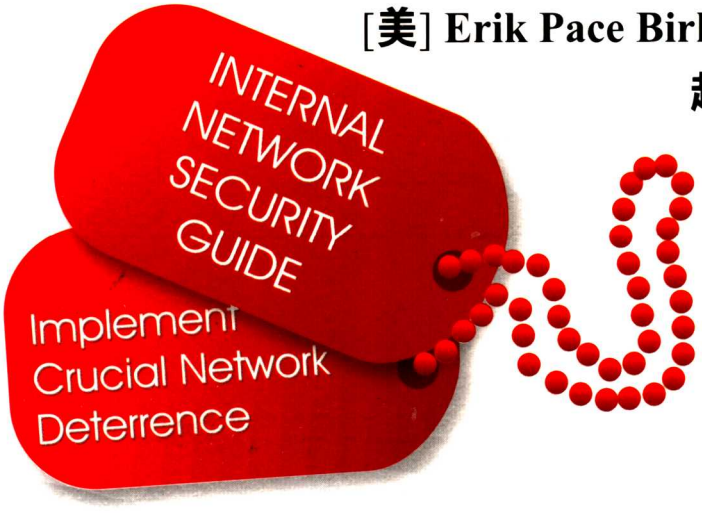
Broadview®
www.broadview.com.cn

安全技术大系

SPECIAL OPS
Host and Network Security
for Microsoft, UNIX, and Oracle

Microsoft, UNIX 及 Oracle 主机和网络安全



[美] Erik Pace Birkholz Foundstone 公司 著
赵彦玲 潘吉兵 董春红 等译

SYNGRESS®
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

Microsoft, UNIX 及 Oracle 主机和网络安全

SPECIAL OPS Host and Network Security for Microsoft, UNIX, and Oracle

[美] Erik Pace Birkholz　Foundstone 公司 著

赵彦玲　潘吉兵　董春红 等译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书凝聚了数十位权威的国际安全专家的实战经验和技术总结。它不仅提供了 Windows 系统、UNIX 系统和 Oracle 系统的主机及网络安全解决方案，而且包括了企业的安全管理规范和原则；它既高屋建瓴地描述了企业内部网整体面临的安全威胁和漏洞，又细致地介绍了 Windows，UNIX，Oracle 及无线 LAN 等各种系统具体的漏洞，同时还提供了各种漏洞评测方法和补救预防措施。

本书可作为企业安全技术人员实战的好帮手，也适合作为安全技术初学者了解各种漏洞和安全工具的实用指南，更适合做大中院校相关专业和企业安全技术培训的教材。

版权贸易合同登记号　图字：01-2003-2425

图书在版编目（CIP）数据

Microsoft, UNIX 及 Oracle 主机和网络安全/（美）布莱克赫兹（Birkholz, E.P.）等著. 赵彦玲等译.
北京：电子工业出版社，2004.7
（安全技术大系）
书名原文：Special OPS the Host and Network Security for Microsoft, UNIX, and Oracle
ISBN 7-121-00002-4

Ⅰ. M…　Ⅱ. ①布…　②赵…　Ⅲ. ①窗口软件，Windows—安全技术　②UNIX 操作系统—安全技术　③关系数据库—数据库管理系统，Oracle—安全技术　Ⅳ. ①TP316　②TP311.138

中国版本图书馆 CIP 数据核字（2004）第 056035 号

责任编辑：孙学瑛
印　　刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：48.25　字数：967 千字
印　　次：2004 年 7 月第 1 次印刷
印　　数：5 000 册　　定价：79.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译 者 序

20 世纪末，信息技术在全世界飞速发展，在人们尽情享受着它所带来的好处的同时，也因为没有对信息安全问题给予足够的重视而蒙受了许多重大的损失。进入 21 世纪以来，网络和主机的安全防护技术已逐渐成为一个新兴的重要技术领域，并且受到政府、企业及全社会的高度重视。越来越多专家和技术人员在为寻求圆满的安全解决方案而努力。

应当说本书正是那些因为企业信息安全问题而寝食难安的技术人员的良药，它汇聚了数十位安全专家的实战经验和技术总结，不仅提供了 Windows 系统、UNIX 系统和 Oracle 系统的主机及网络安全解决方案，而且包括了企业的安全管理规范和原则。

本书的第一作者 Erik 是 Foundstone 公司的首席咨询师和主讲师。自 1995 年以来，Erik 已经在世界各地执行了多次内部安全评估、渗透测试、主机安全评测、Web 应用程序评估和安全培训。Erik 是全球最畅销丛书（共 6 部书）中 4 部书的合著者。在他的职业生涯中，Erik 向美国各大企业和政府机构的成员都进行过黑客方法和技巧的演讲，包括微软、联邦调查局、国家安全局和国防部。

本书的其他作者也都是信息安全各个分支领域的专家，如 Chip 是一位有 12 年经验的程序员和计算机安全咨询师，擅长在软件开发的各个方面应用安全技巧。他是第 12 章“攻击和防护 Microsoft SQL Server”的作者。John 是 Foundstone 公司的 R&D 工程师，他主要擅长无线安全和网络评估技术。他是第 15 章“无线 LAN：发现和防护”的作者，等等。总之，本书每章的作者都对相关的领域有着丰富的工作经验和独到的见解。关于作者更详细的介绍，参见“Speical OPS 的创立者和主要作者”。

本书既高屋建瓴地描述了企业内部网整体面临的安全威胁和漏洞，又细致入微地介绍了 Windows，UNIX，Oracle 及无线 LAN 等各种系统具体的漏洞。同时又提供了各种漏洞评测方法和补救预防措施。本书既是企业安全技术人员实战的好帮手，也是安全技术初学者了解各种漏洞和安全工具的实用指南。

本书主要由赵彦玲、吴红、董春红、潘吉兵等翻译。译者力求反映原书的特点和风貌，但由于时间关系及水平所限，不当和疏漏之处在所难免，敬请广大读者批评指正。

献　　词

您的爱
是珍贵的礼物
我从不奢求
从不期望
但自从
我们见面的
那一刻
已开始渴望

从您那里
我找到了
我的激情和灵感

我把这本书献给您
Rachele

——*Erik Pace Birkholz*

致　谢

感谢我的 4 位父母（父亲和 Peg，母亲和 Art），感谢他们所给予我一生的好运、支持和爱。

感谢在我生命的各个阶段把我当成朋友的所有人，特别是我最好的 8 位朋友：Dave，Paul，TJ，Rains，Turtle，Alex，Rex 和 Cole。

感谢 Stuart 和 Joel。你们的友谊和教诲是无价之宝。你们为我打开的大门已经在我的职业生涯中和未来的道路上打下了不可磨灭的烙印。我会把你们的爱发扬光大。

感谢国家攻击和渗透组（National Attack and Penetration Team）的老员工，你们过去的努力为我们大家铺好了通往光明未来的路。感谢 Foundstone 的 IT 主管 Tom Lee，还有我的“顾问妈妈”Janet，在我一个星期接一个星期在世界各地奔波时，帮我安排好一切事情。

感谢 Jeff 和 Ping Moss，创建并完善着“Black Hat”通报会议。我十分珍惜作为这一伟大会议一部分的机会。

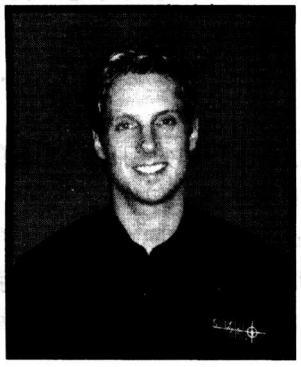
感谢 Maurice“Mo”Smith（世界重量级泰拳、跆拳道和终极搏击冠军），他向我提出的计算机方面的问题与我向他提出的搏击方面的问题一样多。结果证明，搏击和安全评估并没有什么不同：都是攻击和防御的策略。感谢你给予我的训练、技巧和自信。我希望这一切是互惠的。

感谢我的技术编辑 Eric Schultze 和 Mark Burnett，感谢每一位特殊作者和合著者在百忙之中参与了这本书的工作，使它能够得以完成。

最后，感谢 Andrew 和 Syngress 团队其他成员的指导和鼓励。整个 Special OPS 团队都行动起来了！

——*Erik Pace Birkholz*

Special OPS 的创立者和主要作者



Erik Pace Birkholz

erik@SpecialOpsSecurity.com

Erik Pace Birkholz（CISSP，MCSE）是 Foundstone 公司的首席咨询师和主讲师。自 1995 年以来，Erik 已经在世界各地主持了多次内部安全评估、渗透测试、主机安全评测、Web 应用程序评估和安全培训。Erik 是全球最畅销丛书（共 6 部书）中 4 部书的合著者，也是“*Hacking Exposed: Network Security Secrets & Solutions*”（Osborne/McGraw-Hill）的合著者。

2002 年，Erik 应邀在华盛顿州雷蒙德市的微软公司总部向 500 名 Windows 开发人员发表了演讲“Hacking Exposed: Live!”。稍后，他又应邀在 2002 年微软全球通报会议（2002 Microsoft Global Briefings）上向 3000 名来自全球各地的微软员工发表演讲。由于他已经向 9500 名听众发表了500 次演讲，这次他的演讲被排在第一位。基于这样的成绩，他成为了“Microsoft MEC 2002”会议的重要发言人。

在他的职业生涯中，Erik 向美国各大政府机构的成员发表过有关黑客的方法和技巧的演讲，包括联邦调查局、国家安全局和国防部。他出席了 Microsoft 的全部 Black Hat Windows 安全通报会议，以及 Internet 安全会议（TISC）。在接受 Foundstone 的首席咨询师职位之前，他是 Internet 安全系统（ISS）的评估官，是 Ernst 和 Young 所负责的国家攻击和渗透组（National Attack and Penetration team）的高级咨询师和 KPMG 的信息分析管理组（Information Risk Management Group）的咨询师。

Erik 毕业于宾夕法尼亚州卡莱尔市迪金森学院，获得计算机科学的理学士学位。1999 年，他被授予 Metzger Conway Fellow 称号。这是一项每年一次的奖赏，授予在自己的研究领域中取得卓越成绩的迪金森优秀毕业生。

Erik 是 Special OPS 项目的第一作者和技术编辑。他提出了本书的概念，组建了作者组，并撰写了第 1，2，3 和 9 章。

其他作者

Chip Andrews（MCDBA）是一位有 12 年经验的程序员和计算机安全咨询师，擅长软件开发过程中的安全咨询。他负责维护专攻 SQL Server 安全问题的 SQLSecurity.com 网站。他是 *"Hacking Exposed：Windows 2000"*（ISBN:0072192623）、*"SQL Server Magazine"*, *"Microsoft Certified Professional Magazine"* 和 *"Dr.Dobbs Journal"* 等书和期刊中关于 SQL Server 安全问题的作者。Chip 也是各种安全会议的发言人，向 SQL Server 用户组讲述企业中实际存在的 SQL Server 安全战略。

Chip 是第 12 章"攻击和防护 Microsoft SQL Server"的作者。

John Bock 是 Foundstone 的研发工程师。他主要擅长无线安全和网络评估技术。John 有很强的网络安全背景，他是一个企业安全组的咨询师和领导者。加入 Foundstone 之前，他作为 ISS 的咨询师执行渗透测试和安全评估，是无线安全的讲解人。加入 ISS 之前，他是 marchFIRST 的网络安全分析师，负责维护一个拥有 7 000 个用户的全球网络的安全。John 是 *"Hacking Exposed：Network Security Secrets & Solutions"*,（第 4 版，ISBN：0072227427）一书中关于无线安全内容的作者。

John 是第 15 章"无线 LAN：发现和防护"的作者。

Earl Crane 是 Foundstone 的咨询师，致力于为寻求 GLBA，HIPAA 和 ISQ17799 解决方案的企业提供安全咨询。作为一名咨询师，Earl 已经为《财富》50 强和全球 2000 强中的许多客户执行了安全评估，制定和检查策略，以及开发和部署安全程序，其中包括 Microsoft，Toyota Motor Credit Corporation，Sempra Energy，Safeco Corporation 和 Pacificare 等公司。加入 Foundstone 之前，Earl 是波音公司 Phantom Works 研发实验室的一名技术人员，负责开发一个能自动装配飞行器机械工具箱的机器人 kitting 系统。在加入波音公司之前，Earl 是 General Electric Aircraft Engines 的一名软件开发人员，设计并编写了一个产品研究数据库。此外，他还用 Capability Maturity Model（CMM），Operationally Critical Threat，Asset and Vulnerability Evaluation 模型（OCTAVE）和 Survivable Network Analysis 模型（SNA）工作。他的公认最好的项目之一是成功地应用 SNA，评估了东海岸医院系统的网络生存能力。Earl 毕业于卡内基·梅隆大学，获得机械工程理学士学位并辅修机器人学。毕业后，他继续在卡内基·梅隆大学学习，获得信息系统管理硕士学位，专攻信息安全。这是一个跨学科的专业，由卡内基·梅隆大学的 CERT/CC、H.John Heinz III 公共政策和管理学院，工业管理研究生院和计算机科学学院共同培养。他毕业时名列前茅，获得"Highest Distinction"称号。

Earl 是第 18 章"创建高效的企业安全策略"的作者。

Hal Flynn 是 Symantec 公司的漏洞分析专家。他主管 SecurityFocus 网站的 UNIX Focus Area，维护 Focus-Sun，Focus-Linux，Focus-BSD 和 Focus-UNIX-Other 邮件列表。在这个领域，他先是一个 Internet 服务提供商的高级系统和网络管理员，然后与美国国防信息系统局签约，后来又成为 Sprint 的企业级咨询师。Hal 居住在加拿大阿尔伯达省卡尔加里市。业余时间，他是一名潜水运动爱好者。

Hal 是第 14 章“攻击和防护 UNIX”的作者。

James C.Foster（CISSP，CCSE）是 Foundstone 公司智能威胁（Threat Intelligence）部门的经理，负责领导一个由研发工程师组成的小组，建立一种检查 FoundScan 套装产品本地和网络漏洞的高级安全算法。加入 Foundstone 之前，James 曾任 Guardent 有限公司的高级咨询专家和研究科学家，《信息安全杂志》（Information Security Magazine）的特邀作者，以及计算机科学公司的信息安全和研究专家。由于他对编程、编写 Web 应用程序、密码学和无线技术的精通，James 已经多次指导了商用 OS 组件的代码评阅、Win32 应用程序评估、Web 应用程序评估、无线和有线的渗透测试，以及查看商用级的密码实施。他曾经多次为政府和企业客户咨询，包括国防部、DCITP、DISA、Federal Reserve Bank、CitiGroup、Dupont、IBM、Merrill Lynch 和 GE。James 是一个经验丰富的演讲者，活跃在遍布北美的会议、技术论坛、安全峰会和研究座谈会上，在微软安全峰会、MIT 无线研究论坛、SANS、MilCon、TechGov、InfoSec World 2001 和 Thomson Security Conference 上都有精彩表现。他也经常被邀请评论相关的安全问题，并被《今日美国》（USAToday）、《信息安全杂志》、Baseline、《计算机世界》、《安全计算》（Secure Computing）和《MIT 工程师》（MIT Technologist）引用。James 拥有商业、软件工程、信息系统管理的学位和证书，以及多部有关计算机或编程的著作。James 还参加或指导耶鲁商业学院、哈佛大学，国会大厦学院（Capitol College）和马里兰大学的研究工作。

James 是第 4 章“攻击和防护 Windows XP Professional”的作者。

Norris L.Joghson,Jr.（MCSA，MCSE，CTT＋，A+，Linux+，Network+，Security＋，CCNA）是一位技术培训教师，并且在西雅图-塔科马地区开办了一家咨询公司。他的咨询业务不仅包括为当地的公司和公众机构提供安全计划，而且还为当地计算机公司的客户提供排忧解难的服务。除了咨询工作，Norris 还为地区社区和技术学校的客户和技术人员提供技术培训。他是许多 Syngress 出版物的合著者，包括最畅销的“*Security+DVD Training & Study Guide*”(ISBN：1-931836-72-8)，“*SSCP Study Guide & DVD Training System*”(ISBN：1-931836-80-9)，“*Configuring and Troubleshooting Windows XP Professional*”(ISBN：1-928994-80-6)和“*Hack Proofing Your Network*”（第 2 版，ISBN：1-958994-70-9）。Norris 还对“*Hack Proofing Windows 2000 Server*”(ISBN：1-931836-49-3)和“*Windows 2000 Active Directory*”（第 2 版，ISBN：1-958994-60-1）进行了技术上的编辑和评阅。Norris 曾获华盛顿州立大学的学士学位。他深深地感谢他的妻子 Cindy 和三个儿子，他们的帮助使他能专

心从事计算机培训和教育工作。

Norris 是第 5 章“攻击和防护 Windows 2000”的作者。

Brian M. Kenyou (CCNA，MCSE)是 Foundstone 企业漏洞管理系统 FoundScan 的产品服务主管。Brian 建构了 Foundstone 安全操作中心，现在还在参与这项服务器的规划和扩展的工作。他目前负责为 FoundScan 客户提供定制安装和培训服务，并和供应商合作，增强产品的互操作性。在加入 Foundstone 之前，Brian 曾致力于为两个技术创业公司设计和保护大型电子商务基础体系结构。在 9 年多的 IT 职业生涯中，Brian 曾经为许多公司提供了结构分析和项目规划咨询服务。Brian 曾获洛亚拉·玛丽蒙特大学（Loyola Marymount University）的学士学位。

Brian 是第 16 章“网络架构”的作者。

David Lichfield 是世界著名的安全专家，专攻 Windows NT 和 Internet 安全。他发现和修正了 100 多个产品漏洞，如微软的 Internet 信息服务器和 Oracle 的应用服务器，使得世界各地的网站更加安全。他也是世界上最流行的免费漏洞扫描工具之一——Cerberus 的 Internet Scanner（以前是 NTInfoscan）——的开发者。除了 CIS，David 还建立了许多其他工具，帮助发现和修补安全漏洞，是许多关于安全的技术文档的作者，以发现了 Slammer 蠕虫所利用的 Microsoft SQL 缺陷而出名。

David 是第 13 章“攻击和防护 Oracle”的主要作者。

Jim McBee（MCSE，MCT）在亚洲、环太平洋各国和美国传授、咨询和讲解关于 Exchange 和活动目录的知识。他的客户名单包括美国国防部、微软、EDS 和其他 500 强的公司。Jim 经常为 Exchange and Outlook Administrator、.Net Magazine，Exchange 新闻组和邮件列表写作。他是流行的“Exchange 2000 Server 24Seven”（ISBN：0782127975）和“*Exchange Server 5.5: 24Seven*”（ISBN：0782125050）的作者。业余时间，他在科罗拉多滑雪或夏威夷海滩上冲浪，吃着辣味热狗，玩笔记本电脑。他住在夏威夷的檀香山。

Jim 是第 7 章“保护 Exchange 和 Outlook 网络入口”的作者。

Haroon Meer(B.Com[Info.Systems]，CAN，CNE，MCSE，CISSP，CCSA，CCSE)是 SensePost 研究和发展部的主管。他毕业于纳塔尔大学，主修信息系统、市场营销和信息系统技术。一年级时他就开始为大学的计算机服务部工作，并担任系统咨询员，主攻网间通信和 Internet 相关系统。2001 年他加入 SensePost，成为技术组的一名成员，用大部分时间研究安全工具的发展和概念验证（proof of concept）代码。他已经发布了一些关于网络/Web 应用程序安全的工具和论文，并出席了 Black Hat 和 DEFCON 会议。

Haroon 是第 11 章“攻击客户 Web 应用程序”的作者。

Aaron Newman 是应用程序安全有限公司（AppSecInc）的创立者和首席技术执行官，被公认是世界上最优秀的安全专家之一。他与人合著了一本关于 Oracle 安全的书，并在世界各地发表数据库安全的演讲。创立 AppSecInc 之前，Aaron 建立了 DbSecure 和

ACN 软件系统。他还在 Internet Security Systems，Bankers Trust 和 Price Waterhouse 担任过其他技术咨询职位。

Aaron 是第 13 章“攻击和防护 Oracle”的作者。

Michael O'Dea 是 Foundstone 的运营主管，为其漏洞评估产品和所提供的服务提供支持和定制服务。Michael 从 1995 年开始从事信息管理和安全保证工作，着重于运营安全实践、事故响应和过程自动化。加入 Foundstone 之前，Michael 曾担任迪斯尼集团的网络服务分支——迪斯尼世界服务有限公司的高级 Internet 安全分析师和 Network Associates 有限公司全球专业服务部门的咨询师。

Mike 是第 17 章“构建人力资源因素”的作者。

Vitaly Osipov（CISSP，CCSE，CCNA）是 Syngress 出版的“*Check Point Next Generation Security Administration*”（ISBN:1-928994-74-1）和“*Managing Cisco Network Security*”（第 2 版，ISBN: 1-931836-56-6）的合著者。他最近 6 年在欧洲的一些公司任咨询师，专长是设计和实施信息安全解决方案。业余时间，他还为防止垃圾邮件的公司 CruelMail.com 提供咨询服务。Vitaly 十分愿意把他的谢意传达给许多英国朋友，特别是一位爱尔兰朋友。

Vitaly 是第 6 章“保护活动目录”的作者。

Matthew Ploessel 是 Foundstone 公司的网络安全工程师。他十分精通 DoS、不对称加密、入侵检测系统和 BGP 工程。同时，Matthew 还是加利福尼亚州洛杉矶的 Internet 服务提供商——Niuhi 公司的 CTO、一名经验丰富的讲师、IEEE 成员。Matthew 作为几个强大的地下黑客组织的主要成员，在 19 岁之前就成为了 CCIE 的候选者。他曾为许多大的通信公司、国际银行和福布斯排行前 100 名的企业提供安全服务。Matthew 还是“*Hacking Exposed:Network Security Secrets & Solutions*”（第 4 版，ISBN: 0072227427）的主要作者。现住南加州。

Matthew 是第 8 章“攻击和防护 DNS”的作者。

Roelof Temmingh（B.Eng[electronic]）是 SensePost 的技术主管和创立者之一。他 1995 年完成了电子工程学位的学习，在 Crypto Development House Nanoteq 担任了 4 年系统架构师。2000 年，他和南非 IT 安全评估思想的领导者一起创立了 SensePost。在 SensePost，Roelof 致力于实现关于 Web 应用程序安全、特洛伊木马/蠕虫/病毒技术和自动跟踪的复杂概念。最近两年，Roelof 在一些会议上发表了论文，包括 SummerCon，Black Hat，DEFCON 和 RSA 会议。

Roelof 是第 11 章“攻击客户 Web 应用程序”的作者。

特殊作者

Steven Andrés (CISSP，NSA，CCNP，CCSE，MCSE-2000)是 Foundstone 公司的安全工程师。他的职责是管理基础体系结构，保证 Foundstone 公司管理安全服务的可靠性。他还负责所有 FoundScan 软件许可证和应用一个双层分布网络提供安全升级产品和管理服务。Steven 是全球畅销书“*Hacking Exposed:Network Security Secrets & Solutions*”（第 4 版，ISBN:0072227427）的主要作者。加入 Foundstone 之前，他曾在最大的 Private Tier-1 ISP 架构安全网络的主机管理分部任职，拥有 8 年维护娱乐、金融和高等教育工业的高可靠网络的经验。Steven 持有加利福尼亚州洛杉矶大学的文学学士学位。

Dave Aitel 是位于纽约的安全咨询和产品公司 Immunity, Inc.（www.immunitysec.com）的创立者。Immunity 的产品 CANVAS 和开发源代码项目 SPIKE 被世界各地的金融、政府和咨询机构广泛采用。

Dave Cole 是经验丰富的信息安全专家，具有 7 年实践和管理经验。他曾就职于 Deloitte&Touche LLP 和 ISS，他领导 Pacific Northwest 的咨询活动。目前，Dave 担任 Foundstone 的产品主管，负责指导公司旗舰技术的设计和开发。

Joshua Leewarner（CISSP，MCSE）是 Deloitte&Touche LLP 企业风险服务方面的高级咨询师。过去 6 年，他一直在信息技术和安全咨询领域工作，侧重于微软产品和技术的安全。他编著了几本评价微软操作系统安全性能的白皮书，一些 Web 安全课程和一本关于 Windows 2000 PKI 实施的实验课教程。Joshua 在华盛顿州的西雅图太平洋大学获得计算机科学文学学士学位。

Aaron Rhodes 是 Foundstone 公司的安全咨询师，主要为 Foundstone 公司的客户提供网络安全服务。Aaron 曾是 Cisco Systems 安全咨询组的成员、一家计算机安全公司的创立者、美国空军第 609 信息战空军中队的成员。Aaron 在科罗拉多州的美国空军学院获得运筹学专业（Operations Research）的理学学士学位。

Melanie Woodruff（CISSP，MCSE）是 Foundstone 公司的高级咨询师，擅长攻击和渗透评估。在 Foundstone，Melanie 有丰富的针对不同用户的咨询经验，包括银行、政府和零售业。她还主讲 Foundstone 的 Ultimate Hacking 和 Ultimate Hacking NT/2000 Security 课程。Melanie 是全球畅销书“*Hacking Exposed:Network Security Secrets & Solutions*”（第 3 版，ISBN:0072193816）的主要作者。作为一名测试客户，她与许多商业拨号软件供应商保持着密切联系，提供 bug 报告和性能改善建议。

技术编辑和作者

Mark Burnett 是一位独立安全咨询师和自由作家，专攻 IIS 保护。他是“*Maximun Windows Security*”（ISBN：0672319659）和“*Dr.Tom Shinder's ISA Server and Beyond:Real Word Solutions for Microsoft Enterprise Networks*”(Syngress Publishing，ISBN：1-931836-66-3)的合著者，同时是许多有关安全技术的杂志、时事通讯和 Web 出版物的长期作者。作为 www.iissecurity.info 的编辑，Mark 与全球安全研究人员一样，共享他的独特经验。

Mark 是第 10 章“保护 IIS”的作者。

技术编辑

Eric Schultze 是 Shavlik Technologies 公司产品研究和发展的主管，负责 Shavlik 的产品版本和实施。他最近担任微软安全响应中心的程序管理员和微软 Trustworthy Computing 组的高级技术人员的职务，负责管理微软安全补丁和公告牌发布过程，开发微软产品的安全方案，包括补丁管理和部署方案。加入微软之前，Eric 和其他人共同建立了 Foundstone 公司，指导 Ultimate Hacking：Hands On 培训程序的编写。他的评估、渗透和保护微软的技术形成了 Foundstone 关于 Windows 操作系统的审计和评估方法论。创立 Foundstone 公司之前，Eric 是 Ernst&Young 的国家攻击和渗透组的高级主管，并被公认是公司的微软安全专家。Eric 是“*Hacking Exposed, Network Security Secrets & Solutions*”（第 3 版，ISBN: 0072121270）的主要作者，并经常在业内的各种会议上发表演讲，如 Black Hat，CSI，MIS，SANS 和 NetWorld＋Interop。Eric 在阿姆赫斯特大学获得了心理学和社会学的文学学士学位。

前　言

在快速发展的、躁动不安的、有的甚至是鲁莽无序的计算机安全世界中，把安全类比为“金玉其外，败絮其中”，无疑是正确的，因为我们投入了数百万的资金保护和加固外围网络，却不愿意在解决内部威胁上花一毛钱。然而，让人们能够自由控制内部系统也许很方便，但是一旦有人在毫无防备的内部“咬”一口，就会变成一场灾难。关于这一点，可以想想公司那些有权访问中心的员工和合作伙伴可能带来的危害（无论是有意还是无意的）。对内部松散、混乱的局面缺乏足够的重视可能会在任何时候破坏你的安全。本书作者的目的是让你经常想起人们谈到安全时常忽略的一个方面，即内部安全和“败絮其中”的类比。在这本书中，你会找到使内部系统不受攻击的关键点，以及几乎囊括全部内部安全问题的描述。

保护企业内部安全的任务是令人生畏的：如此多的系统，如此多的漏洞，如此有限的时间。你必须管理无数的系统缺陷，并控制天天如此的网络故障。你必须能把微薄的 IT 安全资源分配给最重要的安全战役。你也许觉得这是几乎不可能做到的。在一天结束的时候，如果不能采取恰到好处的措施来恰到好处地保护适当的资产，你也许会怀疑自己究竟在干什么。动机不等于过程，努力不等于回报。即使你在短期能控制一切，但一些漏洞迟早会挑战这种控制。管理层并不关心存在多少漏洞，弥补这些漏洞有多困难，或者控制它们的方式又多么不同；他们所关心的只是一些问题的正确答案，如“我们是安全的吗？”和“我们的情况变得更好了吗？”，如果你不能对这些问题给出肯定的答案，最终你和你的公司都将不能生存。

本书将有助于你对这些问题给出肯定的答案。书中首先讲述如何确定和理解你的资产、漏洞和面临的威胁，然后介绍如何保护这些资产，使它们避开所面临的威胁。这种方法大多具有 Pareto 法则，或者说 80/20 法则的特性。这种法则经常应用于计算机安全问题，意思是“80%的危险是由 20%的漏洞产生的”。简而言之，集中解决少数最关键的漏洞，就可以消除一大半所面临的危险。

注意

20 世纪之交，一位意大利经济学家 Vilfredo Pareto 观察到意大利 20%的人口拥有 80%的社会财富。这个简单的调查就产生了 Pareto 法则，或 80/20 法则。

遵循这个法则需要两个条件：首先，收集可靠的数据；其次，用可靠的方法分析这些

数据。

第一个要收集的可靠数据变量是*资产清单*，它是最常被低估的安全要素之一。了解有什么资产、它们在哪（如在哪个国家、哪栋楼、哪个房间）、它们有什么重要性和价值，对解决计算安全风险问题具有至关重要的作用，它们可以帮助你建立一个恒定的安全管理程序。

第二个变量就是要确定漏洞。对于收集到“干净”的基础数据而言，企业准确地获取漏洞的能力是最关键的。为此，必须减少误报（明明没有漏洞却说有）和漏报（明明有漏洞却说没有）。

最后一个变量是了解系统面临的威胁。漏洞本身并不是重要的风险——只有当黑客抓住这个漏洞，并写了漏洞利用程序，开始利用它，它才会带来至关重要的风险。要了解你面临的主要威胁，就需要了解地下黑客组织目前的活动，例如，他们如何工作和联系，他们最终如何利用已知的薄弱环节等。不了解这些威胁，就不能安全管理你的数据（你的资产和已知漏洞）。

只有当你收集的数据已足够让你了解系统面临的危险时，你才能开始进入保护系统的工作。本书提供了各种工具和技术，可以帮助你分析数据，并根据 Pareto 法则确定加固你的内部网所必不可少的补丁。你永远不可能 100%的安全，但你可以 100%地确信你最大限度地发挥了所有资源的能量来打赢这场战斗。

数据本身没有什么价值。为了提供一份“风险完全描述”的安全漏洞报告已经浪费了太多的时间。事实上，这些报告除了充满了无关的、互相矛盾的描述和大量不合格的数据外，没有任何价值。没有一个有效、动态、健壮的数据接口，不依据 Pareto 法则行动，你也许永远不能真正解决内部的风险。

“疯狂”的定义是一遍又一遍地做同样的事，却期望不同的结果——所以如果你已经陷入了产生太多未过滤数据的怪圈，那么不要让失败的过去在不经意间重演。现在读这本书吧，注意它的警告，采取行动有效地管理你的安全问题。

——Stuart McClure，Foundstone 公司的主席和 CTO
“Hacking Exposed Fourth，Windows 2000, and Web Hacking Editions”的合著者

目　录