科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

Vista信息安全

Larry Chaffin, Scott Granneman, Laura E. Hunter, Alun Jones,
Jan Kanclirz, Marc Perez, Daniel Sheperd, Matt Sheperd
Robert J. Shimonski, Henrik Walther, Anthony Piltzecker 著

沈晴霓 卿斯汉 等译

Microsoft Vista for
IT Security Professionals

科学出版社

Microsoft Vista for IT Security Professionals

Vista 信息安全

Larry Chaffin
Laura E. Hunter
Jan Kanclirz
Daniel Sheperd
Robert J. Shimonski
Anthony Piltzecker
Scott Granneman
Alun Jones
Marc Perez
Matt Sheperd
Henrik Walther
著

沈晴霓　卿斯汉　等译

科学出版社

北京

图字：01-2008-2609 号

This is a translated version of
Microsoft Vista for IT Security Professionals
Larry Chaffin
Copyright ©2007 Elsevier Inc.
ISBN-10: 1-59749-139-X
ISBN-13: 978-1-59749-139-6

图书在版编目（CIP）数据

Vista 信息安全/（美）查芬（Chaffin, L.）等著；沈晴霓，卿斯汉等译. —北京：科学出版社，2010

（21 世纪信息安全大系）

ISBN 978-7-03-026009-3

Ⅰ.V… Ⅱ.①查… ②沈… Ⅲ.窗口软件，Windows Vista–安全技术 Ⅳ.TP316.7

中国版本图书馆 CIP 数据核字（2009）第 205934 号

责任编辑：田慎鹏 霍志国 / 责任校对：陈丽珠
责任印制：钱玉芬 / 封面设计：耕者设计工作室/封面图片：徐 湛

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销
*
2010 年 1 月第 一 版 开本：787×1092 1/16
2010 年 1 月第一次印刷 印张：29 1/2
印数：1—4 000 字数：696 000

定价：59.80 元
（如有印装质量问题，我社负责调换<环伟>）

技术编辑

Tony Piltzecker (CISSP, MCSE, CCNA, CCVP, CCSA, Citrix CCA) Syngress 出版的"*MCSE Exam 70-296 Study Guide and DVD Training System*"一书的作者和技术编辑，是马萨诸塞州 Woburn 网络信息系统的咨询工程师。他也是"*How to Cheat at Managing Microsoft Operations Manager 2005* "(Syngress, ISBN:1597492515)一书的贡献者。

Tony 的专长包括网络安全设计、微软操作系统和应用架构，以及思科 IP 电话实施。他曾任职 SynQor 公司的 IT 经理、设计系统网络架构和集成信息系统的高级网络咨询顾问。除了拥有不同的资格证书外，他还获得了商业管理的学士学位。目前，他和妻子 Melanie 以及女儿 Kaitlyn 和 Noelle 定居在马萨诸塞州的 Leominster。

贡 献 者

Larry Chaffin 是 Pluto 网络的 CEO/主席/创建者，这是一家分布在 23 个国家的致力于 VoIP、WLAN 和安全方面的图书写作的虚拟网络咨询公司。他是一位签约作者。他也是“*Managing Cisco Secure Networks* ”(Syngress, ISBN：1931836566)、“*Skype Me!*”(Syngress, ISBN：1597490326)、“Practical VoIP Security”(Syngress, ISBN: 1597490601)、“*Configuring Check Point NGX VPN-1/Firewall-1*”(ISBN: 1597490318)和“*Building a VoIP Network with Nortel's Multimedia Communication Server 5100*”(Syngress, ISBN: 1597490784)的贡献者。他也与其他人合作了关于 VoIP、WLAN、安全和光纤技术的其他 11 种科技图书。他获得了超过 29 种来自公司的证书，如 Avaya、Cisco HP、IBM、isc2、Juniper、微软、Nortel、PMI 和 VMware 等公司。他曾为 22 个国家的许多财富 100 强的公司做过 VoIP、WLAN、安全和光纤网络的主要架构设计。他被同行看作 VoIP 和安全领域在全球范围内的最值得尊敬的专家之一。他的大量时间花费在教学和指导全球的 Voice/VoIP、安全和无线网络领域的初级人员/工作组。目前，他在进行“*Building a VoIP Network with Nortel's Multimedia Communication Server 5100*”一书的后续工作，而且在写一本关于 Cisco VoIP 网络、微软 Vista 和 VoIP 实践案例分析的书。

Larry 合作编写了第 1 章。

Scott Granneman 是一位作者、教师和咨询顾问。他是 *SecurityFocus* 和 *Linux Magazine* 月刊的专栏作家，也编写了 3 本关于开放资源技术方面的图书，这些图书以不同的方式关注安全问题——“*Don't Click on the Blue E!: Switching to Firefox*”、“*Hacking Knoppix*”和“*Linux Phrasebook*”。作为在 St.Louis 的华盛顿大学和 Webster 大学的兼职教授，他讲授关于安全、技术和 Internet 的一系列受欢迎的课程。作为主要的 Web 管理人员，他管理公司的基于 UNIX 的服务器环境，帮助开发公司的内容管理系统——被教育的、商业的和非营利性的客户广泛使用。

Scott 编写了附录 A 和附录 B。

Laura E. Hunter (CISSP, MCSE: 安全, MCDBA, 微软 MVP) 是一位致力于公司组织和人员结构的活动目录架构师，她负责网络规划、实施，以及排除活动目录和其他微软技术的故障。她的专长包括 Windows 2000 和 2003 活动目录设计和实施，排除故障和安全主题。她有 Windows 计算机方面的 10 多年的经验；她曾担任过 Pennsylvania 大学的 IT 项目经理和救世军的计算机服务的主任。她对 Web 站点的教学目标组和 *Redmond Magazine*（以前是微软 *Certified Professional Magazine*）有过贡献。

Laura 曾以 DVD 制作、作者和技术审查的方式对 Syngress 的“Windows 服务器 2003 MCSE/MCSA DVD 指南与训练系统”系列图书有过贡献。她是 APress 的

"*Active Directory Consultant's Field Guide*"(ISBN: 1-59059-492-4)的作者，以及是O'Reilly 传媒的"*Active Directory Cookbook, Second Edition*"(ISBN: 059610202X)的合作者。她获得 4 次著名的 Windows 服务器-网络领域的微软 MVP 奖。她获得 Pennsylvania 大学的计算机科学硕士学位，也是自由作家、培训师、演讲人员和咨询顾问。

Laura 编写了第 6 章。

Alun Jones (MVP, MCP) 是得克萨斯帝国软件公司的主席。得克萨斯帝国软件公司开发安全网络软件，提供安全工程咨询服务。得克萨斯帝国软件公司的旗舰产品是 WFTPD Pro——一种完全由 Alun 编写的服务于 Windows 的安全的 FTP。

越来越多的 WFTPD 的支持需求——表明在网络上有很少公司来试着满足安全安全需求——使 Alun 进入安全工程领域。目前，他是坐落于美国西北海岸的一家健康保险提供商 Premera Blue Cross 的信息系统安全工程师。

Alun 进入 Corpus 基督学院、剑桥和 Bath 大学进修，但还没有完成学业。目前，和妻子 Debbie 及儿子 Colin 生活在华盛顿的 Seattle。

Alun 编写了第 5 章。

Jan Kanclirz Jr. (CCIE #12136-安全, CCSP, CCNP, CCIP,CCNA, CCDA, INFOSEC Professional, Cisco WLAN 支持/设计专家) 是 IBM 全球服务部门的高级网络信息安全架构师。Jan 擅长为多种技术，如 VPNs、IPS/IDS、 LAN/WAN、防火墙、内容网络、无线和 VoIP，提供多方设计和售后实施。除了网络设计和工程方面，Jan 的专业背景还包括关于开放资源应用和 Linux 的大量经验。Jan 对 Syngress 的几种图书有过贡献："*Managing and Securing Cisco SWAN*"、"*Practical VoIP Security*"和"*How to Cheat at Securing a Wireless Network*"。

除了在 IBM 全球服务部门的时间外，Jan 还运营一家安全门户网站 www.MakeSecure.com，在这里他把时间贡献给安全意识和咨询。Jan 生活在 Colorado，享受户外探险。他感谢家庭成员 slunicko 和朋友对他的支持。

Jan 编写了第 7 章。

Marc Perez (MCSE:Security, Security+) 是马萨诸塞州波士顿网络信息系统的高级咨询顾问。依据在微软的网络信息系统经验，他为坐落于东北区域的中等规模和企业级的客户提供策略和技术咨询。关注于消息和协作解决方案的安全集成目录服务，他为企业向更有效的、重要的、通信的技术投资提供必要指导。

他毕业于 Southern Maine 大学，为波士顿地区的多个组织做过咨询，并且在 New England 地区起到了作用，包括为期 4 年的 MBNA 美国银行信息安全经理。目前，他和妻子 Sandra，以及两个孩子，Aidan 和 Lucas，生活在北岸。

Marc 编写了第 8 章。

Daniel Shepherd(MCP,GSEC) 是石油液化气贸易协会的 IT 经理。其总部设在华

盛顿。D.C.Dan 为协会提供全方位的 IT 服务，这些服务包括设计、管理、企业网络的故障排除。仅约 30 多位员工却能承载为协会的 4000 多位员工提供服务。DAN 所设计和执行的项目,用于集团全范围内办公室的网络电话，网络基础设施的升级更新，由于软硬件服务器老化所引起的检修，虚拟化网络服务环境资源利用的提高以及通过隔离作用保护网络安全。

Dan 曾供职于一家快速成长餐饮公司在东南部地区的一个销售网点的网络管理者。还曾在 Faith Based Design Inc.公司担任过顾问，主要为美国军方提供培训、技术写作及相关工程领域的服务。

Daniel 撰写了本书的第 9 章，并与其他作者共同合作撰写了本书的第 1 章。

Matt Shepherd(CISSP,MCSE,GCFW,CEH) 是 Project Performance Corporation 公司，McLean,VA. 项目的顾问,Project Performance Corporation 公司在安全工程体系方面拥有强大的实力，可以用最好的设备为客户在公共及私人区域提供高效安全的解决方法。Matt 凭借自己作为网络高管、IT 经理的实践经验以及该项目的安全体系为 Project Performance Corporation 的客户提供高质量的解决方案。Matt 取得了马里兰州 St.Mary's 大学的学士学位，目前正在攻读信息安全的理学硕士学位。

Matt 在此向自己的妻子 Leena 致谢，感谢在他做这个项目过程中给予的大力支持。感谢他一生钟爱的家庭，是家庭的爱和支持让他的每一天都感到特别。同时还要感谢他的弟弟 Daniel 与他一起完成这个项目。

Matt 在此向他在 PPC 公司的同事 Mike Nigro,Martin Wright,Jan Hill 对于他这个项目所给予的所有支持表示感谢，还要感谢微软公司的 Shon Eizenhoefer 及时为 MATT 提供了相关问题清晰而准确的解决方法。

Matt 撰写本书第 4 章。

Robert J.Shimonski(MCSE) 是一名企业家、畅销作家以及上百种公共书刊和杂志、行业文章的编辑。Rob 在他所撰写的每一页通过对当今最具挑战性行业的内部及技术环境的咨询了解，为读者们提供了最前沿的行业知识。Rob 总是站在时代的尖端上，时时根据现实世界的前景报导着行业的状态。作为本书的作者之一，Rob 目前在为全球的一家大公司分配测试并发展保护 Vista 图片及设计 Longhorn 的升级。

对于 Sygress,Rob 已写过很多备受读者青睐的书，包括“The (ISC)2 SSCP Study Guide and DVD Training System” (ISBN 1931836809)、“The Best Damn Firewall Book Period!” (ISBN 1931836906)、“Designing and Building Enterprise DMZs” (ISBN1597491004)、“ Nokia Network Security Solutions Handbook ” (ISBN1931836701) 、“ Sniffer Pro Network Optimization and Troubleshooting Handbook ” (ISBN 1931836574)、“Configuring and Troubleshooting Windows XP Professional with CD-ROM” (ISBN 1928994806)、“Configuring Symantec Antivirus Corporate Edition” (ISBN 1931836817)和 “the Network+ Study Guide & Practice Exams: Exam N10-003” (ISBN 1931836426)。Robg 还帮助 Syngress 开发了第一个

DVD video，并推出了最为畅销的书“The Security + Study Guide and DVD Training System ”(ISBN 1931836728)。

Rob 经营着自己的媒体公司 Sound Room Studios Inc.，公司位于 Long Island，NY。他负责生产，还是电视音频和视频的工程师，负责电子产品的分销。

Rob 撰写了本书的第 2 章和第 3 章。

Henrik Walther(交互 MVP,MCSE 信息/安全) 是微软公司的黄金搭档 Interprise Consulting A/S 公司的高级顾问。其公司总部设在丹麦的哥本哈根。Henrik 有 14 多年的 IT 行业的从业经验。他曾从事 Microsoft Exchange、ISA Server、MOM、IIS、集群技术、活动目录以及虚拟服务器技术。

此外，他还是交换系统的专家。Henrik 负责 Danish 网站的 Exchange-fap.dk 运行。他是这个网站内容的主要创作者、著名的论坛主持人，以及时事快讯的编辑。他的作品有“*CYA: Securing Exchange Server 2003 & Outlook Web Access*”(Syngress, 2004)。他还是其他几本信息类图书的评论家（包括另外的几本 2007 年出版的关于网络交换系统的书）。

Henrik 撰写了本书第 10 章。

（刘晓颖　译）

前言贡献者

Brien Posey 是 Relevant Technologies' Vice（www.relevanttechnologies.com)的研究与发展的总裁。 Brien 先前是全国医疗保健设施网络链信息系统的董事，高级网络防御工程师。公司设在诺克斯堡。他还是几个主要科技出版社的编辑，以及全国最大一家保险公司的高级网络管理者。

Brien 是一位在科技方面屡获殊荣的作者，如微软认证的系统工程师(MCSE)、微软的 MVP。他曾撰写或提供作品材料的书有 28 种。他在各种网站上发表及出版的文章大概有 3000 多篇，其中包括 CNET, Jupiter Media, Microsoft's TechNet Magazine,Windows Magazine,Windows Networking,TechTarget 和 *ZDNet*。

前　言

2001 年，IT 界庆祝人们期待已久的微软的 Windows XP 的发布。Windows XP 的发布对微软来说是一个重要的里程碑，因为这是该公司首次同时为企业和普通用户制作一个基于 NT 内核的操作系统。Windows XP 的目的是永远摒弃基于 DOS 的操作系统，例如 Windows 9x 和 Windows ME。可惜，庆祝的时日不长，因为很明显，Windows XP 及其 Internet Explorer 同时遭受到许多安全问题。

起初，这些安全问题大多只被企业所关注。但时隔不久，消费者也开始感觉到了这些安全漏洞的后果。像木马、间谍软件、弹出窗口和浏览器黑客等滋扰行为迅速从默默无闻状况发展成为几乎一夜之间流行起来。

2003 年，微软正在为 Windows XP 的 SP2 努力工作着，SP2 原本要形成一个由一系列重要的安全补丁和修补程序捆绑成的服务包，但在受到 Slammer 病毒侵袭后，这一切都发生了变化。

微软开发团队当时正在全力开发一个新的桌面操作系统，代号为 Longhorn（现在称为 Windows Vista）。Longhorn 预计包括可有效防止 Slammer 类型蠕虫的代码。但这个新的操作系统还需要几年才可以发布。

由于担心其他的 Slammer 类攻击，微软副总裁 Jim Allchin 做出一个决定，即暂停 Longhorn 的开发，并命令将 Longhorn 的代码应用到 Windows XP 并包含到 SP2 中。

SP2 发布于 2004 年 8 月 6 日。但是，该服务包没能修复 Windows XP 中的所有安全问题，尽管它在一定程度上起到了帮助作用。但回过头来看，微软根据 Longhorn 中的代码建立 SP2 应该是一件好事情。因为这个策略使公司有机会看到：这些代码并不是完全安全的。因此，这也为微软提供了一个机会，即在发布 Vista 之前重写这些代码。

不过，所有努力似乎得到了回报。Windows Vista 是第一个基于微软提倡的可信赖计算目标发布的桌面操作系统，毫无疑问是微软目前发布的最安全的操作系统。

即便如此，Vista 并不是完全安全的。如同微软以前的每个操作系统版本一样，Vista 是高度可定制的，配置 Vista 使用的设置发挥如何真正保证操作系统安全的作用。举例来说，当新的安全威胁被发现时肯定就会有 Vista 安全更新被发布。但是，如果 Vista 没有被配置为接受这些更新，那么它的安全性比更新的 Vista 版本更弱。

对 IT 安全专业人员来说，微软 Vista 是很有帮助的。本书讨论了 Vista 中所有的增强的安全机制，还展示了如何配置这些安全机制来获得最佳安全。

—Brien M. Posey
技术部研发副总裁
www.relevanttechnologies.com

目　录