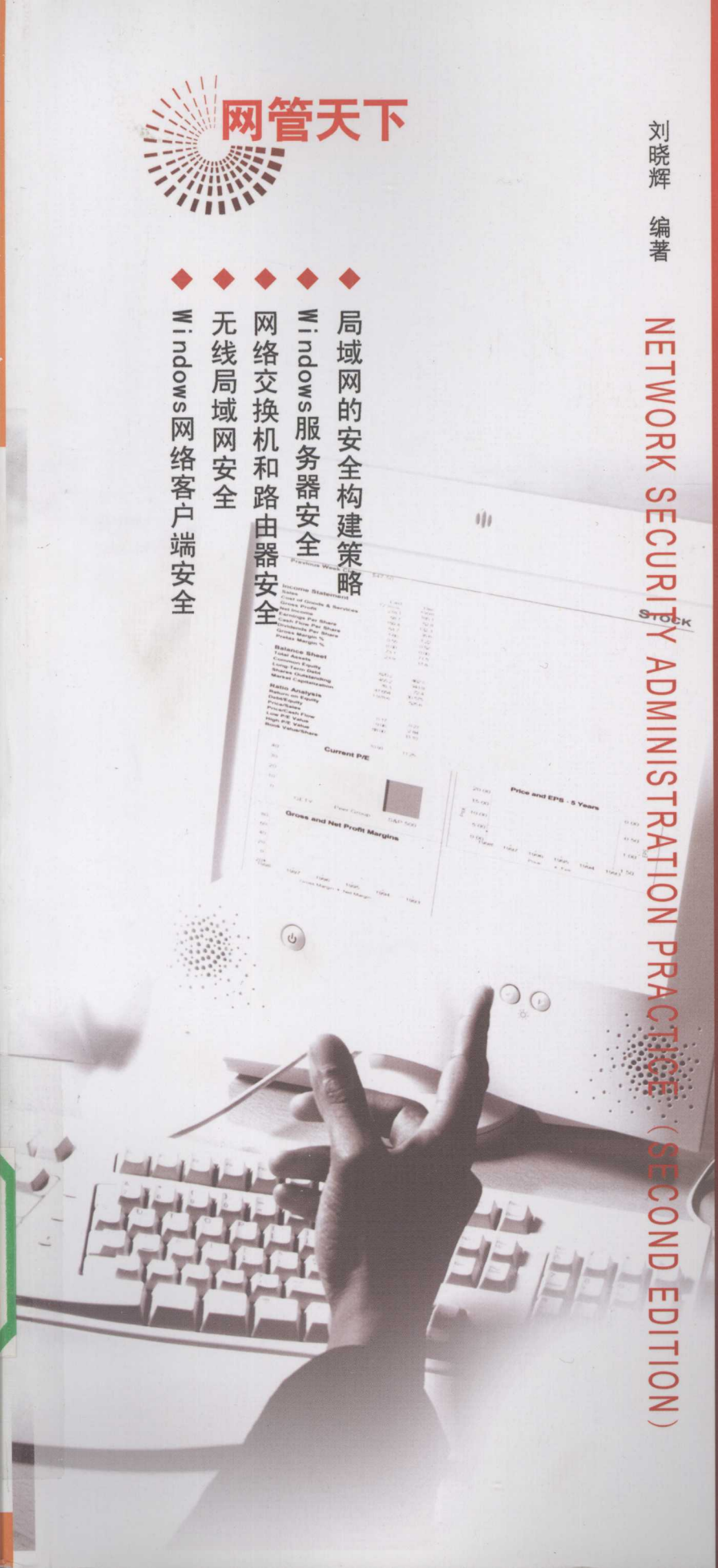
网管天下

网络安全管理实践（第2版）

刘晓辉 编著

NETWORK SECURITY ADMINISTRATION PRACTICE（SECOND EDITION）

- 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

（第2版）

刘晓辉　编著

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

内 容 简 介

本书全面深入地介绍了 Windows 服务器、交换机、路由器、无线网络和网络安全设备的安全设置，系统补丁服务器、网络防病毒服务器和 NAP 网络访问保护的构建，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 / 刘晓辉编著.—2 版.—北京：电子工业出版社，2009.1
(网管天下)
ISBN 978-7-121-07747-0

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（2008）第 177427 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：787×1092　1/16　印张：37　字数：947 千字
印　　次：2009 年 1 月第 1 次印刷
印　　数：5000 册　　定价：59.80 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

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，包括综合布线设计、实施与测试，网络设计与设备选择、连接与配置，网络服务搭建、配置与监控，网络故障诊断、排除与预防，网络安全设计、配置与监视，网管工具选择、使用与技巧，网络设备、服务和客户管理的自动化等诸多方面；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。

《网管天下》第 1 版已经出版近两年的时间，取得了不错的销售业绩，在同类图书中名列前茅，受到了广大读者朋友的喜爱。《网络管理工具实用详解》一书的版权还输出到了中国台湾，得到了中国台湾出版业同行的认可。不过，在这两年时间里，新的网络设备不断推出、新的网络技术不断成熟、新的管理软件不断升级、新的网络应用也不断丰富，原来图书中的有些内容已经不能适应新设备、新技术、新软件和新应用的需求。因此，在保留图书原有写作风格的基础上，对目录结构做了进一步优化，对过时的内容进行了大幅度的更新，隆重推出了《网管天下》第 2 版。

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，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

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。部分专家们甚至指出，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、ARP 攻击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。根据调研机构的调查报告显示，国内企业中 63%经常遭受病毒或蠕虫攻击，而 41%的企业受到恶意间谍软件的威胁。企业经受着网络攻击的“外部威胁”及内部人员信息泄露的“内部威胁”双重考验，企业所面临的网络安全形势日趋严峻。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，日常业务甚至关键业务对网络的依赖程度越来越高，安全问题所导致的网络瘫痪、传输效率下降、服务器拒绝服务，以及数据不能访问、存储数据丢失和非授权访问，都将严重影响的企事业单位的正常运作。而网络蠕虫、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。

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，具有丰富的实践经验，曾经出版过五十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，希望能对大家搭建和管理网络有所帮助。

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

2008 年 12 月

目录

CONTENTS

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，这些风险正日益加重。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。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。

1.1.2 网络平台的安全风险分析

网络结构的安全涉及到网络拓扑结构、网络路由状况及网络的环境等。

1. 公开服务器面临的威胁

局域网络公开服务器区、特殊服务节点作为集团与外界联系的枢纽，一旦不能运行或受到攻击，将影响集团的业务。同时，公开服务器本身要为外界服务，必须开放相应的服务。因此，规模比较大的网络的管理人员，对 Internet 安全事故做出有效反应就变得十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

2. 整个网络结构和路由状况

安全的应用往往是建立在网络系统之上的。网络系统的成熟与否将直接影响安全系统的成功建设。

1.1.3 系统的安全风险分析

所谓系统的安全显而易见是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。

网络操作系统、网络硬件平台的可靠性：对于中国的用户来说，恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 系列，还是其他任何商用 UNIX 操作系统，其开发厂商必然有其 Back-Door。可以这样讲：没有完全安全的操作系统。但是，可以对现有的操作平台进行安全配置、对操作和访问权限进行严格控制，提高系统的安全性。因此，不但要选用尽可能可靠的操作系统和硬件平台，而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

1.1.4 应用的安全风险分析

应用系统的安全与具体的应用有关，它涉及很多方面。应用系统的安全是动态的、不断

变化的。应用的安全性也涉及到信息的安全性，它包括很多方面。

1. 应用系统安全的动态变化

应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的 Bug 是很少有人能够发现的，因此一套详尽的测试软件对管理人员来说是有必要的。但是应用系统是不断发展，且应用类型也是不断增加的，其结果是安全漏洞不断增加且隐藏越来越深。因此，保证应用系统的安全也是一个随网络发展不断完善的过程。

2. 应用的安全性涉及到信息、数据的安全性

信息的安全性涉及到：机密信息泄露、未经授权的访问、破坏信息完整性，以及假冒、破坏系统的可用性等。由于局域网络跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的需要对内部进行保密的信息（比如领导子网、财务系统传递的重要信息等）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

1.1.5 管理的安全风险分析

管理是网络安全中最重要的部分。责权不明、管理混乱、安全管理制度不健全，以及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄漏所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求管理员必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

1.1.6 其他安全风险

1. 黑客攻击

在计算机网络飞速发展的同时，黑客技术也不断提高。目前，黑客能运用的攻击软件已有 1000 多种。黑客自己开发或利用已有的工具寻找计算机系统和网络的缺陷和漏洞，并通过这些缺陷实施攻击，如软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误等。

发现并证实一个计算机系统漏洞可能需要做大量测试、分析大量代码和长时间的编程。大部分黑客是利用已有的软件，这并不需要多么高超的技术。现在的黑客站点在 Internet 上到处可见，黑客工具可任意下载，从而对网络的安全构成了极大的威胁。

2. 通用网关接口漏洞

有一类风险涉及通用网关接口（CGI）脚本，包括许多页面文件和指向其他页面或站点的超链接。搜索引擎是通过CGI脚本执行的方式实现的，黑客可以修改这些CGI脚本，使其执行非法的任务。通常，这些CGI脚本只能在所指WWW服务器中寻找，但如果进行一些修改，就可以在WWW服务器之外进行寻找。要防止这类问题发生，应将这些CGI脚本设置为较低级用户特权，以提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

3. 恶意代码

恶意代码主要利用本地主机上一些特殊的Native API函数和内核系统函数，进行感染、传播和隐藏，从而达到对系统进程、文件、注册表、系统服务和网络服务等进行控制的目的。恶意代码通常包括病毒、蠕虫、特洛伊木马、逻辑炸弹、间谍软件，以及其他未经授权的软件。网络管理人员应该加强对恶意代码的检测。

4. 病毒

计算机病毒一直是计算机安全的主要威胁。随着计算机技术的不断进步，计算机病毒的发展速度也是非常惊人的，每天网络上都会出现成千上万种新的病毒，国际空间每天要处理和查杀的病毒数量更是大得惊人。用户可以使用各种防病毒软件，抵御病毒入侵，一旦遭到入侵应立即查杀或隔离，避免其继续感染其他用户。

5. 不满的内部员工

不满的内部员工（计算机人员、其他工作人员）熟悉服务器、小程序、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的方法，避免这类风险。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的损失更大。例如，可以传出至关重要的信息、泄露重要安全信息、错误地进入数据库、删除数据等。

6. 针对网络的其他手段

一般认为，目前对网络的攻击手段主要表现在以下几方面。

■ 非授权访问

没有预先经过同意，就使用网络或计算机资源为非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息等。非授权访问主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

■ 信息泄漏或丢失

指敏感数据在有意或无意中被泄漏出去或丢失，通常包括：信息在传输中丢失或泄漏（如“黑客”利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息），信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息。