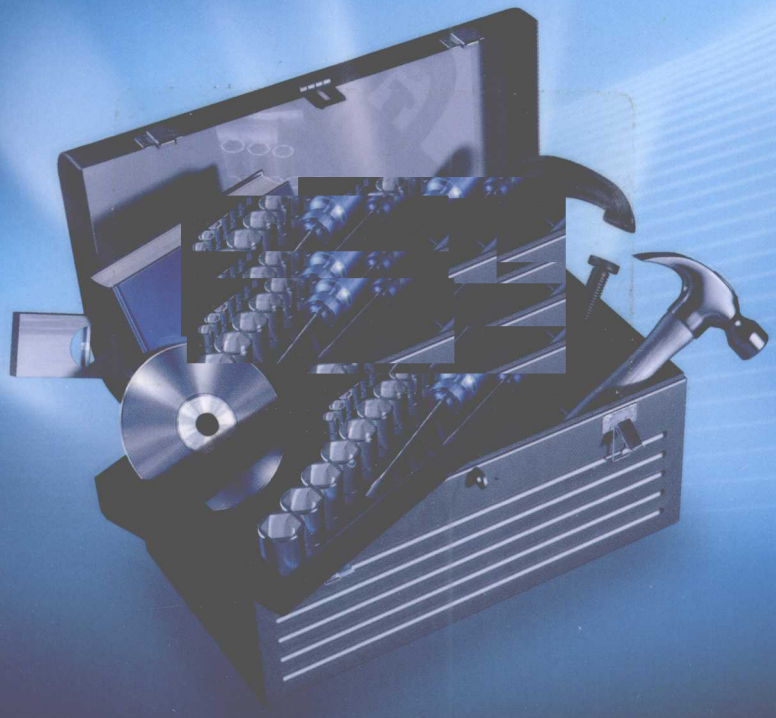
Microsoft

Windows Server 2008

安全技术详解

[美] Jesper M. Johansson 等 著
刘晓辉 陈祎磊 译
马倩 校



人民邮电出版社
POSTS & TELECOM PRESS

Windows Server 2008
安全技术详解

[美] Jesper M. Johansson 等 著
刘晓辉 陈祎磊 译
马倩 校

人民邮电出版社
北京

图书在版编目（CIP）数据

Windows Server 2008 安全技术详解 / （美）约翰逊等著 ; 刘晓辉, 陈祎磊译. -- 北京 : 人民邮电出版社, 2010.6
ISBN 978-7-115-22628-0

Ⅰ. ①W… Ⅱ. ①约… ②刘… ③陈… Ⅲ. ①服务器—操作系统（软件）, Windows Server 2008—安全技术
Ⅳ. ①TP316.86

中国版本图书馆CIP数据核字(2010)第054631号

Windows Server 2008 安全技术详解

◆ 著 [美] Jesper M.Johansson 等
译 刘晓辉 陈祎磊
校 马 倩
责任编辑 刘 浩

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：23.75
字数：536千字 2010年6月第1版
印数：1－2 500册 2010年6月北京第1次印刷

著作权合同登记号 图字：01-2008-3848号
ISBN 978-7-115-22628-0

定价：69.00元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

Windows Server 2008 是 Microsoft 服务器操作系统旗舰产品的升级版，不仅具备优异的特性，并且部署起来更加安全。

本书是 12 位顶级 IT 专家的心血结晶，结合彼此在各领域中的专长，为读者打造了这本 Windows Server 2008 安全指南。本书包括 3 篇：Windows 安全基础、实现身份与访问（IDA）控制和常用的安全方案。

本书结构严谨、组织清晰，包含大量专家的实际经验，是大中型企业中 IT 安全专业人员的必备参考书。

致谢

本书的出版得到了很多人的大力帮助，在此笔者深表感激。他们在本书的撰写过程中起到了不可或缺的作用，可以说，没有他们的努力，就不会有本书的问世。

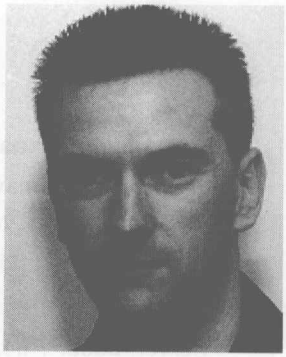
这些可敬的朋友包括：Chase Carpenter、Aaron Margosis、Paul Young、Pablo F. Matute、Dana Epp、Charlie Russel、Wolfgang Schedlbauer、Nick Gillot、Steve Riley、John Michener、Greg Cottingham、Austin Wilson、Chris Black、Ed Wilson、Erin Bourke-Dunphy、Kirk Soluk、Lara Sosnosky、Lee Walker、Tal Sarid、Dan Harman 和 Richard B. Ward。

特别要感谢的是：技术编辑 Mitch Tulloch，他审阅了本书的每个细节，使此书表达的观念更加明确；文案编辑 Becka McKay，她统一了 12 位作者的风格，使本书的文法更为顺畅；Devon Musgrave，他协调了整个团队，使我们的步调更加一致；Maureen Zimmerman，她安排了团队分工，使本书撰写有条不紊；最后要感谢的是 Martin DelRe，他负责与 12 位作者沟通，为本书提供了全面的指导。

关于作者

与之前工具箱那本书不同，本书并非由一名作者独立完成，大多数章节都是由相关领域的专家负责撰写的。服务器非常复杂，Windows 服务器尤其繁琐。因此，12 名 IT 专家通力合作，结合彼此在各领域中的专长，为读者打造了这本《Windows Server 2008 安全技术详解》。

Jesper M. Johansson



Jesper M. Johansson 是本书的主要作者，他设计了本书的架构，并且组织了作者团队。如果本书有拍案叫绝之处，应当归功于其他合著者的汗水和智慧，倘若本书有某些遗漏的地方，Jesper M. Johansson 才是当之无愧的罪魁祸首。

在信息安全和 Windows 安全方面，Jesper M. Johansson 是知名作者，他现在是首席软件安全设计师，负责设计软件的基础结构。Jesper 曾经专注于微软的安全问题，从入侵网络到设计安全软件都有涉及。Jesper 在信息安全方面有很多成就，他出席了许多重要安全会议，并撰写了很多安全方面的文章，甚至还是微软安全 MVP（Most Valuable Professional，最有价值专家）。Jesper 拥有管理信息系统的博士学位，他是一名 CISSP（Certified Information Systems Security Professional，国际信息安全认证专家），并且是 ISSAP（Information Systems Security Architecture Professional，信息系统安全架构专家）。在业余时间，Jesper 则是一名佩戴水肺的潜水教练。

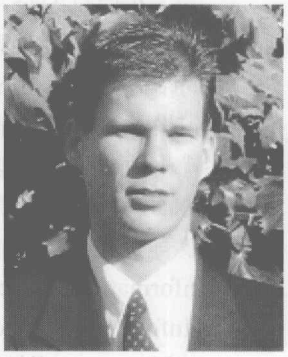
Jimmy Andersson

Jimmy Andersson 是瑞典 Q Advice AB 的首席顾问，专注于目录服务。他也是一名培训师，并且开发了名为“AD 疑难解答与高级理论”的 AD（Active Directory，活动目录）课程。最近 9 年间，Jimmy 每年都获得了微软颁发的 MVP，他的身份是全球企业计划的目录服务项目主管。

Susan Bradley

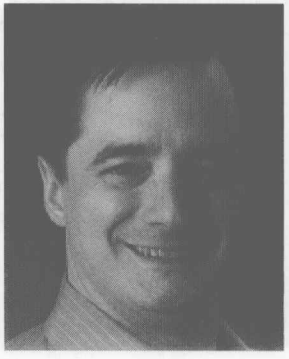
在公司买进第一台 IBM 8088 时，Susan 就开始使用计算机了。作为一名致力于技术的专家，她研究过基于软盘和 Novell 的网络安全，现在她的主要方向是微软的网络安全。在研发和设计本公司安全技术的同时，她还加入了其他行业协会，专注于推进中小企业的安全软件发展。离开 sbsdiva.com 的博客后，Susan 开始为 WindowsSecrets.com 撰写软件补丁方面的文章。她善于使用 Windows Vista，在本书的编写过程中，她甚至从来没有触发过 UAC 提示。并且，Susan 是微软的中小企业服务器 MVP （微软公司评选的公司外最有价值专家）。

Darren Canavor



Darren Canavor 是微软的缔造者之一。他在 1999 年就加入了微软，并且对 Windows 核心操作系统的设计和测试做出了卓越的贡献，其中包括 Windows 2000 中的 PKI 和 Windows Server 2003 中的证书服务，以及 Windows Vista 和 Windows Server 2008 中的用户账户控制。Darren 还是一名特约作者，他参与撰写了很多白皮书和微软出版社的安全及 PKI 方面的书籍，例如《Windows Vista 安全指南及部署》和《使用 Windows Server 2003 实施交叉认证和合格的次级凭证》。

Kurt Dillard



在阿根廷风光秀丽的首都布宜诺斯艾利斯，Kurt 写了很多书和文章，提出在计算机上保护数字信息和存储数字信息的方法。他参与制定了许多微软发布的解决方案，例如《Windows Server 2003 安全指南》、《安全风险管理指南》和《风险与对策：Windows Server 2003 和 Windows XP 中的安全设置》。Kurt 出席了数目众多的会议，包括 RSA、TechEd 和微软联盟安全峰会。他现在持有的证书包括 CISSP、ISSAP、CISM 和 MCSE + Security。

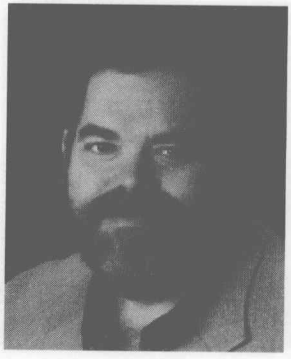
Eric Fitzgerald

Eric (CISSP，MCSE) 在微软的 Forefront Security 产品分部工作，他专注于分析安全传感器所收集的数据。Eric 在 Windows Core OS Security 团队中研究了 6 年的审核和授权技术，并且多年为微软的企业客户提供技术支持，协助他们解决安全、网络和目录服务方面的问题。在业余时间，Eric 最喜欢的运动是帆船竞赛。

Roger Grimes

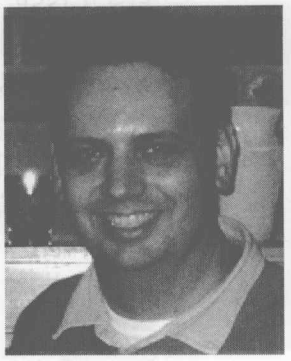
Roger A. Grimes（CPA、CISSP、CISA 和 MCSE: Security）是一名有 22 年工作经验的安全专家，他致力于主机安全、PKI、身份管理以及防范黑客和恶意软件方面。Roger 是微软 ACE 团队的高级安全顾问，并且是 InfoWorld 杂志的安全专栏作家。他参与撰写了 8 本计算机安全方面的书，并且在国内杂志上发表了 200 多篇文章。Roger 使用 8 个蜜罐（honeypot）来截获黑客的活动，在世界各地巡回报告，并且帮助客户保护网络安全。

Byron Hynes



Byron Hynes 是微软的企业技术规划师。自从 2005 年加入微软后，他一直致力于安全技术方面，包括 BitLocker 驱动器加密、用户账户控制以及其他技术。Byron 与客户紧密合作，许多帮助文件、Web 站点、杂志文章、书籍和简报都是出自他的手笔。Byron 喜欢离开办公室去参加各种会议和活动，只要老板允许，他就会去与客户交流。Byron 生于加拿大，他的大部分时间都是在遥远北方的寒冷冬季度过的。他现在都不相信自己会定居在 Washington 的 Redmond 郊区。Byron 已经结婚了，并且有两个天真活泼的儿子。

Alun Jones

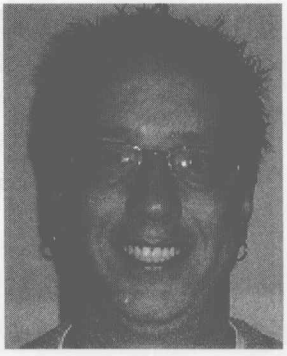


Alun Jones (MVP，MCP) 是 Texas Imperial Software 的总裁。Texas Imperial Software 专注于研发安全网络软件和提供安全工程顾问服务，它的软件旗舰产品是 WFTPD Pro，用于 Windows 的一款安全 FTP 服务器，并且完全由 Alun 编写。越来越多的 WFTPD 支持需求表明，企业要保障网络的安全，必须要有软件的协助，而正是在这种情形下，Alun 开始向安全领域进军。Alun 的日常工作是为一家在线旅游订票公司提供安全规划。Alun 曾经就读于 Corpus Christi 学院、剑桥大学和 Bath 大学，现在和妻子 Debbie 、儿子 Colin 一起居住在 Washington 的 Seattle 附近。因为忙于这本书，Alun 很少回家，他非常感谢妻子和儿子对他的支持。另外，Alun 还是微软的安全 MVP。

Brian Komar

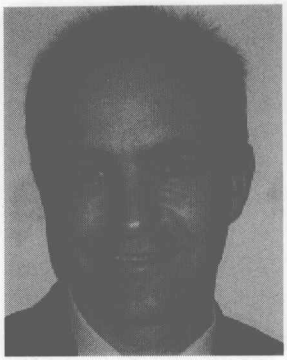
Brian Komar 是 IdentIT 的总裁。IdentIT 是致力于规划和实施公共密钥基础设施与集成身份认证的咨询公司。Brian 与微软的关系非常紧密，他编写了 PKI 和 ILM 2007 培训材料和白皮书，并且是企业 PKI 和 ILM 2007 部署战略的首席顾问。Brian 常常在 IT 行业会议中发表演讲，例如微软 TechEd、微软 IT 论坛以及 Windows IT Pro Magazine Connection。Brian 也是一位微软安全 MVP。

Brian Lich



Brian Lich 是 Windows 服务器用户协助组的核心安全技术作家，他负责撰写活动目录权限管理服务方面的内容。在加入微软之前，Brian 作为一名系统管理员和安全分析专家，在信息技术行业工作了长达 11 年之久。Brian 在 Purdue 大学取得了电子工程技术学位。

Darren Mar-Elia



Darren Mar-Elia 是 SDM 软件的首席技术总监和创始人，在信息技术和软件部署方面有 20 余年的经验。他是 DesktopStandard（已被微软收购）的产品工程高级总监，并且曾经是 Quest Software 的 Windows 管理解决方案首席技术总监。Darren 以前是 Charles Schwab & Co 的分布式系统总监，负责企业的 Windows 技术应用。他参与撰写了 12 本关于 Windows 管理方面的书籍，并且是微软组策略 MVP。Darren 创建了 gpoguy.com 网站，提供组策略的相关信息和工具。

前　言

在本书面市之际，相信读者和笔者一样，也是激动不已的。当然，这并不是仅仅因为这本书，而是在于其所展现的一片广阔天地。

Windows Server 2008 是 Microsoft 服务器操作系统旗舰产品的升级版。研发人员做了大量工作，确保 Windows Server 2008 不仅具备优异的特性，并且部署起来更加安全。本书可以作为用户探索 Windows Server 2008 新特性的指南，使工作更加得心应手。本书同样针对 IT 专业人士，介绍了 Windows Server 2008 某些鲜为人知的功能。

本书包含所有工具包中的应有技术细节，这是 12 位顶级 IT 专家的心血结晶，值得一提的是，每位参与撰写的专家都是其所在领域的佼佼者，他们的著作总数已经超过了 20 本。

概述

本书由 16 章组成，这些章节由以下三个部分组成。

第 1 部分：Windows 安全基础

- 第 1 章“主体、用户以及其他角色”　本章叙述在 Windows 中如何管理用户和其他对象。
- 第 2 章“认证系统和认证协议”　在定义了一个对象以后，必须对其进行身份认证。本章叙述在 Windows 中，认证是如何进行的。
- 第 3 章“管理对象”　用户访问的目标，例如文件和注册表项等，必须确保是安全的。本章探讨如何实现这一点。
- 第 4 章“用户账户控制（UAC）”　Microsoft 在 Windows Vista 中引入了用户账户控制（UAC）的概念。作为一名服务器管理员，应当了解 UAC，这样才能合理地管理服务器。但是，如果是在比较大的 IT 范围内工作，就必须知道如何使用 UAC 来保护工作网络。本章正是讲解这方面内容的。
- 第 5 章“防火墙和网络访问保护”　Windows 中最主要的防火墙就是 Windows 高级安全防火墙。本章介绍该防火墙在 Windows Server 2008 中的工作原理。
- 第 6 章“服务”　如果一个进程必须运行，而不管用户是否登录，那么该进程就会以服务的形式加载。因此，服务就极其容易受到恶意攻击，相应的用户也必须了解其安全策略。
- 第 7 章“组策略”　当使用 Windows 网络连接的时候，应用组策略是明智的选择。修改系统安全设置的工作大多数都是由组策略来完成的。

● 第 8 章“审核” 审核是非常有用的，可以证明某个程序在做什么。审核是安全的基本元素之一。本章详细介绍了审核是如何在 Windows 中工作的。

第 2 部分：使用活动目录实现身份与访问控制

● 第 9 章“活动目录域服务安全性设计” 任何人都可以创建一个活动域名配置，但是想要使之有助于提升网络安全级别，就需要一定的技巧了。本章将讲授这方面的知识。

● 第 10 章“活动目录证书服务” 很多人认为公共密钥基础设施（PKI）是多余的。然而在大多数情况下，它却是非常必要的，本章介绍在 Windows Server 2008 中 PKI 的新特点。

第 3 部分：常用的安全方案

● 第 11 章“服务器角色安全” Windows Server 2008 最显著的特点是取消了以前的程序安装方式，取而代之的是以基于角色方式来工作的服务器管理控制台。本章介绍该变动对于安全性的影响，同时也叙述了如何使用角色来保护服务器安全。

● 第 12 章“补丁管理” 每台服务器都需要经常更新。人类所创造出的最复杂的事物——软件并不是完美无瑕的。补丁管理不是一件轻松的工作，但是有了好的工具和方法，就会变得易如反掌了。

● 第 13 章“保障网络安全” 每台电脑的安全都依赖于某个软件或者是某个人。管理这些所依赖的服务当然就成了维护网络安全最重要的事。本章介绍这些服务，并且讲解如何进行关于网络的威胁模型分析，以及当今最流行的安全技术：服务器和域隔离。

● 第 14 章“分支机构的安全” Windows Server 2008 的一个重要特色就是分支机构的安全策略。本章介绍如何利用这些安全策略。

● 第 15 章“中小企业解决方案” Windows Server 2008 比以往微软出品的任何服务器操作系统更加能够满足用户需求，其中两款是特地为中小企业量身打造的。对经营该类企业的用户来说，本章的内容不可不读。

● 第 16 章“应用服务器安全” 大多数服务器的作用是提供应用程序支持，尽管本书不能面面俱到的介绍所有的程序，但是微软在 Windows Server 2008 中集成了 IIS 7.0 平台。本章讲解如何在该组件中进行安全管理。

在线内容

本书提供了一些在线内容，包括新的和升级的内容，笔者把它们放在微软出版社在线 Windows 服务器和客户端站点上。基于 Windows Server 2008 的最终版本，笔者会提供章节内容、文章、相关资源链接、勘误表以及样张等在线内容的更新。在线内容的网址是 http://www.microsoft.com/ learning/books/online/serverclient，并且会不定期更新。

特殊标注

本书用下面的这些标注来强调某些注意事项。

读者帮助

本书中用一些标记来提示有用的细节，见下表。

读者帮助	含义
注意	强调特定内容或是表明某些情况并不是通用的
下载代码	相关的脚本、工具和帮助信息，有助于读者理解书中讲解的操作

旁注

本书中用工具条来介绍一些心得或技巧，涉及不同的 Windows Vista 功能，见下表。

工具条	含义
专家意见	由微软最有价值专家提供，包含 Windows Vista 的工作原理、管理安全的最佳方案以及解决问题的方法
工作原理	简要介绍 Windows 服务器的功能及其工作原理

命令行样式

下表中是一些本书里命令行例子中常用的字体及其含义。

字体	含义
粗体	用户输入（用户输入的文字）
斜体	需要提供指定值的变量（例如用以指代任何合法文件名的 *file_name*）
固定宽度字体	代码或命令行输出
%System%	环境变量

下载代码

代码中含有以下内容：

提升工具

毫无疑问，用户账户控制（UAC）增加了管理系统的复杂性，也毫无疑问，这种变化有些过时，使用计算机时，要绝对执行必须的步骤。然而，作为系统管理员，我们有时需要修改一些只有系统管理员才有权限访问的文件或者需要通过提示符快速打开一个文件夹，这类工具在 Windows Explorer 中添加了右键菜单，如图 1 所示。很简单，右击文件夹，选择

“Elevate Explorer Here”命令，这样，无论在什么位置，都可以运行 Windows Explorer 窗口，并且具有管理员权限。同样也可以使用 elevate.exe 工具，它能在提示符下运行任何的程序。

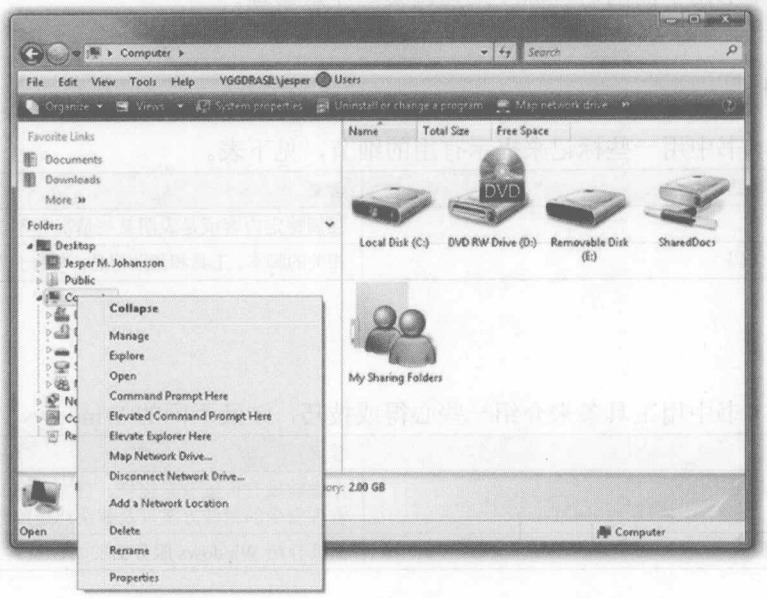


图 1 安装了提升工具，在 Windows Explorer 中就可以使用新的右键菜单

Passgen

Passgen 是一个管理内建管理员账户密码的工具，它还可以远程维护账户。这个工具可以让管理员账户密码难于破解，也能为其他账户设置密码以及相应的权限。

脚本管理

代码中还附带了一系列用于管理 Windows 的脚本，如获取计算机设置信息（包括软件安装信息）的脚本。这些脚本都需要安装 Windows PowerShell。下面列出这些脚本。

CreateLocalUser.ps1：在本地或远程计算机上创建一个本地用户。

EvaluateServices.ps1：统计本地或远程计算机上的服务并输出报告，通知用户自动运行、手动运行和被禁止的服务各有哪些。然后统计所使用的账户，包括本地系统、本地服务、网络服务以及用户创建的账户。最后由用户选择是否显示统计的详细信息。

FindAdmin.ps：列出某台计算机上的本地管理员组。

FindServiceAccounts.ps1：该脚本会创建一个列表，显示本地或远程计算机上的服务及其账户。

ListUserLastLogon.ps1：该脚本会列出在本地或远程计算机上某个用户最近一次登录的日期。可以使用-user 参数来显示多个用户。

LocateDisabledUsers.ps1：定位本地或远程计算机上被禁止的用户。

LocateLockedOutUsers.ps1：定位本地或远程计算机上被锁定的用户。

LocateOldComputersNotLogon.ps1：定位本地或远程计算机域上数天内未登录的账户。

LocateOldUsersNotLogOn.ps1：扫描本地或远程计算机域，查看是否有用户长期未登录。

LookUpUACEvents.ps1：列出本地或远程计算机上的用户账户控制事件。

ScanForSpecificSoftware.ps1：扫描软件的残余文件。

ScanForSpecificUpdate.ps1：扫描本地或远程计算机上的更新。该脚本会创建计算机上已安装的所有更新的列表。

ScanConfig.ps1：该脚本创建一个列表，可以显示已安装的软件更新、ActiveX 对象、浏览器辅助对象、网络端口、代理设置、自动运行、服务、未签名驱动和防火墙策略等。

UnlockLockedOutUsers.ps1：解锁被锁定的用户账户。

WhoIs.ps1：从网络 whois 服务器上检索 whois 信息。

附加章节

“实现活动目录权限管理服务”包含一些未能及时收录在书中的最新动态。在 CD 中同样也收录了一些微软出版社出版的其他书籍里的相关章节。

相关资源

有些章节会涉及一些文件或者小工具，它们都已经收录在下载代码中了。

本书涉及的工具

为了使读者能够下载到最新版本的实用工具，本书提供相关链接，可以用来下载它们。

Windows PowerShell

Windows PowerShell 是一种为系统管理设计的新型交互式的命令和脚本语言。基于 NET Framework，使 IT 管理员和开发者能够全面地自动操作和控制 Windows 和应用程序管理任务。可以在下面的网址下载 Windows Power Shell：

http://www.microsoft.com/downloads/details.aspx?FamilyID=c6ef4735-c7de-46a2-997a-ea58fdfcba63&DisplayLang=en(Windows Vista x64 版)以及 http://www.microsoft.com/downloads/details.aspx?FamilyID=af37d87d-5de6-4af1-80f4-740f625cd084&DisplayLang=en (Windows Vista x64 版)。

Process Explorer

本书中的很多例子讲到 Process Explorer，Process Explorer 是一款强大的任务管理器，能够让使用者了解在后台执行的处理程序。可以从下面的网址下载到 Process Explorer：

http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx。

Microsoft Network Monitor

最新版的 Microsoft Network Monitor 是一种强大的网络管理工具，它能帮用户解决很多问题。该软件可以测量并且显示出网络上的所有流量，是每位管理员的必备工具。可以从下面的网址下载 Network Monitor：

http://www.microsoft.com/downloads/info.aspx?na=22&p=2&SrcDisplayLang=en&SrcCatego-ryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3d18b1d59d-f4d8-4213-8d17-2f6dde7d7aac%26DisplayLang%3den。

Privbar

Privbar 是用于 Windows Explorer 和 Internet Explorer 的工具条，它能够直观地显示当前运行权限(超级管理员、高级管理员、普通用户或者受限用户) 。可惜的是，在本书写成的时候，此版本的 privbar 仅在 Windows Vista 下可用，而在 Windows Server 2008 无法使用。可以从下面的网址下载 privbar：

http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/195350.aspx。

技术支持

为了使书的内容尽量实用，微软出版社在下面的网址提供了勘误内容：http://www.microsoft.com/learning/support/search.asp。

如果有关于本书和下载代码的任何评论、疑问或建议，或有知识库无法解决的问题，可以通过以下方式与微软出版社联系：

电子邮件：

rkinput@microsoft.com

普通信件：

Microsoft Press

Microsoft Windows Server 2008 Security Resource Kit

One Microsoft Way

Redmond, WA 98052-6399

目　录

第 1 部分　Windows 安全基础