Broadview
www.broadview.com.cn

网管宝典

刘晓辉 编著

网络安全设计、配置与管理大全

随书含一张演示光盘，涵盖了书中所有重要的操作，读者只需根据光盘中的示例操作，即可实现相应的功能。

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

网管宝典

网络安全设计、配置与管理大全

刘晓辉　编著

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

内 容 简 介

本书主要介绍计算机网络安全的设计、配置与实施，内容由网络操作系统安全、网络设备安全、网络访问安全和数据存储安全四部分组成，基本涵盖了当前主流的网络应用安全的方方面面。操作系统安全部分，主要以 Windows Server 2008 系统平台为例，穿插介绍 Windows Server 2003 系统中的特有安全功能，可以满足不同类型读者的安全需求。网络设备安全部分，主要介绍 Cisco 路由器、交换机、自适应安全设备和无线设备的安全配置和管理。网络访问安全部分主要介绍目前新型的网络访问控制技术，数据存储安全部分主要介绍网络存储技术。

本书主要面向初级网络管理员，尤其是系统安全和网络安全的爱好者。通读全书，即可解决网络管理工作中遇到的各种安全难题，在提高网络安全的同时，丰富自己的知识，迅速成长为专业的网络管理工程师。

图书在版编目（CIP）数据

网络安全设计、配置与管理大全 / 刘晓辉编著.—北京：电子工业出版社，2009.3
（网管宝典）
ISBN 978-7-121-07978-8

I. 网… II. 刘… III. 计算机网络－安全技术 IV. TP393.08

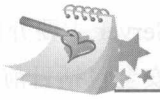
中国版本图书馆 CIP 数据核字（2008）第 196517 号

责任编辑：顾慧芳
印　　刷：北京京科印刷有限公司
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：850×1168　1/16　印张：48.5　字数：1140 千字
印　　次：2009 年 3 月第 1 次印刷
印　　数：3500 册　　定价：89.00 元（含光盘 1 张）

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

中国互联网络信息中心（CNNIC）发布的报告显示，截至 2008 年 6 月底止，我国网民数量达到了 2.53 亿，首次大幅度超过美国，跃居世界第一位。近几年来，互联网技术发展迅速，由于用户水平参差不齐，网络安全事件频发，计算机病毒扩散、网络遭黑客攻击、计算机网络犯罪等违法事件的数量迅速增长，网络安全问题已成为人们普遍关注的问题。

随着计算机网络技术的不断发展，开放性、共享性和互联程度也越来越高，网络应用已经遍布社会的每个部门和行业，电子商务、数字货币、网络银行等业务的兴起以及各种专用网（如校园网）的建设，网络系统的安全与保密问题显得越来越重要。目前，全世界每年由于信息系统的脆弱性而导致的经济损失逐年上升，系统的安全问题日益严重。

网络攻击事件之所以频频发生，其根本的原因还在于操作系统、网络设备甚至网络协议本身存在着严重的安全漏洞。只要稍有疏忽或防范不及时，网络安全灾难便如影而至。但随着网络应用越加普及和深入，网络内存储的重要和敏感数据越多；那么核心业务对网络的依赖性越大，人们对网络安全的要求也就越高。由此不难看出，网络安全已经成为网络管理员在网络构建、网络升级和网络日常管理中的头等大事。

在影响计算机网络安全的诸多因素中，用户无疑是最重要的因素之一。一方面，网络客户缺乏网络安全知识，很少采用系统补丁更新、病毒防火墙和网络防火墙等安全措施，所有的计算机基本上都在 Internet 这个危机四伏的海洋中裸泳，不断地中招、被劫持、做肉鸡、给其网络用户带来麻烦，甚至导致整个网络的瘫痪。另一方面，网络安全工程师人才匮乏，不能充分借助现有设备和技术构建安全防护屏障，打造固若金汤的局域网络，确保网络内部的用户和数据安全。

本书目的

因此，本书旨在帮助网络管理员，迅速成长为系统安全或网络安全工程师，打造出安全的服务器、安全的网络设备和安全的数据存储。同时，借助各种安全策略和手段，拒绝存在各种安全隐患的用户接入网络，从而有效督促普通用户采用安全措施。只有所有用户都安全了，网络安全才能够得到保障。

本书内容

本书由操作系统安全、网络设备安全、网络访问安全和数据存储安全四个部分共 24 章构成，内容涵盖网络安全的各种技术，从不同角度阐述实现网络安全的意义及实现方式，并配合相关实践操作，帮助用户快速掌握所学技能。操作系统安全包括 Windows Server 2008 和 Windows Server 2003 系统平台，以最新推出的 Windows Server 2008 为主，重点突出新功能的介绍和应用，如用户账户安全、Active Directory 安全、系统事件日志等。网络设备安全包括路由器、交换机、新一代防火墙和无线设备的安

全配置和管理等。网络访问安全包括 VPN 远程访问安全和 ISA Server。VPN 部分的内容可以帮助读者掌握当前主流的 VPN 技术，架设所需类型的远程安全传输。ISA Server 主要介绍 ISA Server 2006 的相关应用，包括安全访问代理、防火墙、服务器发布等。网络存储安全包括目前主流的网络存储、磁盘阵列、数据备份与恢复、磁盘配额等。

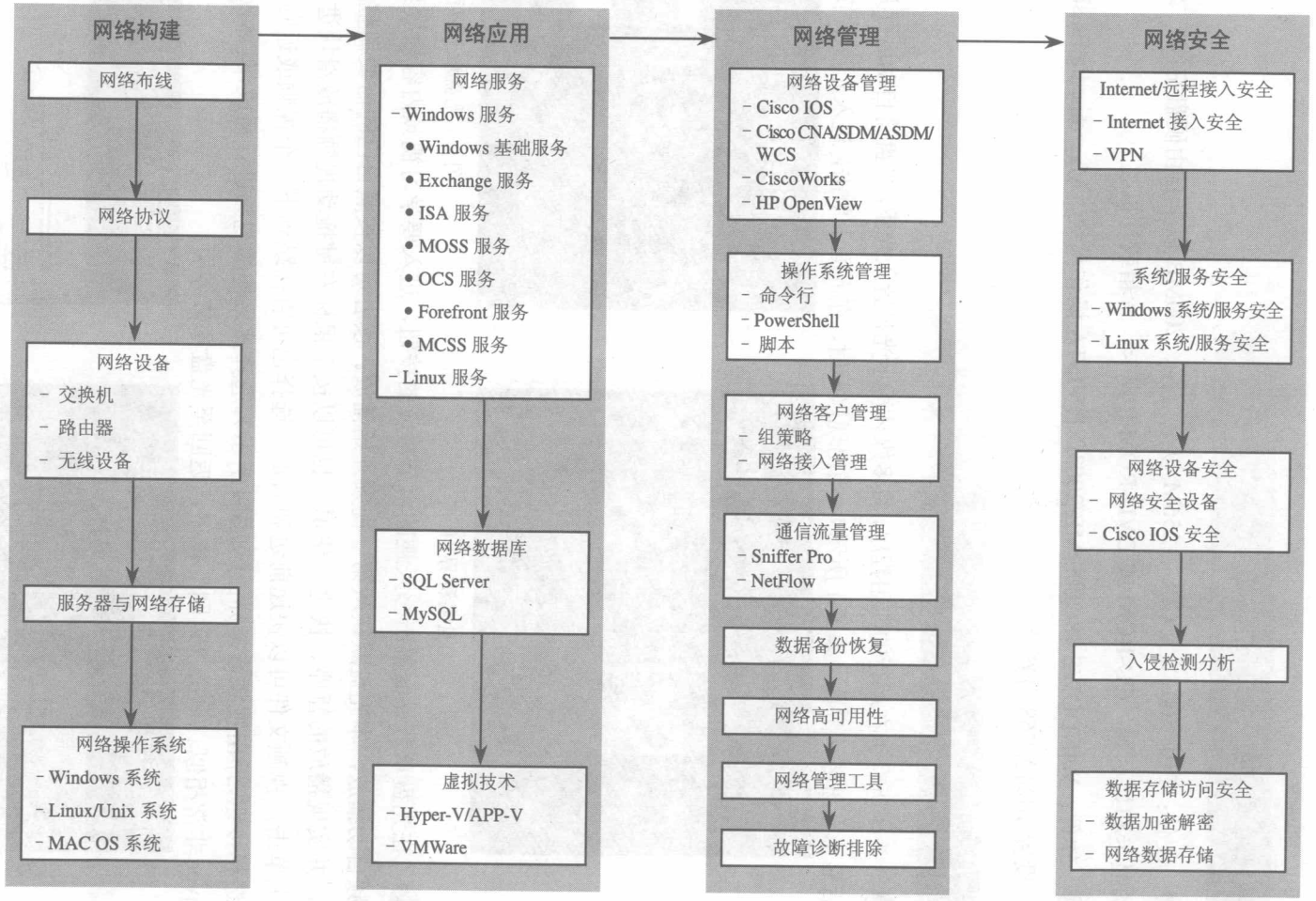
本书由刘晓辉编著，田俊乐、刘淑梅、赵卫东、杨伏龙、李文俊、王同明、石长征、郭腾、白华、李海宁、陈志成、李寅、刘国增、王延杰、刘红、王春海、王淑江等也参与了部分章节的编写工作。笔者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，曾经出版过三十余部计算机类图书，均以易读、易学、实用的特点，受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望对大家的系统维护和网络管理工作能有所帮助。

刘晓辉

2008.10

网管宝典学习路线图

笔者就自己对网络管理体系的理解，对网络管理学习者给出一个粗略线路图：



光盘说明

软硬件需要

硬件：PIII 500 以上 CPU、256M 以上内存、200MB 以上自由硬盘空间、支持 1024 X 768 分辨率的显卡和显示器、CD-ROM 或 DVD-ROM、声卡、音箱或耳机。

软件：WINDOWS 98/2000/ME/2003/XP/VISTA 操作系统，Macromedia Flash Player6.0 以上播放器、设置 1024 X 768 分辨率。

操作指南

关闭所有正在运行的应用程序，将多媒体演示光盘置入光驱，光盘将自动运行并播放宣传片头动画，然后显示光盘名称界面（如图 1 所示），当出现鼠标时，在界面上单击，进入光盘章节界面（如图 2 所示）。

图 1　光盘名称界面

图 2　光盘章节界面

在光盘章节界面单击感兴趣的章节对应的按钮，进入要学习视频内容播放界面（如图 3 所示），视频自动播放，本光盘默认从第一视频开始播放。读者可以按照自己的需要调整解说和背景音乐的音量，并实现播放的暂停、快进、快退，也可以按下鼠标左键拖动视频播放滑块进行快速浏览，在播放条上单击，视频文件可以快速前进和后退。选择也可直接跳到下一个视频或返回上一个视频。点击视频选择按钮，弹出视频选择界面（如图 4 所示），选择感兴趣的视频进行播放，具体操作与 Windows Media Player 非常相似。单击“返回”按钮，返回至光盘章节界面。

图 3　视频内容播放界面

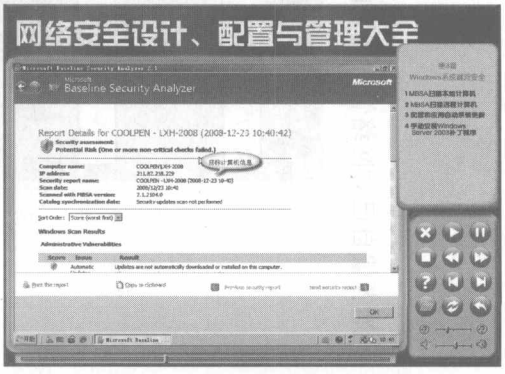


图 4　视频选择界面

在光盘章节界面和播放界面中，单击“光盘帮助”按钮，显示光盘使用帮助文件（如图 5 所示）。点击返回按钮，返回章节界面。

单击“退出光盘”按钮，显示光盘的制作团队信息（如图 6 所示），在退出界面上点击鼠标左键将自动结束光盘播放。

图 5　光盘帮助

图 6　退出界面

目　录

第 1 部分　操作系统安全

第 2 部分 网络设备安全

第 3 部分 网络访问安全

第 4 部分 数据存储安全

第 1 部分　操作系统安全

第1章 网络安全概述

通常情况下，“安全”是指抵抗风险的能力和状态，意味着受到保护，免受那些有意或其他方式产生危害的攻击。网络安全系统是指保障计算机网络通信免受来自各方面的入侵或攻击的整体系统，通常包括系统安全、访问安全、接入安全、存储安全、设备安全等方面。随着网络应用的不断扩展，人们对网络安全的要求也不断提高，甚至许多国家的政府部门都不惜投入大量的人力、物力和财力，来提高计算机网络系统的安全性。

1.1 网络安全基础

计算机网络是地理上分散的多台计算机互联的集合，借助相关的通信协议和网络链路实现资源共享和网络通信。计算机网络安全的脆弱性是伴随计算机网络一同产生的，换言之，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。

➤➤ 1.1.1 网络安全的含义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受任何破坏、更改和泄露，确保系统能连续可靠正常运行，确保网络服务不中断。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。为了保证计算机网络的安全性，通常需要从计算机安全、链路传输安全、网络应用和服务安全等多方面入手。

计算机网络安全之所以如此重要，其主要原因在于：

- 存储和处理重要信息的政府部门的计算机，往往直接关系到国家政治稳定、经济兴衰、军事国防等领域，而这些重要机密信息往往成为不法分子、敌对势力热衷的攻击目标。
- 随着计算机系统功能的不断扩展，系统组成越来越复杂、系统规模越来越大，特别是 Internet 的迅猛发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的漏洞都可能造成巨大的损失。
- 人们对计算机系统的依赖性越来越强，甚至在有些领域这种依赖已经无法替代。
- 计算机应用人员技术水平有限，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误和缺乏经验，都会造成系统的安全功能不足。
- 计算机网络安全问题涉及许多学科领域，如自然科学、社会科学、密码学等。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、检验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄漏技术等。因此，它是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。
- 对网络安全问题重视程度不够，广泛存在着重应用轻安全、质量法律意识淡薄、计算机素养不高的问题。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐藏的、潜在的、难以明确却又是广泛存在的。

➤➤ 1.1.2 网络安全的属性

从本质上来讲，计算机网络安全就是网络上的信息安全。凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全具有以下几个基本属性。