锻造职业能力
拓宽发展空间

- 基于不同操作系统的安全技术与实现
- 针对各种安全威胁给出有效的防范措施
- 介绍多种网络安全配置及安全工具的应用
- 快速提升解决实际问题的综合技能

NETWORK

网管常用

ADMINISTRATOR

网络安全

王 群 编著

- TCP 和 UDP 端口的安全设置和应用
- 防火墙防御攻击的常用技术
- Norton Internet Security 的应用
- 蠕虫\脚本病毒\木马\间谍软件的清除和防治
- IPC$\Telnet\注册表\终端服务入侵方法与防范
- DoS 与 DDoS 攻击与防范
- 强化 Windows 2000 的 TCP/IP 堆栈安全
- 数字证书的应用与管理
- 站点间 Active Directory 数据的安全
- Active Directory 数据库的备份与还原
- Windows 2000\ 2003 的网络安全
- 配置安全可靠的 Linux 系统

人民邮电出版社
POSTS & TELECOM PRESS

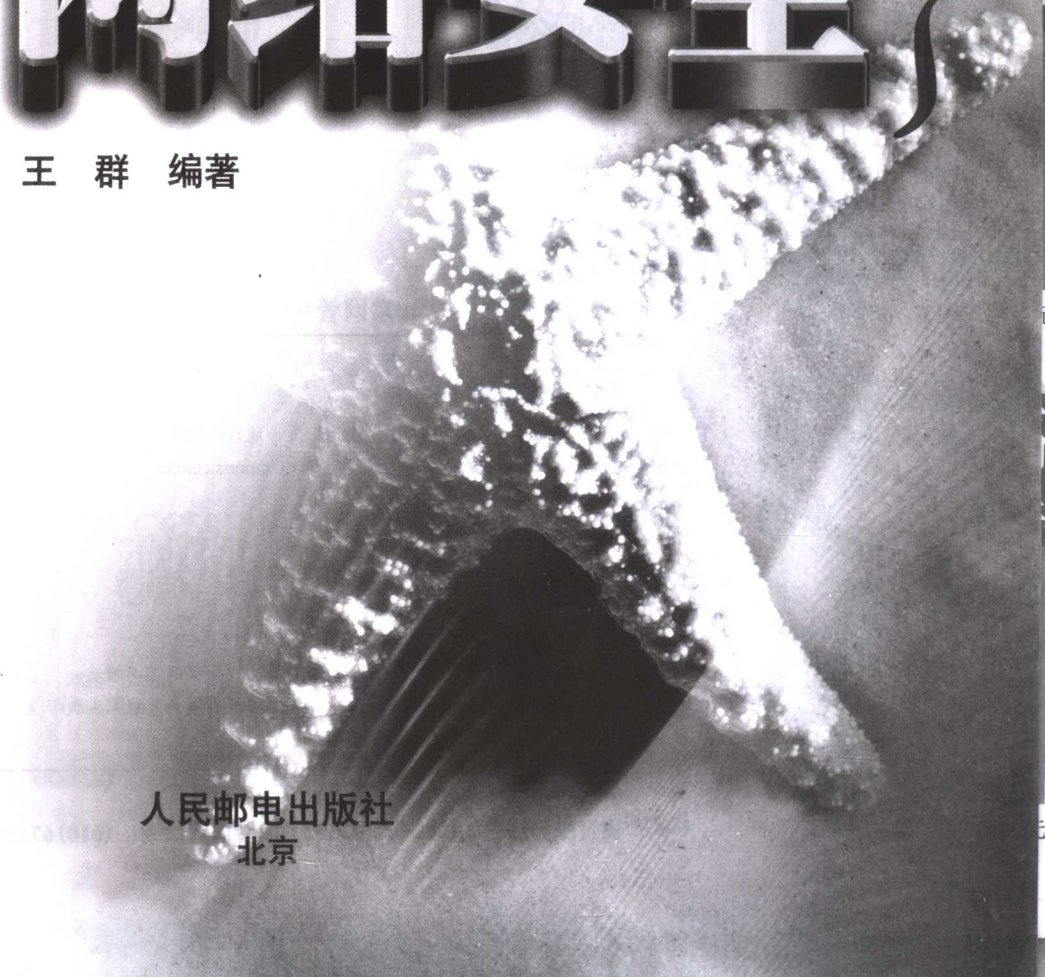
NETWORK

非常网管

ADMINISTRATOR

{网络安全}

王 群 编著



人民邮电出版社
北京

图书在版编目（CIP）数据

非常网管·网络安全/王群编著. —北京：人民邮电出版社，2007.4
ISBN 978-7-115-15815-4

Ⅰ. 非… Ⅱ. 王… Ⅲ. 计算机网络—基本知识 Ⅳ. TP393

中国版本图书馆 CIP 数据核字（2007）第 014716 号

内 容 提 要

本书通过大量实例，使用通俗易懂的语言和简洁明快的叙述方式，以防范实际应用中可能存在的安全隐患为基础，较为系统地介绍了各种安全知识。在此基础上，结合目前广泛使用的 Windows 2000 Server、Windows Server 2003 和 Linux 操作系统，分别介绍了安全技术的应用和实现方法。

本书的主要内容包括网络安全基础知识、TCP 和 UDP 端口的安全设置和应用、防火墙技术及应用、计算机病毒及防治方法、网络入侵与防范、网络攻击与防范、数字证书与网络安全、企业服务器的安全、Windows Server 2003 网络安全、Windows 2000 Server 网络安全和 Linux 网络安全。通过学习本书，读者能够独立地从事企业网络系统的安全配置和管理任务。

本书可供各类网络的建设者、使用者和管理者参考，也可作为高职高专和相关培训机构的教材，以及高等学校计算机网络安全课程的辅助教材，是读者系统学习计算机网络安全知识、技术和实现方法的指导教程。

非常网管——网络安全

◆ 编　　著　王　群
责任编辑　杜　洁

◆ 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
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：880×1230　1/16
印张：31.75
字数：976 千字　　2007 年 4 月第 1 版
印数：1 - 5 000 册　　2007 年 4 月北京第 1 次印刷

ISBN 978-7-115-15815-4/TP

定价：49.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

网络管理员与本丛书

也许你经过一翻努力，终于有了份网络管理员的工作，忐忑不安地坐在计算机旁，激动得手心冒汗，却不知如何去管理、维护、排查网络；面对突如其来的网络问题，投诉电话响个不停，同事们的意见、老板的批评此起彼伏，不知你此刻是否能够静下心来。

可能你学了不少网络技术方面的知识，也可能做了很多故障排除的实验，可当真正面对各种网络应用、管理、服务、故障排除、安全等方面的问题时，却显得那么手足无措，困难总是从意想不到的地方出现。

网络本身就是值得注意的麻烦制造者：多种平台和工具的配置、不同层次的应用需求、数不清的补丁和恶意攻击，以及很多没有意料到的突发事件等。

由于工作的特殊性和专业技能的高要求性，要成为一名优秀的网络管理员，就必须具备较为全面的网络技术知识，并具有丰富的网络管理和维护经验。

0.1 做一名优秀的网络管理员

对于程序员来说，也许只需要掌握几门编程语言就能够胜任软件开发工作；对于网络工程的建设者来说，主要强调的是系统集成中的相关技术；对于系统开发者来说，他们在较长的时间内可能仅专注于某一项技术或应用。而对于网络管理人员来说，由于他们时刻面对的是整个网络系统的情况，所以要求具备与此相关的各个方面的专业知识。作为一名优秀的网络管理员，需要掌握以下知识。

1. 网络基础知识

- 计算机网络的组成、分类和应用知识。
- 局域网的组成和工作方式，尤其要掌握以太网的工作原理和管理方式。
- Windows 2000 Server、Windows Server 2003、Linux 等操作系统的特点和应用。
- Exchange 2000 Server、Exchange Server 2003 系统的特点和应用。
- Microsoft SQL Server 2000 和 Oracle 8i/9i 的应用。
- 局域网中常用传输介质和连接设备的相关技术。
- 网络安全方面的相关知识。

- 对计算机网络中的协议及其功能有较深入的理解，尤其能够将各类网络设备与ISO参考模型中各层的功能对应起来，真正做到理论联系实际。
- 掌握网络的架构知识，能够熟练地处理各种因素引起的网络故障，同时对网络中潜在的故障和安全隐患要有预见性，并能够事先做好各种预防措施。

2．网络的组建、维护和管理知识

- 能够根据用户的需求对网络进行设计，画出网络拓扑图。
- 能够根据网络设计图（网络拓扑图）指导网络的工程施工。
- 较为熟练地安装Windows 2000 Server、Windows Server 2003、Linux等操作系统。
- 熟悉Windows 2000 Server、Windows Server 2003活动目录（Active Directory，AD）、DNS、DHCP、FTP的功能、安装与配置。熟悉在多VLAN情况下的DHCP服务器配置以及相应三层交换机的设置。
- 熟悉Windows 2000 Server、Windows Server 2003下用户账号及组账号的功能、创建及管理方法。
- 能够利用Windows 2000 Server、Windows Server 2003中的域来对整个网络进行管理。
- 熟悉Linux下DHCP、DNS、FTP的安装与配置方法。
- 熟悉Windows 2000 Server、Windows Server 2003、Linux下Web网站的发布与管理。
- 熟悉Apache的安装与配置。
- 能够根据企业的要求部署电子邮件、流媒体、及时信息等服务系统。
- 能够独立完成Microsoft SQL Server或Oracle等主流数据库系统的安装和维护，并可以管理运行在这些数据库平台上的应用系统。
- 熟悉数据的备份和还原操作。
- 能够较为熟练地利用组策略对系统和用户进行管理。通过使用第三方软件和工具，对组策略的应用进行扩充，达到“全自动”管理网络的目的。
- 熟悉网络的远程管理方法。
- 熟悉网络的监视及故障排除方法，熟练使用事件查看器及排除网络故障的一些常用工具，控制和监视网络行为。
- 能够配置虚拟专用网（VPN），并且能够使用各种方式实现共享网络连接，懂得如何配置路由与远程访问，掌握NAT（网络地址转换）的配置与管理，能够完成企业网的Internet接入配置，还要掌握利用Internet通过使用VPN路由的方式为企业组建广域网。
- 熟悉ISA Server 2004标准版和企业的安装、配置、使用和管理。熟悉多VLAN网络下ISA Server 2004的配置，掌握多种服务与ISA Server 2004并存于同一台服务器的配置方法等。
- 熟悉Microsoft SharePoint Portal Server 2003在多种环境下的安装、配置和使用，熟悉WSS与SPS网站的管理与维护。
- 能够综合Windows 2000 Server、Windows Server 2003、Linux、UNIX的优势，使不同的应用系统运行在最适合其要求的操作平台上。
- 熟悉Windows Server 2003企业证书、标准证书的安装、配置、管理与使用，熟悉用证书对邮件、文件进行签名、加密的方法，熟悉用户证书、计算机证书的用处。
- 熟悉SUS、WSUS的使用，掌握在局域网内组建升级服务器的方法。
- 熟悉网络版杀毒软件的使用、掌握把“单机版”杀毒软件“改”成“网络版”的方法，掌握防病毒、防黑客、防攻击的一定知识。
- 熟悉Active Directory的管理、对Active Directory的更名、故障恢复、灾难拯救。
- 熟悉本地用户、本地用户组、Active Directory用户、Active Directory用户组、组织单位、组策略的管理。重点掌握配置文件路径、主文件夹的应用。
- 熟悉Windows服务器的日常管理，掌握使用终端服务、远程桌面、使用MMC管理控制台等多种方式对服务器进行管理。

- 可以组建和管理由不同操作系统组成的异构网络。
- 熟悉集群和集群的组建、应用及管理知识，熟悉网络负载平衡的使用，掌握 Exchange 群集、SQL 群集、ISA Server 阵列等内容。
- 熟悉虚拟机的使用，具有使用虚拟机搭建多种网络与单机环境进行实验的能力。
- 对于 SNMP 协议有较深入的理解，可以利用 SNMP 协议对网络进行管理。
- 可以熟练地配置和管理主流的交换机、路由器和防火墙，熟悉这些设备的冗余配置和应用。

0.2 本丛书特点

为了帮助刚刚涉及这一行业的读者尽快适应工作要求，全面提升自己解决实际问题的综合能力，并为他们在职场中的迅速发展提供有力的支持，我们针对网络管理员的工作内容和需要掌握的专业技能，历经数月，精心策划和组织编写了“非常网管”丛书。

本丛书在内容上力求专业、系统、全面，所有内容的实现，既考虑到内部用户的应用，也考虑到了 Internet 用户的使用；在定位上力求高效实用，重视目前企业网络的实际需求，贴近网络管理员的日常工作；在写作方式上力求简洁明了，清晰易懂，注重理论与实践的结合，并提供大量来自应用第一线的真实案例，使其具有很强的可操作性；在结构布局上，强调不同知识点之间的有机衔接和综合运用，而不是孤立地介绍各个部分的内容，例如，在介绍 Web 服务器的发布时，除介绍 IIS 和 Apache 之外，还介绍了交换机、路由器和 NAT 配置等内容。此外，本丛书还融合了作者丰富的网络项目经验和长达十几年的网络管理积累，为读者带来了全新的学习体验。

0.3 本丛书结构

为了系统全面地介绍网络管理员所需要掌握的知识和技能，本丛书按照网络基础、网络服务、网络管理、网络应用、网络安全及网络典型故障排除等多个主题，对整体内容进行了以下划分，形成不同的主题分册，每个分册重点介绍各自领域中的专业技术、应用解决方案和热点问题。

为了系统全面地介绍网络管理员所需要掌握的知识和技能，本丛书按照网络基础、网络服务、网络管理、网络应用、网络安全及网络典型故障排除等多个主题，对整体内容进行了以下划分，形成不同的主题分册，每个分册重点介绍各自领域中的专业技术、应用解决方案和热点问题。

- **网络基础——不积跬步，无以致千里**

介绍了丰富的计算机网络基础知识，为读者扫清网络知识盲点提供了捷径。

- **网络应用——运筹帷幄之中，决胜千里之外**

重点介绍了 Windows Server 2003 网络应用、ISA Server 2004 标准版与企业版的应用、网络电话、即时消息、视频点播和视频广播、远程办公、基于 SharePoint Portal Server 2003 的门户网站、IDC 数据中心系统的实现。

- **网络服务——工欲善其事，必先利其器**

重点介绍了网络服务操作系统平台、电子邮件系统、Web 站点和 FTP 站点等目前主流网络服务系统的组建和应用。

- **网络管理——不以规矩，不成方圆**

介绍了基于 Windows 2000/2003 的文件、磁盘、组策略、活动目录、DHCP、WSUS、证书服务、防病毒系统，以及网络交换机、路由器、防火墙等设备的管理方法。

- **网络安全——千里之堤，毁于蚁穴**

介绍了网络操作系统、网络设备、常见应用系统的安全使用和管理方法，为加强网络安全提供了技术保障。

- **网络工程案例——他山之石，可以攻玉**

以企业网络用户的实际需求为依据，全程再现了网络系统规划、设备选型与配置、应用系统部署与维护等过程的典型实例。

- **网络典型实验——为者常成，行者常至**

本书根据网管员必须掌握的知识和技能，精心设计了 20 多个实验，从实验内容的介绍、实验的注意事项、实验过程及实验总结，都一一进行了说明，而且附书光盘提供了本书所有实验的视频演示文件，播放时间长达 50 多个小时。

- **DOS 命令技术详解——运用之妙，存乎一心**

合格的网管员需要熟悉并精通 DOS 命令。本书从 DOS 入门开始，介绍了“纯”DOS 命令、Windows 窗口中的 DOS 命令以及基于 DOS 的工具软件的使用技巧等内容。

- **Windows 脚本应用详解——删繁就简，事半功倍**

在网络管理过程中，有许多繁琐的重复性工作，这些工作实际上都可以通过编写的 Windows 脚本自动完成。本书介绍了 Windows 网络管理全过程中需要用到的脚本，包括了脚本的源代码、脚本的使用注意事项等，附书光盘提供了本书中所有脚本的源代码。

- **网络典型故障排除——对症下药，量体裁衣**

经过大量的归纳筛选，精选出了一些典型的网络故障现象和排除方法，是网络管理员日常工作中的必备工具和速查手册。

0.4 本丛书读者对象

本丛书主要为以下几类读者服务。

- 网络的管理人员。本丛书在内容上以目前许多企业的应用需求为主，致力于解决网络管理人员普遍关注的技术和热点问题，并提供专业的网络解决方案。
- 网络应用系统的建设者。不管是网络公司的系统工程师，还是各单位的技术人员，都需要全面了解和掌握网络服务平台的建设和使用方法，而本丛书以实例的形式对大家展现了每一个系统的建设和使用过程。
- 高校和各类培训机构的学生。本丛书所涉及的几部分内容，一方面紧紧围绕用户的实际需求，另一方面符合高校和各类培训机构实践课程的要求。为此，本丛书的部分内容可作为高校计算机网络实践课程的操作指导书，也可支持作为各类培训机构的教学用书。
- 网络初学者。本丛书完全放弃了理论说教式的介绍方法，而是结合实际，以通俗易懂的表达形式，引导初学者逐渐深入掌握各种网络应用技术和工具，从而实现快速入门和进阶。

前　言

Preface

关于本书

作为现代信息基础的网络技术，其发展和应用得到了全社会的普遍关注。我们根据目前用户的实际需要，紧紧围绕网络建设、应用和管理这一主线，精心组织和策划了“非常网管”这套丛书。《网络安全》就是其中的一本。

本书结合目前计算机网络所面对的各种安全威胁，首先介绍了与安全有关的一些基础知识；接着以实例方式介绍了一些主流的安全威胁及防范方法；随后针对中小型网络的应用实际，重点介绍了数字认证和域服务器的安全管理技术；最后针对Windows 2000 Server、Windows Server 2003 和 Linux 等操作平台，分别介绍了相关的安全技术和实现方法。

- 在内容选择上，本书从网络安全基础知识，到目前计算机网络所面对的各类安全威胁及防范，再到一些典型的安全技术介绍与实现，最后针对不同的操作平台来介绍有关的安全技术、策略和实现方法，系统全面地介绍了网络安全中的一些主要元素。
- 要进行安全管理和安全防范，首先要意识到可能存在的安全威胁。为此，在本书开头部分重点介绍了现代计算机网络所面对的各类不安全因素以及所产生的危害。网络管理人员，不管自己的网络采取了多么强的安全防范措施，都要“居安思危”，“道高一尺，魔高一丈”这句俗语在当今的计算机网络中几乎体现得淋漓尽致。
- “知己知彼，百战不殆”，要进行可靠的防范就必须掌握各类不安全因素的产生原因和可能的危害情况。为此本书结合应用实际，重点介绍了防火墙、计算机病毒、网络入侵和网络攻击的原理和应用。
- 安全管理的目的，一方面是保护现有网络的正常运行，另一方面是保护信息在公共网络中传输时的安全性。为此，本书重点介绍了目前应用最为广泛的数字认证的原理、实现和应用，同时结合企业域服务器的管理，介绍了数据的安全备份、还原等方法。
- 加强服务平台的安全管理是保障整个网络系统可靠运行的关键。本书结合目前中小型网络用户的实际，分别以 Windows 2000 Server、Windows Server 2003 和 Linux 操作平台为基础，在介绍了系统自身安全管理的同时，针对不同系统的特点，介绍了大量的基于不同平台的安全技术和实现方法。

● 与本丛书中的其他分册互相呼应，有效地帮助读者提升解决实际问题的综合能力，而不是片面地强调局部的内容。安全问题可能源于整个网络的任何一点，所以要彻底解决网络安全问题必然要综合考虑网络系统的方方面面。为此，本书紧紧与《网络基础》、《网络服务》、《网络应用》、《网络工程案例》和《网络管理》等分册相结合，从安全角度增加了读者对网络的认识。例如，在《网络管理》一书中，我们以 Symantec 企业防病毒软件为例，介绍了企业防病毒系统的部署和应用，使读者在掌握了这一软件的功能和使用方法的同时，意识到了网络安全的重要性。而在《网络安全》一书中，将重点放在病毒的产生、分类、危害、防治和清除等技术细节的介绍上，针对性较强，适用面较广。

本书结构

本书包括 4 篇，共 11 章。

第 1 篇 网络安全基础，包括第 1 章～第 2 章，主要介绍了网络安全基础知识，包括常见的网络安全技术、数据加密技术、认证授权技术、防病毒技术、网络黑客、间谍软件、TCP 和 UDP 端口安全、Windows 操作系统端口的查看和安全配置、网上邻居与 IP 端口、路由器和防火墙上 IP 端口的安全配置。

第 2 篇 安全威胁与防范，包括第 3 章～第 6 章，主要内容包括企业和个人防火墙技术及应用，蠕虫、脚本病毒、木马、间谍软件的危害、破坏原理、防范和清除，网络入侵技术、方法和过程，网络攻击、入侵检测、入侵防御等技术的实现原理和防范。

第 3 篇 安全技术的应用，包括第 7 章～第 8 章，其中第 7 章介绍了数字证书在网络安全中的应用，主要包括数字证书的概念、PKI 与数字证书、企业 CA 和独立 CA 的安装和应用、CA 的管理等；第 8 章介绍了企业服务器的安全，主要包括目录服务的功能、站点的应用和安全、Active Directory 数据库的安全管理、Active Directory 与防火墙等。

第 4 篇 基于操作平台的安全技术和实现，包括第 9 章～第 11 章，主要结合 Windows 2000 Server、Windows Server 2003 和 Linux 操作系统，在分别介绍了操作系统自身的安全管理后，再针对不同的操作平台和应用，介绍了各类安全技术和应用。例如，在 Windows Server 2003 中，分别介绍了用户的安全、VPN 技术和实现、IPSec 技术和应用等内容；在 Windows 2000 Server 中，主要介绍了安全策略及相关安全软件的应用；在 Linux 中，针对网络体系结构介绍了相关的各种安全设置，同时使用较大篇幅介绍了 Linux 下的一些重要的安全管理工具以及 Linux 系统的安全配置方法。

本书约定

为了更好地向读者讲解本书内容，提出以下约定。

（1）地址选择

由于目前使用的 IPv4 版本的 IP 地址资源已经非常少，所以在组建单位网络时，内部用户一般都使用私有 IP 地址，如表 1 所示。

表 1　　内部私有 IP 地址

类　别	网　络　号	地 址 范 围	适 用 范 围
A 类	10.0.0.0/8	10.0.0.0～10.255.255.255	大型企业
B 类	172.16.0.0/12	172.16.0.0～172.31.255.255	中型企业和学校
C 类	192.168.0.0/16	192.168.0.0～192.168.255.255	小型企事业单位

本书实例将选择 B 类网络的 172.16.0.0/16 网段，部分应用使用了 C 类网络的 192.168.0.0/24 网段。

如果在实际操作中，IP 地址不在表 1 所列的范围内，则该 IP 地址为外网的 IP 地址。

（2）操作系统的选择

针对目前的网络应用特点，在网络操作系统的选择上，主要以 Windows 2000 Server、Windows Server 2003 和 Linux 为主。个人操作系统一般使用 Windows XP Professional，必要时使用 Windows 2000 Professional。因为一些安全测试是在操作系统尚不安全（还没有安全补丁程序或未去除 IPC%共享）的情况下进行的，所以读者在操作时一定要考虑当前所使用的操作系统的具体情况。

（3）所涉及的安全威胁

本书所涉及的安全威胁主要有计算机病毒、网络入侵和网络攻击，其中在计算机病毒部分除介绍了传统概念上的计算机病毒外，主要针对当前实现介绍脚本病毒、蠕虫、木马、间谍软件等新型的网络威胁，在网络入侵部分主要针对 Windows 2000 Server 和 Windows Server 2003 介绍了相关的入侵技术和实现过程，在网络攻击方面除介绍了大家较为熟悉的 DoS、DDoS 外，还介绍了目前正在兴起的 IPS 的特点和应用。

（4）所涉及的安全技术

本书所涉及的安全技术较多，除常见的一些技术（如防病毒、防攻击等）之外，还结合不同的操作平台和应用，介绍了数字证书、PKI、VPN、IPSec、RADIUS 等目前热门的技术和应用。

关于我们

感谢李馥娟、陶慎亮、郭亚峰、孙晓赟、聂明辉、刘浩、李旭、许璇、宋玲华、张卫东、何稼男、张世伟、刘庆航、黄步根、张亮等朋友为本书的实验、文字录入和校对等做了大量的工作。另外，在本书的编写过程中，得到了国内一些安全厂家的技术支持，在此一并表示感谢。

网络技术的发展十分快速，新技术、新应用将不断涌现。为此，我们也将密切关注技术的发展和读者的需要，将更新、更实用的技术介绍给读者，将更好的产品和应用推荐给大家。

由于编者水平有限，并且本书所涉及的是一项大家都关注的热点问题，同一技术在不同的环境中可能会存在不同现象和处理方式，虽然我们力求本书的完美，但是考虑到技术和用户实际需求等因素，本书的某些内容可能还不够准确、完善，甚至还会存在一些不妥之处，敬请读者多提宝贵意见。

对本书有任何问题，欢迎大家联系本书作者（book@jspi.cn）或本书编辑（dujie@ptpress.com.cn），希望我们共同进步。

编者

2007 年 2 月

目　录

Contents

第一篇　网络理论基础

第三篇 安全技术的应用