Broadview
www.broadview.com.cn

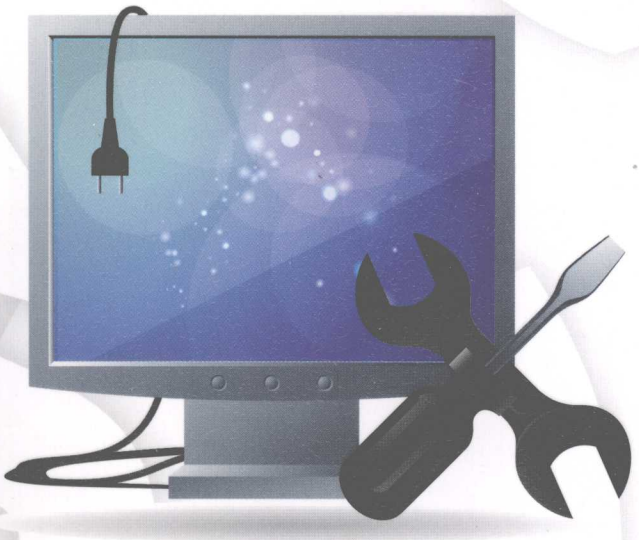
INSPC

INSPC认证培训教程系列

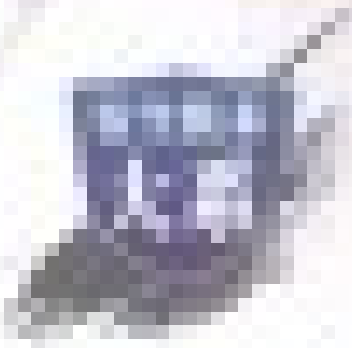
安全技术大系

Windows Server 2003 系统安全管理

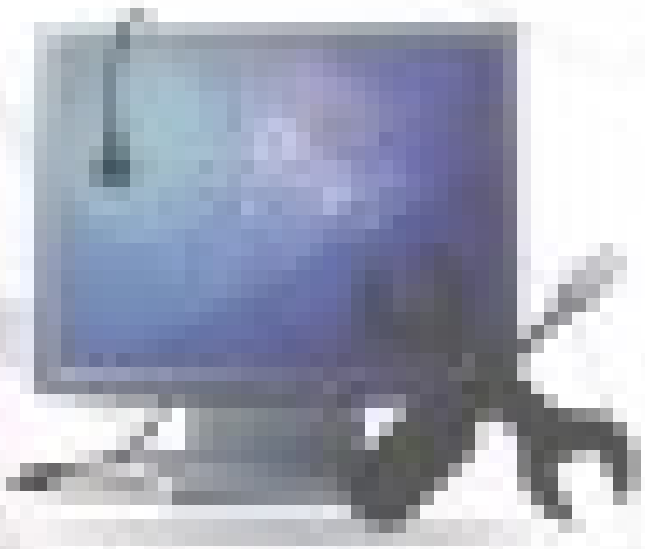
国家反计算机入侵和防病毒研究中心 组编
王淑江 刘晓辉 张奎亭 编著



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



Windows Server



INSPC认证培训教程系列

Windows Server 2003 系统安全管理

国家反计算机入侵和防病毒研究中心 组编
王淑江 刘晓辉 张奎亭 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书以 Windows Server 2003 操作系统为背景，详细地阐述了 Windows Server 2003 系统本身，以及基于该系统应用的安全设置，并给出了相应的完全解决方案，从而最大限度地确保系统能够安全、稳定、高效地运行。本书语言流畅、通俗易懂、深入浅出、可操作性强，注重读者实战能力的培养和技术水平的提高。

本书适合系统管理人员、安全管理人员和网络管理人员，以及对计算机系统维护和网络管理感兴趣的电脑爱好者阅读，并可作为大专院校计算机专业的教材或课后辅导资料。

图书在版编目（CIP）数据

Windows Server 2003 系统安全管理 / 王淑江，刘晓辉，张奎亭编著. —北京：电子工业出版社，2009.3
（安全技术大系.INSPC 认证培训教程系列）
ISBN 978-7-121-08139-2

I. W… II.①王… ②刘… ③张… III. 服务器－操作系统（软件），Windows Server 2003－安全管理
IV. TP316.86

中国版本图书馆 CIP 数据核字（2009）第 008342 号

策划编辑：毕　宁
责任编辑：葛　娜
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
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
开　　本：787×980　1/16　印张：22.25　字数：478 千字
印　　次：2009 年 3 月第 1 次印刷
印　　数：4000 册　定价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

前　言

Windows Server 2003 操作系统是一套成熟的操作系统，拥有较高的使用率。所有系统管理员都已经认识到系统安全是网络管理工作中非常重要的，同时也是最基础的组成部分，无论看似简单的基本操作，如强密码设置、启用 Windows 防火墙、启用安全策略，还是组策略设置，都是安全管理的一部分，系统安全涉及的内容太多，而每个安全漏洞都有可能导致安全问题。

系统安全是网络安全的基础防线，操作系统安装完成后，已经通过默认的安全模板进行了安全设置，但是要使该系统更加安全必须对其进行加固。除了必要的漏洞修复、补丁安装之外，密码管理和 NTFS 权限应用将是保护系统安全的基本措施。因此，系统管理员非常需要一本图书来全面指导其系统安全设置工作。

本书特点

本书从基础入手，全面、深入、系统地介绍如何加固系统，书中涉及的内容均是作者在实际工作中的写照，目的性和针对性都很强，最大限度地介绍了 Windows Server 2003 系统有关安全的因素，归纳和总结了作者多年的安全工作经验和管理技巧，部分以案例的方式提供给读者，希望读者能够举一反三，根据自己的实际工作环境制定详细的安全策略，加固系统安全，全面提升安全水平，迅速成长为合格的系统管理员。

本书中介绍的关于系统安全方面的知识，不仅适用于 Windows Server 2003 操作系统，同时适用于其他 Windows 操作系统，部分章节的内容也适用于 Linux 操作系统。

本书内容

本书内容共分为 11 章，内容安排如下：

章　名	内容介绍
第 1 章 Windows Server 2003 系统安全概述	简要介绍了网络安全威胁，提出了基本的网络安全建议，并概要介绍了 Windows Server 2003 安全系统架构
第 2 章 Windows Server 2003 安装配置安全	从 Windows Server 2003 系统安全安装开始，全面介绍了用户的安全管理，包括如何设置密码，以及基本密码设置原则

续表

章　名	内容介绍
第 3 章 用户账号安全	介绍如何管理系统管理员，以及域系统管理员的权限、用户访问权限的设置
第 4 章 文件访问安全	介绍了文件权限与访问安全，包括如何部署基于 NTFS 的权限管理，如何启用文件审核管理，如何能更安全部署共享文件夹，如何限制用户空间使用，以及在写入数据时对数据的写入限制，如何使用 EFS 保护数据
第 5 章 网络通信安全	介绍了计算机之间的通信安全，如何限制、查看、关闭、屏蔽、启用端口，如何使用 IPSec 策略部署安全的访问策略
第 6 章 应用程序与服务安全	介绍了 Windows Server 2003 系统中的基础服务安全，以及部分应用程序如何安全地使用，读者可以以该部分内容为基础，合理地规划应用程序的使用，着重介绍了 IIS 服务、FTP 服务、Windows 内置服务、Internet Explorer 浏览器，以及 Runas 服务的安全应用
第 7 章 软件限制安全	介绍了软件限制策略在系统中的应用，该部分的内容有很大的拓展空间，通过组策略的部署可以限制病毒、木马及游戏等应用程序在客户端计算机上的运行，间接地提高系统安全
第 8 章 安全配置和分析	介绍了 Windows Server 2003 安全配置向导的使用，以及如何使用预定义的安全模板通过“安全配置分析工具”对系统进行分析，根据匹配的结果部署更加安全的策略
第 9 章 注册表安全	介绍了 Windows Server 2003 的核心数据库注册表的安全配置及安全使用
第 10 章 系统监控审核	介绍了日志、事件、性能日志和警报在系统中的监控机制，做到提前发现问题，将问题解决在萌芽之中
第 11 章 备份与恢复	介绍了备份和恢复在 Windows Server 2003 中的应用，不仅要备份数据同时要备份操作系统、Active Directory 数据库、网络基础信息等，如果关联其他的应用，则根据应用类型制定不同的备份策略等方面的内容

本书涉及系统安全的方方面面，相信一定会得到广大系统管理员的认同和欢迎。

本书由王淑江、张奎亭、刘晓辉编著，上海交通大学信息安全工程学院的王轶骏老师进行了审稿，赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、石长征、郭腾、李海宁、田俊乐、陈志成、王春海等也参与了部分章节的编写工作。作者均长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，出版过多本计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望能对大家的系统管理工作有所帮助。本书能够得以出版，有赖于毕宁先生和张奎亭先生的精心策划，以及许多宝贵的意见和建议，在此深致谢意！

INSPC 认证丛书介绍

随着全球科学技术的迅猛发展和信息技术的广泛应用，信息网络系统的安全性问题已经成为全社会关注的焦点，并且已成为涉及国家政治、军事、经济和文教等诸多领域的重要课题。在国内，随着中国国民经济和社会信息化建设进程全面加快，网络与信息系统的基础性、全局性作用日益增强，迫切要求加强信息安全保障工作。

为贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号），《国务院关于大力发展职业教育的决定》（国发[2005]35号），进一步加强信息网络安全专业人员队伍建设，培养和建设一支政治可靠、技术过硬的信息网络安全专业人员队伍。国家公安部第三研究所、国家反计算机入侵和防病毒研究中心首先发起，联合国内信息安全专业教育和研究服务机构、国际知名信息安全厂商企业、国家重点行业代表性用户单位，按照优势互补、资源共享原则，以联盟合作的形式共同推动中立、专业、实用的**信息网络安全专业人员认证培训体系（Information Network Security Professional Certification，简称 INSPC）**，建设以国家信息化产业政策为指导，适应中国信息安全产业发展的信息安全职业技能认证体系，INSPC 体系的建设以人才市场需求为导向，以培养和锻炼职业技能为核心，将推动 INSPC 认证体系逐渐获得政府职能部门、行业协会、信息安全产业和人才市场的认同，成为信息网络安全从业人员资格认证、技能鉴定、企事业单位聘用信息网络安全专业人才的测评标准，同时为中国的信息安全保障工作建立信息网络安全专业人才库。

INSPC 认证体系分为**公共基础认证**和**安全专业人员认证**。其中安全专业人员认证根据不同的安全领域或产品分为不同的认证模块。

一、公共基础认证（Common Basal Certification，CBC）

- **认证对象**
  - ✓ 高中（含中专）以上学历，使用 PC 进行办公、学习和生活娱乐的个人电脑用户；
  - ✓ 专业人员进阶认证的基础。
- **认证目标**
  - ✓ 普及信息安全基本知识和政策法规，提高信息网络安全防范意识；
  - ✓ 形成个人电脑操作良好规范，提高电脑使用效率；

- ✓ 掌握个人电脑安全防护技能，防止病毒、木马等恶意程序对系统的破坏；
- ✓ 掌握个人电脑网络安全防范技能，防止常见的网络攻击手段对系统的侵害；
- ✓ 掌握系统和用户数据备份技能，保护个人电脑用户数据安全。

二、安全专业人员认证（Security Professional Certification，SPC）

- **认证对象**
  - ✓ 企事业单位中从事技术岗位的专业人员，如网络管理员、系统管理员、数据库管理员等专业人员；
  - ✓ 信息安全企事业单位售前和售后技术支持人员。
- **认证目标**
  - ✓ 掌握信息安全工程和管理所必需的专业理论知识；
  - ✓ 掌握信息系统的安全管理、评估和攻防技术；
  - ✓ 掌握主流网络和信息安全产品的配置管理；
  - ✓ 培养信息安全解决方案设计和工程实施能力。

根据 INSPC 认证培训教学的需要，由公安部第三研究所和电子工业出版社联合组织国内信息安全领域的专家和工程实践人员、通过对用户单位在信息安全知识需求方面进行的针对性调研，组织编写和出版了该套 INSPC 认证丛书，从书包括以下书目：

编　号	名　称	认证类别	计划出版日期
CBC01	信息安全之个人防护	公共基础	2008/4
SPC01	Windows 2003 Server 系统安全管理	系统安全	2009/1
SPC02	UNIX 系统安全管理实践	系统安全	2009/6
SPC03	数据库系统安全	数据安全	2009/10
SPC04	网络安全攻防实战	网络安全	2008/4
SPC05	计算机病毒防御技术	网络安全	2009/6
SPC06	防火墙配置实践	网络安全	2009/12
SPC07	路由与交换设备安全配置实践	网络安全	2009/6
SPC08	密码应用 PKI 技术	密码技术	2009/10
SPC09	安全审计与计算机取证技术	安全管理	2009/8
SPC10	信息安全管理实践	安全管理	2009/10

该丛书的出版，本着“出精品”的原则，成熟一本，出版一本，并建立了完善的教材修订机制，及时更新教材内容。

作为一套用于认证培训的丛书，它具备以下特点。

- **实用性**

本套丛书从信息系统用户的安全知识和技能需求出发，组织相关内容，同时与教程配套，由教学和工程实践经验丰富的专家精心设计了若干针对性实验，理论结合实践，可有效提高用户的专业知识和实践技能，有“立竿见影”之效。

- **趣味性**

本套丛书结合了用户在信息系统使用中遇到的很多实际问题，文档风格生动活泼，有机地结合了知识性和趣味性，让学员或读者共同走进书中内容，与教师或编者分享经验心得。

- **开放性**

为保证教程内容的时效性和针对性，INSPC 认证管理网站（www.inspc.cn）专门开设了教程交流学习论坛，读者和学员用户可把自己遇到的问题和内容建议交流反馈，我们将由专人负责整理和解答，并把其中精彩的内容体现在修订教程中。

INSPC 认证教材编审委员会

2008 年 1 月

目　录

CHAPTER 1

第 1 章　Windows Server 2003 系统安全概述

Windows Server 2003 操作系统是成熟的网络服务器运营平台，但安装和部署一套安全的服务器操作系统难度较高。安全配置是一项具有较高难度的网络技术，如果权限配置得太严格，那么许多应用程序不能正常运行；而如果权限配置得太松，又很容易遭受入侵者的侵入。Windows 操作系统本身平台的安全无疑是构建服务器安全的基础，涉及操作系统和应用程序的安装安全、系统服务安全、系统设置安全和用户账户安全等诸多方面。我们需要对操作系统平台的安全进行关注和细致设置，就能在很大程度上杜绝安全漏洞，确保网络服务和数据访问的安全。

1.1　安全威胁

随着网络应用的深入、网络规模的扩大和数据存储量的增加，以及网络蠕虫、恶意攻击的日益猖獗，网络信息系统对安全的要求也就越来越高。网络攻击事件之所以频频发生，最根本的原因还在于操作系统、网络设备甚至网络协议本身，都存在着严重的安全漏洞。只要稍有疏忽和防范不及，灾难便如影而至。由此不难看出，对于网络信息系统管理员而言，网络信息系统的安全工作最为重要。对许多用户而言，知道面临着一定的威胁，但这种威胁来自哪里、究竟有什么后果，并不十分清楚。一般来说，对于普通用户来说，面临的安全问题主要有以下几个方面。

1.1.1　病毒

这是广大用户最了解的一个安全问题。计算机病毒程序很容易制作，有着巨大的破坏性，其危害已被人们所认识。以前的单机病毒就已经让人们谈毒色变了，通过网络传播的

病毒无论是在传播速度、破坏性和传播范围等方面都是单机病毒所不能比拟的。

继冲击波、震荡波洗劫 Internet 以后，熊猫烧香又以更快捷的传播速度、更多样的传输方式，再次挑战本已脆弱的系统安全。目前全球已发现将近十万余种病毒，并且还在以每天 10 余种的速度增长。有资料显示，病毒威胁所造成的损失占网络经济损失的 76%，仅“爱虫”发作在全球所造成的损失，就达 96 亿美元。一般谈到病毒问题还包括特洛伊木马（Trojan Horse）和蠕虫（Worms）问题。这两种程序不是严格的病毒，但不仅和病毒的危害性相当，而且一般也会伴随着病毒一起向用户发起攻击。特洛伊程序一般是由编程人员编制的，它提供了用户所不希望的功能，这些额外的功能往往把预谋的功能隐藏在公开的功能中，可掩盖其真实企图。蠕虫则是一个或一组程序，它可以从一台机器向另一台机器传播。与病毒不同的是，蠕虫不需要修改宿主程序就能传播。

另外，病毒的生命周期正在无限制地延长。计算机病毒的产生过程可分为：程序设计→传播→潜伏→触发→运行→实行攻击。从近些年主要计算机病毒发作频率和变种速度看，病毒的生命周期延长的趋势十分明显，这主要是由于病毒载体的增多造成的。无线上网技术、蓝牙、手机短信服务、IM 聊天、电子邮件木马捆绑、BLOG 中的跨站攻击代码隐藏、免费音频、视频中的病毒嵌入等都会寄存病毒代码，而变种和交叉感染的存在，都使得病毒从生成开始到完全根除结束的时间大大延长。

1.1.2 非法访问和破坏

黑客攻击已有十几年的历史。黑客技术对于许多人来说已经不再高深莫测，黑客技术逐渐被越来越多的人掌握和发展。目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用，以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，是网络信息安全的主要威胁。

黑客活动几乎覆盖了所有操作系统，包括 UNIX/Linux、Windows NT、VMS 及 MVS 等。黑客攻击比病毒破坏更具有目的性，因而也更具有危害性。Yahoo!、Amazon 等国际著名网站“被黑事件”早已不是新闻。

1.1.3 管理漏洞

网络信息系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。目前，美国 75%~85%的网站都抵挡不住黑客的攻击，约有 75%的企业网上信息失窃，其中 25%的企业损失在 25 万美元以上。此外，管

理的缺陷，还可能出现系统内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄露，从而为一些不法分子制造了可乘之机。

1.1.4　恶意代码

恶意代码已经成为影响安全的新品种。恶意代码不限于病毒，还包括蠕虫、特洛伊木马、逻辑炸弹、间谍软件和其他未经同意的软件。

中国互联网协会对恶意软件的定义是：在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵害用户合法权益的软件，但不包含我国法律法规规定的计算机病毒。

具有下列特征之一的软件可以被认为是恶意软件。

- 强制安装：指未明确提示用户或未经用户许可，在用户计算机或其他终端上安装软件的行为。
- 难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。
- 浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
- 广告弹出：指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
- 恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- 恶意卸载：指未明确提示用户或未经用户许可，或者误导、欺骗用户卸载其他软件的行为。
- 恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。
- 行为记录：行为记录软件是指未经用户许可，窃取并分析用户隐私数据，记录用户电脑使用习惯、网络浏览习惯等个人行为的软件。
- 其他侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。

1.1.5　不满的员工

不满的内部员工（计算机人员、其他工作人员）熟悉服务器、业务系统、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工可能造成更大的损失，例如，可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等。