

## <<计算机网络安全>>

### 图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787302225508

10位ISBN编号：7302225508

出版时间：2010-6

出版时间：清华大学出版社

作者：王文斌，王黎玲 等编著

页数：464

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<计算机网络安全>>

### 前言

随着信息化进程的推进，几乎所有的企事业单位都有自己的网络，而由此产生的网络管理人才的需求缺口正在逐年扩大。

据相关部门统计，2009年网络管理人才缺口达到13.5万人，许多企业不惜重金，招募一名出色的网络管理人员。

随着网络应用的不断拓展，企业发展对计算机网络的依赖性将越来越强，而掌握大量精尖网络技术的人才也会变得越来越受欢迎。

为什么在如此光明的就业形势下，却经常听到网络管理员的工资只有几百元呢？

原因很简单，企业真正需要的网络管理员是能够独当一面的专业人员。

向网络工程师晋升，是摆在网络管理员面前的唯一出路。

本套丛书作为网络工程师培训教材，以实际的公司网络为案例，以打造实用的网络工程为目标，以实用和技能为主，摒弃了复杂的原理，以简明的操作为引导，通俗易懂，上手容易。

读者只需按照书中的操作来学习，就能掌握相应的技能，学完全套书之后，即可掌握大部分的网络知识。

计算机网络技术的应用虽然加速了企业发展的步伐，但随之而来的安全问题，也时刻威胁着企业的根本利益。

近年来，企业网站遭到篡改，病毒泛滥成灾，商业机密失窃，企业网络瘫痪，各种高科技信息犯罪活动正在严重危害着社会的发展和企业的生存。

本书以中小型企业的计算机网络安全为例，全面、系统地介绍了企业网络的安全建设，旨在帮助企业打造安全、可靠、高效、便捷的计算机网络。

## <<计算机网络安全>>

### 内容概要

本书主要以现有企业网络为模型，分别介绍服务器系统安全、网络应用服务安全、网络设备安全、网络安全设备管理、局域网接入安全、Internet接入安全和远程访问安全等内容，全面涵盖了当前主要网络中可能遇到的信息安全问题，并详细介绍了不同的网络安全方案。

本书紧密依托选定项目，对企业网络安全中常用的技术进行了深入浅出的讲解，可以帮助读者快速掌握最基本的计算机网络安全技术，打造安全、可靠的企业网络环境。

本书既可作为培养21世纪计算机网络安全工程师的学习教材，同时也是从事计算机网络安全的规划、设计、管理和应用集成的专业技术人员的必备工具书。

## &lt;&lt;计算机网络安全&gt;&gt;

## 书籍目录

第1章 网络安全规划	1.1 项目背景	1.2 项目分析	1.2.1 安全设备分布	1.2.2 网络设备安全现状	1.2.3 服务器部署现状	1.2.4 客户端计算机	1.2.5 无线局域网安全现状	1.3 项目需求	1.3.1 网络安全需求	1.3.2 网络访问安全需求	1.4 项目规划	1.4.1 服务器安全规划	1.4.2 客户端安全规划	1.4.3 网络设备安全规划	1.4.4 无线设备安全规划	1.4.5 安全设备规划	1.4.6 局域网接入安全规划	1.4.7 Internet接入安全规划	1.4.8 远程接入安全规划	1.4.9 网络可靠性规划						
第2章 Windows系统安全	2.1 Windows系统安全规划	2.1.1 案例情景	2.1.2 项目需求	2.1.3 解决方案	2.2 安全配置向导	2.2.1 配置安全服务	2.2.2 应用安全配置策略	2.2.3 知识链接：安全配置向导	2.3 配置Windows系统安全	2.3.1 Windows Update	2.3.2 管理系统管理员账户	2.3.3 用户密码安全设置	2.3.4 配置Internet连接防火墙	2.3.5 配置默认共享	2.3.6 系统服务安全	2.3.7 用户账户控制	2.3.8 知识链接：配置系统安全	2.4 系统漏洞扫描	2.4.1 使用MBSA扫描本地系统漏洞	2.4.2 扫描单台远程计算机	2.4.3 知识链接：MBSA	2.5 端口安全	2.5.1 查看端口开放情况	2.5.2 查看开放端口的宿主	2.5.3 知识链接：端口划分与netstat命令	习题 实验：扫描本地系统漏洞
第3章 网络服务安全	3.1 网络服务安全规划	3.1.1 案例情景	3.1.2 项目需求	3.1.3 解决方案	3.2 活动目录安全	3.2.1 只读域控制器	3.2.2 重启ADDS	3.2.3 SYSVOL安全	3.2.4 管理员授权	3.2.5 用户账户管理	3.2.6 用户组管理	3.2.7 知识链接：活动目录安全	3.3 文件服务安全	3.3.1 NTFS权限安全配置	3.3.2 磁盘配额	3.3.3 文件屏蔽	3.3.4 知识链接：文件服务安全	3.4 IIS服务安全	3.4.1 IP地址访问限制	3.4.2 安全HTTP	3.4.3 知识链接：身份验证	习题 实验：委派管理权限				
第4章 文件权限管理	4.1 文件权限安全规划	4.1.1 案例情景	4.1.2 项目需求	4.1.3 解决方案	4.2 权限管理服务	4.2.1 安装AD RMS服务器	4.2.2 配置信任策略	4.2.3 配置权限策略模板	4.2.4 AD RMS客户端部署及应用	4.2.5 受限客户端应用被保护文档	4.2.6 知识链接：AD RMS	4.3 信息权限管理	4.3.1 创建被保护的安全文档	4.3.2 打开被保护文档	4.3.3 请求权限	4.3.4 知识链接：IRM	习题 实验：使用IRM保护机密文档									
第5章 网络病毒防御																										
第6章 系统补丁更新																										
第7章 Cisco IOS安全																										
第8章 局域网接入安全认证																										
第9章 Internet接入安全																										
第10章 远程接入安全																										
第11章 网络访问保护																										
第12章 安全设备规划与配置																										
第13章 配置网络可靠性																										
参考文献																										

## 章节摘录

插图：IDS（Intrusion Detection System，入侵检测系统）本身是一个典型的探测设备，类似于网络嗅探器，无须转发任何流量，而只需要在网络上被动地、无声息地收集相应的报文即可。

IDS无法跨越物理网段收集信息，只能收集所在交换机的某个端口上的所有数据信息。

该网络中的IDS部署在安全需求最高的服务器区，用于实时侦测服务器区交换机转发的所有信息。

对收集来的报文，IDS将提取相应的流量统计特征值，并利用内置的入侵知识库，与这些流量特征进行智能分析比较匹配。

根据默认的阈值，匹配耦合度较高的报文流量将被认为是进攻，IDS将根据相应的配置进行报警或进行有限度的反击。

4. Cisco Security MARS Cisco Security MARS（Monitoring Analysis and Response System）是基于设备的全方位解决方案，是网络安全管理的关键组成部分。

MARS可以自动识别、管理并抵御安全威胁，它能与现有网络和安全部署协作，自动识别并隔离网络威胁，同时提供准确的清除建议。

在本例企业网络中，MARS直接连接在核心交换机上，用于收集经过核心交换机的所有数据信息，自动生成状态日志，供管理员调阅。

1.2.2 网络设备安全现状当前网络中的交换机、路由器等网络设备全部都是可网管的智能设备，并且提供Web管理方式，同时配置了基本的安全防御措施，如登录密码、用户账户权限等。

## <<计算机网络安全>>

### 编辑推荐

《计算机网络安全》：案例贯穿从最典型的网络工程入手，提供全面的解决方案。

项目驱动情境导入，项目教学，实训强化，培养技能。

内容全面涵盖网管必须掌握的理论和技术，管用、够用、实用：贴近实战知识与技术围绕网络构建过程展开，学得会、用得上。

兴趣教学情景分析与动手操作有机结合，激发学习兴趣和主动性。

注重动手练中求学，学中求练，练学结合，边练边学。

涵盖认证内容安排与IT认证紧密结合，覆盖网管认证主要知识点。

深度支持QQ答疑，E-mail交流，BBS互动，方案咨询，故障诊断。

<<计算机网络安全>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>