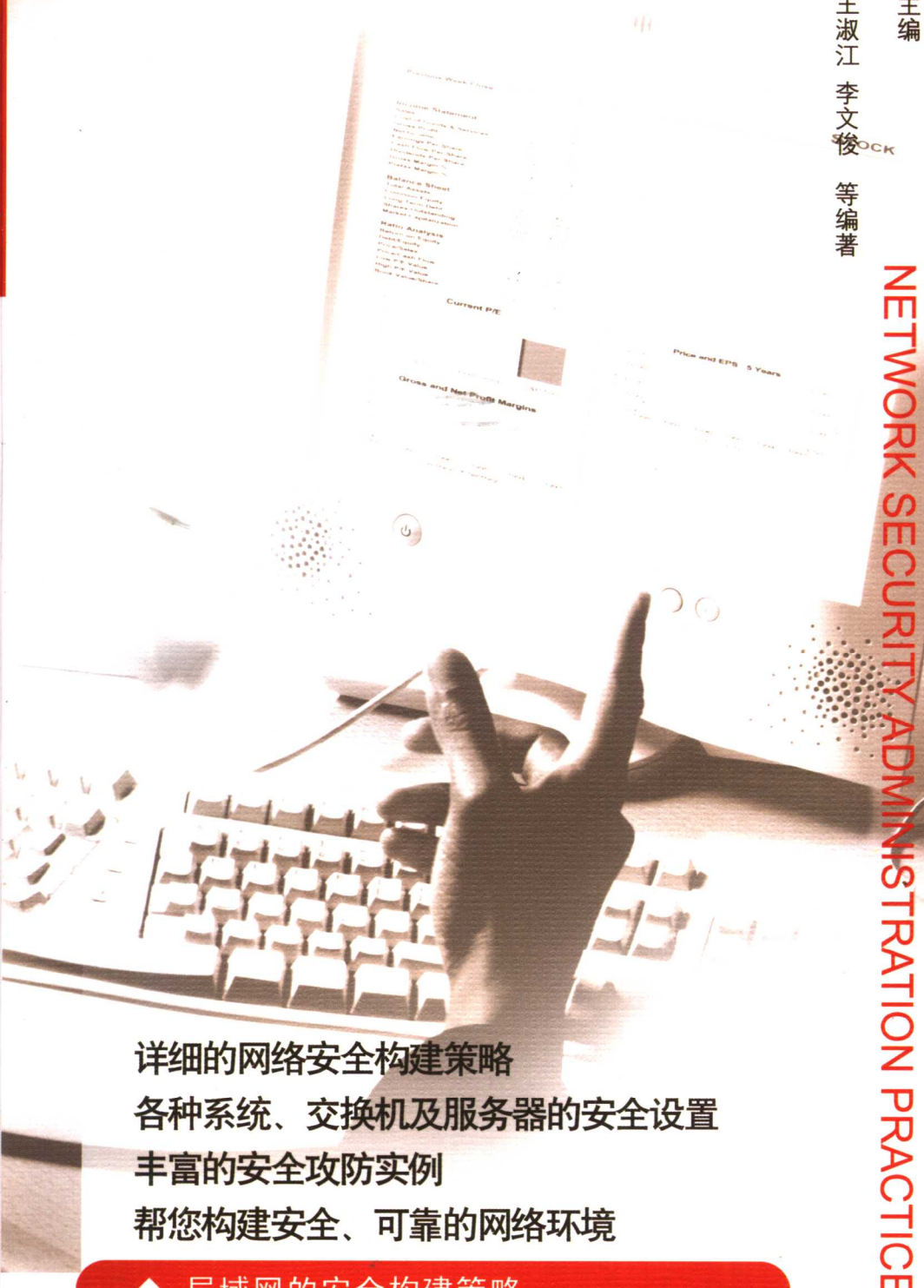
网管天下

网络安全管理实践

NETWORK SECURITY ADMINISTRATION PRACTICE

刘晓辉 主编
杨淑梅 王淑江 李文俊 等编著



详细的网络安全构建策略
各种系统、交换机及服务器的安全设置
丰富的安全攻防实例
帮您构建安全、可靠的网络环境

- 局域网的安全构建策略
- Windows服务器安全
- 网络交换机和路由器安全
- 无线局域网安全
- Windows网络客户端安全

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

网管天下

网络安全管理实践

刘晓辉　主编

杨淑梅　王淑江　李文俊　等编著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书全面深入地介绍了 Windows 网络服务器、Windows 网络客户端、网络交换机、无线网络设备、路由器和网络防火墙的安全设置，以及局域网的安全构建策略，提供了全面的局域网安全解决方案。使读者能够全面掌握局域网络中的安全管理与设置技术，全面提升网络的安全水平，迅速成长为合格的网络管理员和安全规划师。

本书适用于中小型网络管理员和安全规划师，以及所有准备从事网络管理工作的网络爱好者，并可作为大专院校计算机专业的辅导教材。

图书在版编目（CIP）数据

网络安全管理实践 / 刘晓辉主编. —北京：电子工业出版社，2007.3
（网管天下）
ISBN 978-7-121-03774-0

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（2007）第 004076 号

责任编辑：郭鹏飞
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社出版
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：850×1168　1/16　印张：33.5　字数：857 千字
印　　次：2007 年 3 月第 1 次印刷
印　　数：5000 册　　定价：55.00 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，联系电话：（010）68279077；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

关于《网管天下》丛书

《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括网络规划设计、网络布线实施、网络设备连接、网络配置管理、网络服务搭建、网络深入应用、网络故障排除、网络安全管理等诸多方面，囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。

本丛书具有以下特点：

1. 授之以渔而不是授之于鱼。紧贴网络实际情况，从真实的网络案例入手，为网络管理员提供全面的网络设计、网络组建、网络管理和网络维护等解决方案，以提高读者的分析能力、动手能力和解决实际问题的能力。

2. 实用才是硬道理。为网络管理员提供彻底的、具有建设性的网络设计、网络组建和配置解决方案，真正解决网络建设和网络管理中的实际问题，突出实用性、针对性、技术性、经典性，举案说“法”、举一反三。

3. 理论新、技术新、设备新、案例新。所有的应用案例都发生在最近两年以内，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。

关于本书

在 2007 年 1 月举行的达沃斯世界经济论坛上，与会者不但讨论了全球经济和气候变暖的问题，而且还首次触及了互联网安全问题。参与这项话题讨论的既有政治家，也有著名的 IT 界人士。全球网络概念的开发者文森特·瑟弗表示，在目前接入因特网的大约 6 亿台电脑中，有 1.5 亿台左右都已成为黑客们的“俘虏”，并被用来发送垃圾邮件、病毒或是组织网络攻击行动。然而，最令人感到不安的是，上述 1.5 亿台电脑的所有者们经常无法意识到他们的机器正在被别人非法地利用。参与达沃斯世界经济论坛的专家们甚至指出，因特网目前所造成的危险已超过了其所带来的好处。

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网络安全。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时，安全灾难便如影而至。由此不难看出，对于网络管理员而言，网络安全最为重要！

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，网络对安全的要求也就越来越高，因此，网络安全也就随之提上网络管理的重要日程。

本书全面讲述 Windows 服务器、网络客户端、网络交换机、无线网络设备、路由器和网络防火墙的安全设置，以及局域网的安全构建策略，提供了全面的局域网安全解决方案。

使读者能够全面掌握局域网络中的安全管理与设置技术，全面提升网络的安全水平，迅速成长为合格的网络安全管理员。

本书紧紧围绕“网络安全管理实践”这个主题展开，目的性和针对性都很强，最大限度地介绍了网络中所有有关安全的因素，归纳和总结了作者多年的安全工作经验和管理技巧。全面而详细地介绍了中小型网络中服务器、客户端和网络设备的安全策略，涉及从规划设计、搭建配置到管理排障的全部网络硬件技术，是一整套紧贴实际应用的安全解决方案。另外，通过对大量实例深入细致的分析，进一步培养了读者分析问题和解决问题的能力，非常适合网络管理员的实际需求。

本书由刘晓辉主编，杨淑梅、王淑江、李文俊等编著，李海宁、田俊乐、许广博、陈志成、赵卫东、刘淑梅、杨伏龙、王同明等也参加了本书部分内容的编写工作。笔者长期从事网络建设、网络管理、网络教学和网络实验工作，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有关网络搭建和管理的图书，均以易读、易学、实用的特点，得到众多读者的好评。本书是笔者的又一呕心沥血之作，希望能对大家掌握和提升网络安全管理和设置技术有所帮助。

河北三佳电子有限公司的冯士远、张乾、李传来工程师为本书提供了大量的技术资料和大力的技术支持，在此深致谢意！

如果您在配置网络和管理网络时遇到了疑问或难题，或者对本书有什么看法，欢迎发送 E-mail 至 Guopengfei@phei.com.cn 或 hslxh@163.net，进行讨论或寻求支持。由于笔者水平有限，书中难免有疏漏和错误之处，敬请专家和读者不吝赐教。

刘晓辉

2007 年 3 月

目录

网管天下

第1章

网络安全综述

计算机网络安全方案，包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计等。该解决方案的目标是在不影响当前业务的前提下，实现对局域网全面的安全管理。

借助对计算机网络的分析和设计，实现以下网络安全目的：

- 将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非法用户进入网络，减少网络的安全风险。
- 建立统一的漏洞、补丁管理平台。定期进行漏洞扫描、审计跟踪、分发补丁。
- 建立完善的漏洞、补丁评估体系，对于新的漏洞、补丁进行安全评测。
- 建立完善的备份机制，包括：数据库、操作系统、个人应用文件等。
- 通过入侵检测、入侵保护、流量检测等方式实现实时安全监控，提供快速响应故障的手段，同时具备很好的安全取证措施。
- 网络管理员能够很快重新组织被破坏了的文件或应用，使系统重新恢复到破坏前的状态，最大限度地减少损失。
- 在工作站、服务器上安装相应的防病毒、防间谍软件，由中央控制台统一控制和管理，完成带毒设备的阻隔和分离，实现全网统一部署。
- 培养、加强集团职员的安全意识。
- 建立完善的安全保护、预警、检查类的规章制度。

1.1 网络系统安全风险分析

随着 Internet 网络急剧扩大和上网用户迅速增加，网络系统的风险变得更加严重和复杂。原来由单台计算机安全事故引起的损害可能传播到整个系统，导致网络大范围的瘫痪和损失；加上用户缺乏安全控制机制和对 Internet 安全政策的认识不足，这些风险正日益严重。针对企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。下述风险由多种因素引起，与网络结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。

网络安全可以从以下几个方面来理解：

- 网络物理是否安全
- 网络平台是否安全
- 系统是否安全
- 应用是否安全
- 管理是否安全

针对每一类安全风险，结合局域网络的实际情况，下面将具体地分析网络的安全风险。

1.1.1 物理安全风险分析

网络的物理安全主要是指地震、水灾、火灾等环境事故，电源故障，人为操作失误或错误，设备被盗、被毁，电磁干扰，线路截获，以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。

网络的物理安全是整个网络系统安全的前提。hjg 在局域网络内，由于网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险都是可以避免的。