interop，Usenix，BlackHat，SANS 及 MIS 等安全会议上的经常发言人；他也是计算机安全研究所的指导教师。Schultze 先生也经常出现在电视及许多出版物上，比如 NBC，CNBC，TIME，ComputerWorld 和 The Standard 等。Schultz 公司曾任职的公司有 Foundstone，SecurityFocus.com，Ernst&Young，Price Waterhouse，Bealls 以及 Salomon Brothers。他曾是本书第一版中的作者之一，目前是一软件开发公司的安全项目主管。

Martin W.Dolphin

Martin Dolphin 是 Ernst & Young 公司在新英格兰的安全技术解决方案业务部的主管。Dolphin 先生有十年以上计算机管理经验，其中针对 Windows NT、Novell Netware 和因特网的安全方面有五年以上的经验。他也给"极端黑客攻击手段——防御你的站点"课程上课。


这本书的内容就是向读者介绍网络安全的方方面面，从而使读者对网络安全有更多的了解，知道如何去加强安全性。
安氏推荐

序

森林中一棵树倒下的时候，也许无人听见，但其倒下时必有轰然之声；如果一个计算机网络有了安全漏洞却没人知道，它是否就安全呢？对于前者，也许只有极端唯心的贝克莱主义者(Berkeleian)会不以为然；而对于后者，就很难有明显的结论了。

安全上存在漏洞(脆弱性)的网络对于知道这个漏洞的人来说自然是不安全的。如果没人知道——也就是说只是未被发现的漏洞——那么网络就是安全的。如果有一个人知道，网络对他来讲是不安全的，而对其他人仍然是安全的。如果网络设备厂商知道……，如果网络研究者知道……，如果黑客圈子里的人知道——网络的不安全性随着漏洞消息的传播而增大。

果真如此吗？事实上，安全脆弱性的存在，与有没有人知道无关。公开其漏洞也并不会导致网络就不安全。关于事物的知识与事物本身并不能混为一谈。公开漏洞的确会增加攻击者利用其漏洞的可能性，但并没有增加漏洞的可能性。攻击者不能突破其无所知的漏洞，但保卫者也不能保护对漏洞无所知的网络。

所以，如果保守漏洞秘密就可提高安全性的话，这种方式也太脆弱了。保守秘密的有效期决定了这种方式的作用期。但是，对于信息的任何操作总是在传播信息。有些人是无意识地泄了密；而其他一些人可能是有意泄密。而有时候秘密却是某些人制造出来的。有一点，秘密一旦泄露，则再无收回的可能。

建立在漏洞公开基础上的安全将更坚固。不错，攻击者会知道其弱点，但事实上他们也会从各种渠道知道的。因此，更重要的是，防卫的一方知道并了解了这些弱点，产品商就会修补，系统管理员就会防范。知道这些弱点的人越多，就会得到更大的安全性。

这也是“全曝光”安全运动的哲学注脚。这几年因特网上的实践证明是正确的，因特网更安全了。面对那些公开的演示漏洞的代码和研究成果，软件商们要否定其产品的漏洞显然也是更困难了；而公司在报纸上已公开其产品弱点的时候也不能再掩盖问题了。因特网虽然仍是非常的不安全，但如果所有这些安全漏洞均不公之于众，则只会更糟。

正是由于公开的信息不能自动地掌握在应该掌握的人手里，因此本书就有必要和大家见面。黑客大曝光是“全曝光”(Full Disclosure)运动的杰出之作，它是安全漏洞的宝典：漏洞是什么，它们如何起作用，我们该怎么办。读完本书，你会对你的网络

了解更多，也会知道如何去加强安全性，此书的价值如金，如我所知之此类书，无出其右者。

当然，信息的好坏，存乎于运用。也许有些人会将此书作为攻击系统的手册；这很不幸，但的确也是事实。不过，权衡之下仍是值得的。其实，对于攻击者来说，已经有了许多攻击系统的手册：Web 站点、聊天室、各种点击就可得到的工具。因此，意在攻击网络的人早已荷枪实弹，这是不言自明的。而正是守卫者们必须武装起来，必须知道黑客是如何运作的，其攻击工具是如何工作的，自己的系统中又有哪些安全漏洞。

本书第1版是畅销书，在不到一年时间里，销售了7万余册。作者之所以觉得有必要更新，是因为计算机安全的发展是如此迅速，许多新的信息应该补充，于是有了第2版的问世。

美国中央情报局(CIA)大厅的石墙上面刻着圣经的话："你应当了解真相，真相会使你自由"。知识就是力量，因为它使你按世界的本来面目做出正确的决定，而不是按照你所认为或相信的那样去做决定。此书将赋予你知识和力量，请你明智使用。

Bruce Schneier
Counterpane Internet Security公司首席技术官
http://www.counterpane.com
2000年7月1日

Bruce Schneier 是 Counterpane Internet Security 公司的创始者和首席技术官(CTO)，该公司(http://www.counterpane.com) 是首屈一指的安全管理监控的公司。他本人也是Blowfish,Twofish 和 Yarrow 的设计者。他的最新力作是"秘密与谎言：网络世界中的数字安全"(Secrets and Lies: Digital Security in a Networked World)。

前 言

因特网安全性——伤痕累累

《黑客大曝光》(Hacking Exposed) 第1版出版已逾一年，“信息系统是现代社会的命脉”之类的话也逐渐成为陈词滥调了。0和1所构成的电子脉搏维持着我们的生存，瞬间即达的在线商务滋养着我们的生活，数字的流动就像血液，在我们的大众文化和集体意识的动脉中流淌。

然而，我们必须痛苦地指出，这些动脉在今日因特网的战场上伤痕累累。而更令我们痛苦的是，每日在网络丛林中的数以百万计的人们对于这些伤口仍不以为然，或熟视无睹：

- ▼ 自1998年以来，报告给权威的Bugtraq数据库的信息系统脆弱点(vulnerabilities)的数目就大幅上升了4倍。在2000年的几个月内，从20增到了近80(http:// www.securityfocus.com/vdb/stats.html)。
- ■ 通用脆弱点及曝光(CVE:Common Vulnerabilities and Exposures)编辑版，由来自包括安全软件厂商和学术研究机构在内的20多个安全有关组织中的代表组成。仅1999年就发表了1000多个成熟的、并深入研究过的脆弱点(http://cve.mitre.org)。
- ▲ 计算机安全研究所和FBI联合对美国643个计算机安全从业者进行了调查，它们有公司、政府机构、金融机构、医学研究机构以及大学等。结果发现，90%的调查反馈者在去年发现了电子攻击，其中273个组织报告共有265 589 940美元的经济损失 (http://www.gocsi.com, “2000 Computer Crime and Security Survey”)。

上述仅是已报告的一些材料。作为每日沉浸于这个领域的经验较为丰富的安全从业者，我们可以肯定地说，问题远远比你听到或读到的要严重得多。

显然，我们这个诞生不久的数字生存空间受着这些数以千计的伤口的威胁，可能慢慢地流血而死。我们怎样才能保护自己，免受正在日益增长的既广泛又复杂的攻击呢?

答案：更多的信息

答案在你自己的手中。我们在过去的一年里，费尽苦心地跟踪着战场的脉搏，希望从前线带给你最新的报告。我们在此得说，战斗是很激烈的，但战争看来可以取胜。

在此书中，我们罗列了敌人的攻击方法，在每个案例中，我们给出了保护自己数字领地的已经测试的策略。你会拖延错失这些信息吗？

我们认为德高望重的同事 Bruce Schneier 在第 2 版的序（也许你刚刚读过）谈得非常好。我们不妨再重复其中的几句：

> “黑客大曝光是“全曝光”（Full Disclosure）运动的杰出之作，它是安全漏洞的宝典：漏洞是什么，它们如何起作用，我们该怎么办。读完本书，你会对你的网络了解更多，也会知道如何去加强安全性，此书的价值如金，如我所知之此类书，无出其右者。”

10 万读者已先知

我们的话或 Bruce 的话都可以不以为然。下面是 10 多万第 1 版读者中的几位读者对本书的一些评论：

“我 6 个月前拜读了这本书，真是令人难以置信的好，去年 3 月我参加了一次大型美国军队会议，每个参加者（超过 300 人）都人手一本……”——一个计算机培训公司的总裁

“我得向每一个运行商用 Windows NT 的人们推荐这本必读之书……它清晰易懂，形式活泼，实例丰富，而且资源和方案均有提供。如果你本季度只购一本计算机书籍，那就是它。”——Stu Sjouwerman，Sunbelt 软件公司总裁，NTools E-News（超过 60 万订户）杂志的编辑，Amazon.com 前 10 名畅销书“Windows NT Power Toolkit”和“Windows 2000 System Administrator's Black Book”的作者

“当你觉得懂了一个课题时，你可以读读这本书。我原以为我懂 NT 和 UNIX，然而我错了！这本书真正开阔了我的视野，了解了那些我原以为高枕无忧的系统却有如此多的攻击漏洞和枪眼……”——爱尔兰的一位读者

“我为美国政府构建加密数据网络，本书包含比我期望的更多的信息，它覆盖了网络攻击之前和之中所要用到的所有方法。此书令我印象如此深刻，我将它作为藏书，并推荐给我的多位同事。真是件了不起的杰作！”——美国的一位读者

“读之如小说，骇之如地狱！此书是网络安全的使用手册。每个脆弱点都有简明小结，然后指出其发掘的方法，并给出相应的对策。工具和实用程序的总结也是最佳的。如果你尚未一读，应赶快行动！”——密执安的一位读者

“……此书“以贼之道治贼”的方法很具有技巧性，我建议每个 CIO 都读这本书。”——波士顿的一位读者

“市场上计算机安全书中的佼佼者……如果你从事的工作与计算机安全有关，本书为最好的选择”。—— Hacker News Network，www.hackernews.com

国际畅销书

这只是我们去年收到的大量电子邮件或私人信件中赞美之词中的几例。我们希望在此都予付印，因篇幅所限，仅以下面的几个事实作为读者们大量正面赞誉的证明：

- ▼ 许多大学和学院，包括美国空军和得克萨斯大学，专门围绕本书的内容开设了课程，并以此为课本。
- ■ 本书被翻译成十几种语言，包括德语、汉语、西班牙语、法语、俄语和葡萄牙语。而且成为了国际畅销书。
- ■ 本书在出版的第一年连续赢得Amazon.com 前200的排名，在6个月内升高至前10位。在技术专题领域内那是很少有的卓著业绩。
- ■ 在许多图书排行榜、Web 网站、新闻宣传单中，包括 Amazon，Borders，Barnes & Noble 等，本书在技术和计算机安全书籍中均名列榜首。在 2000 年 5 月 Publisher's Weekly 畅销书排名中，在计算机书籍中名列第五。在 2000 年 6 月 26 日被 News & Observer 评为“最热销计算机书籍”。
- ▲ 1999 年秋天在 Networld+Interop 上刚投放市场，本书即排名销量第一。

第 2 版中的新增内容

当然，我们的著作并非完美。因特网安全的领域远比数字经济要发展得快。许多崭新的工具和技术自本书第 1 版面世后已浮出水面。我们花了巨大的努力来落实新版本中的重点，同时，根据读者的建议，做了全面的改进。

新内容超过 220 多页

下面是第 2 版中修改和补充的最主要内容：

1. 增加了全新的一章“攻击因特网用户”，讲述了对 Web 浏览器、电子邮件软件、活动内容的各种恶毒威胁，以及对因特网客户的各种攻击手段，包括最新的 Outlook 日期域缓冲区溢出攻击以及“ILOVEYOU”蠕虫病毒。
2. 增加针对 Windows 2000 攻击和对策的新的篇幅较长的一章。
3. 在第 15 章中对 E-Commerce 黑客攻击方法做了较大修改。
4. 涵盖了所有新的分布式拒绝服务攻击（DDOS）的工具和技巧，这些工具在 2000 年 2 月几乎将因特网击垮（Trinoo,TFN2K,Stacheldraht）。

5. 介绍了新的后门和侦破技术，包括对 Windows 9x 中如 Sub7 之类攻击的防范。
6. 增加新的网络发现工具和技术，包括更新的基于 Windows 的扫描工具，如何用 ARP 重定向在交换网络上实行窃听攻击，以及对 RIP 欺骗攻击的深入分析等。
7. 在每一部分的开头都有新的案例研究，包含了最近的一些安全攻击案例及注解。
8. 更新了 Windows 9x，ME，Windows NT，UNIX，Linux，Netware 以及其他平台的安全攻击信息，并提出了相应的对策。
9. 在拨号攻击的部分，做了修订和更新，增加了关于 PBX 和语音信箱攻击的新材料，以及新的 VPN 内容。
10. 通过新的图示对各种攻击和对策进行了强调，从而更容易获得相关信息。
11. 增加了全新的对应网站 http://www.hackingexposed.com ，有实时更新的内容、新闻和对各种工具及本书引用的因特网资源的链接。
12. 还有，令人尊敬的安全大师 Bruce Schneier（Counterpane Internet 安全公司）为本文所作的序……

所有这些新的材料使得第 2 版有一倍的内容更新。

保留了第 1 版的优点：模块化、组织架构以及可利用性

尽管更新了许多东西，我们仍然保留了全书的基本组织架构，这是第 1 版的读者熟悉和肯定的。即以入侵者的基本攻击方法为线索：

▼ 目标探测和信息攫取
■ 初始探访
■ 特权升级
▲ 掩盖踪迹

我们也努力将内容组织得模块化，从而使忙碌的系统管理员们可以一块一块地消化，不必一次读完。每种攻击和对策都彼此独立，一两页就可以解决问题，无需太多的背景材料。基于操作系统的严格分类可以大大提高效率——比如，你可以直接阅读 Windows 2000 的章节，而不必阅读许多和 UNIX 平台无关的信息。

当然，我们延续了清晰、可读、简洁的写作风格，这是读者们对第 1 版的赞誉之一。我们知道大家很忙，需要直截了当，不需太多的技术术语。正如密执安州的一位读者所写："读之如小说，骇之如地狱"。我们希望不管你是从头至尾地读，还是从中抽取一部分来读，都能让读者满意。

对图示和风险率进行了改进，更易定位

在 Osborne/McGraw-Hill 出版公司的帮助下，我们根据一些读者的建议，对全书

做了一些美术加工：

▼ 对每种攻击技巧均在书的边缘加了强调的图标，从而对特定的穿透测试工具和方法更易定位。比如：

这是一个攻击图标

■ 每个攻击都有对应的可操作的、并经测试的对策，从而直接处理发现的问题。其特定的图标为：

这是对策图标

■ 我们也增加了其他一些有用的标识，对一些容易忽略的细节进行强调：

■ 由于相应的Web站点是本书的重要部分，我们在http://www.hackinge xposed.com中均有图示，以标识更新部分、作者评论以及书中提及的各种工具。

■ 我们对实例中的源代码清单、屏幕快照、图示做了清理，并对用户输入用黑体字标注。

▲ 每种攻击都有相应的风险率，根据作者的经验，归于三个基本因素：

流行度：	***在江湖上用于攻击实际目标的使用频繁度，1为极少，10为广泛使用。***
容易度：	*执行攻击所必须的技巧。1为很少或不需技巧，10为老练的安全程序员。*
影响力：	***攻击成功实施后导致的潜在损害。1为目标的一些无关紧要的信息，10为超级用户账户或类似的信息。***
风险率：	*上述三者的平均值为基本的风险率，向上取整为其值。*

致过去、现在和未来的读者

鉴于大家对本书第1版的厚爱，我们在第2版中倾注了全部身心和满腔热情。我们希望这些努力会使原有的读者仍然惠顾，并且吸引来更多尚未读过本书的朋友，去领略本书的魅力。

—— Joel, Stu, & George

黑客大曝光 网络安全机密与解决方案

无论你是一个想保护自己网络的管理员，还是一个想避免犯历史性安全错误的程序员，或是一个考虑网络安全如何工作的热心人，《黑客大曝光》提供了对付常见攻击过程和防御的坚实基础，安全圈的每个人都应当用心阅读它。

——Rain Forest Puppy (RFP)
Web服务器安全权威，IIS MSADC 漏洞的发现者

大部分有关安全的书往往在一年内就过时了。但是《黑客大曝光》不是这样，它比以往任何类似书籍有更多信息量、也更实用、更及时。这是你能买到的最棒的全方位安全揭密的书了。

——Simple Nomad
知名NT/Netware/Internet 安全专家，《The Hack FAQ and Pandora》的作者

《黑客大曝光》第2版提供了更加全面的安全揭密。作者提供了最新网络攻击技术的详细解释，以及进行防御的必须步骤。鉴于大量的更新内容，以及对最新工具和漏洞的全面覆盖，我强烈推荐《黑客大曝光》的第2版，即使你已经是第1版的读者。

——Fyodor
无法比拟的NMAP安全扫描工具的作者

《黑客大曝光》为安全揭密类书籍设定了标准。最新版本包含更多的信息，更新的攻击方法和防御措施，当然还有作者独具说服力的分析。强烈推荐！

——Todd Sabin
顶级安全程序员，不可缺少的pwdump2工具的作者

这本非常出色的书不仅提示了可能存在于你环境中的漏洞的细节，还提供指导你的机构防范这些风险的方法。

——Lance Spitzner
Honeynet 项目合作者，大受欢迎的《Know Your Enemy》系列丛书的作者

全面揭密是保护你自己和你的网络的一种强有力的工具。《黑客大曝光》是一个非常有价值的典范。

——Georgi Guninski
著名的因特网安全研究者