

<<网络安全管理及实用技术>>

图书基本信息

书名：<<网络安全管理及实用技术>>

13位ISBN编号：9787111310655

10位ISBN编号：7111310659

出版时间：2010-10

出版时间：贾铁军 机械工业出版社 (2010-10出版)

作者：贾铁军 编

页数：348

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>

<<网络安全管理及实用技术>>

前言

在现代信息社会，随着信息化建设和IT技术的快速发展，计算机网络技术的应用更加广泛、深入，网络安全问题不断出现，致使网络安全管理的重要性更加突出。

网络安全已经成为各国关注的焦点，它不仅关系到用户的信息和资产风险，而且也关系到国家和社会稳定，已成为热门研究和人才需求的新领域。

只有在法律、管理、技术、道德各方面采取切实可行的有效措施，才能确保网络建设与应用又好又快地稳定发展。

网络安全已经成为21世纪世界十大热门课题之一，并成为社会关注的焦点。

网络安全是一个系统工程，计算机网络安全管理已经成为网络管理的重要任务。

网络安全管理涉及法规、政策、策略、规范、标准、机制、措施和管理技术等方面，是网络安全的重要保障。

网络安全管理（Network Security Management）通常是指以网络管理对象的安全为目标所进行的各种管理活动，是与安全有关的网络管理，简称安全管理。

由于网络安全对网络信息系统的性能、管理及影响更复杂、更密切，致使网络安全管理逐渐成为网络管理技术中的一个重要分支，正受到业界及用户的广泛关注。

网络安全管理是一种综合交叉学科，需要综合信息安全、网络管理、分布式计算、人工智能等多个领域知识和研究成果。

其概念、理论和技术正在不断发展完善之中。

网络安全在企业管理机制下，借助技术手段得以实现。

网络安全运作是指在日常工作中具体执行的网络安全管理和技术手段，是网络安全工作的关键，“七分管理，三分技术，运作贯穿始终”，管理是关键，技术是保障，可见网络安全管理的重要性。

信息、物资、能源已经成为人类社会赖以生存和发展的三大支柱及重要保障，信息技术的快速发展为人类社会带来了深刻的变革。

随着计算机网络技术的快速发展，我国在网络化建设方面取得了令人瞩目的成就，电子银行、电子商务和电子政务等的广泛应用，使计算机网络已经深入到国家的政治、经济、文化和国防建设等多个领域，遍布现代信息化社会的工作和生活的每个层面，“数字化经济”和全球电子交易一体化正在形成。

计算机网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及国家政治、军事和经济各个方面，而且影响到国家的安全和主权。

随着计算机网络的广泛应用，网络安全的重要性尤为突出。

因此，网络技术中最关键也最容易被忽视的安全问题，正在危及网络的发展和应用，网络安全及管理已经成为世界关注的焦点。

<<网络安全管理及实用技术>>

内容概要

本书主要内容：网络安全管理及实用技术的基本知识；网络安全体系结构、无线网及虚拟专用网安全管理、IPv6安全性；网络安全的规划、测评与规范、法律法规、体系与策略、管理原则与制度；黑客的攻防与入侵检测；身份认证与访问控制；密码与加密管理；病毒及恶意软件防护；防火墙安全管理；操作系统与站点安全管理、数据与数据库安全管理；电子商务网站安全管理及应用；网络安全管理解决方案等。

包括“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和技术应用。

本书主要特色：实用、新颖、操作性强。

每章配有案例和同步实验指导、练习与实践习题等，通过机械工业出版社网站提供配套的多媒体课件和部分习题答案，方便选用。

本书可作为高等院校计算机与工程类、管理类、信息类和电子商务类专业的教材，也可作为培训及参考用书。

作者简介

贾铁军，1957年8月出生，大连人：中国人工智能学会理事.上海电机学院信息技术研究所副所长，计算机三级教授、硕士生导师，校重点学科“计算机应用技术”学术带头人；曾任电子信息学院副院长等职；研究方向：人工智能、网络信息安全；大连理工大学硕士毕业.西安电子科技大学“网络信息安全”博士班深造；近30年来一直从事本科生和研究生的“网络安全”等课程的教学和研究工作；共主持或主要参加国家、省（部）、市级以上科研项目13项。

出版专著和规划教材15部。

发表学术论文60多篇：多次主持省（市）级重点科研或教研项目及重点课程建设项目。

多次获得省（市）级“科技进步奖”、“教学成果奖”和“优秀教师”等。

书籍目录

前言第1章 网络安全管理概论1.1 网络安全管理概述1.1.1 网络安全管理的概念及目标1.1.2 网络安全管理的内容1.1.3 网络安全管理的基本任务1.2 网络安全威胁的现状、类型及发展趋势1.2.1 网络安全威胁的现状1.2.2 网络安全威胁的类型1.2.3 网络安全威胁的发展趋势1.3 网络安全风险及隐患1.3.1 网络系统安全风险及隐患1.3.2 操作系统的漏洞及隐患1.3.3 网络数据库的安全风险1.3.4 防火墙的局限性1.3.5 安全管理及其他问题1.4 网络安全管理的现状及发展趋势1.4.1 国外网络安全管理的现状1.4.2 我国网络安全管理的现状1.4.3 网络安全管理的发展趋势1.5 网络安全管理的主要功能1.5.1 网络管理的主要功能1.5.2 网络安全管理的功能及过程1.6 网络安全管理技术概述1.6.1 网络安全管理的关键技术1.6.2 网络安全管理模型1.7 实体安全管理概述1.7.1 实体安全管理的概念及内容1.7.2 媒体安全及物理隔离1.8 构建虚拟局域网(VLAN)实验1.8.1 实验目的1.8.2 实验要求及方法1.8.3 实验内容及步骤1.9 本章小结1.10 练习与实践第2章 网络安全管理技术基础2.1 网络协议安全体系2.1.1 网络协议安全概述2.1.2 TrcP / IP层次安全2.1.3 IPv6的安全2.2 虚拟专用网管理技术2.2.1 VPN概述2.2.2 VPN的特点2.2.3 VPN的实现技术2.2.4 VPN的应用2.3 无线网络安全管理2.3.1 无线网络安全概述2.3.2 无线网络设备安全管理2.3.3 IEEE802.1 x身份认证2.3.4 无线网络安全技术应用实例2.3.5 蓝牙无线网络安全2.4 常用网络安全管理工具2.4.1 Windows网络安全管理工具2.4.2 Linux网络安全管理工具2.5 无线网络安全管理实验2.5.1 实验目的2.5.2 实验要求2.5.3 实验内容及步骤2.6 本章小结2.7 练习与实践二第3章 网络综合安全管理3.1 网络安全保障体系3.1.1 网络安全保障体系概述3.1.2 网络安全管理及运作体系3.2 网络安全的法律法规3.2.1 国外的网络安全法律法规3.2.2 我国的网络安全法律法规3.3 网络安全管理规范及策略3.3.1 网络信息安全管理规范3.3.2 网络信息安全管理策略3.3.3 网络信息安全政策体系3.4 网络安全评估准则和方法3.4.1 国外网络安全评估标准3.4.2 国内网络安全评估通用准则3.4.3 网络安全评估方法3.5 网络安全管理的原则及制度3.5.1 网络安全管理的基本原则3.5.2 网络信息安全指导原则3.5.3 网络安全管理机构 and 制度3.6 网络安全规划概述3.6.1 网络安全规划原则和策略3.6.2 安全组网和防御方案3.7 Web服务器的安全设置与管理实验3.7.1 实验目的3.7.2 实验要求及方法3.7.3 实验内容及步骤3.8 本章小结3.9 练习与实践三第4章 黑客攻击的防范与入侵检测4.1 网络黑客概述4.1.1 黑客的概念及类型4.1.2 黑客常用的攻击方法4.2 黑客攻击的目的及步骤4.2.1 黑客攻击的目的4.2.2 黑客攻击的步骤4.3 常用的黑客攻防技术4.3.1 端口扫描攻防4.3.2 网络监听攻防4.3.3 密码破解攻防4.3.4 特洛伊木马攻防4.3.5 缓冲区溢出攻防4.3.6 拒绝服务攻防4.3.7 其他攻防技术4.4 防范攻击的策略和措施4.4.1 防范攻击的策略4.4.2 防范攻击的措施4.5 入侵检测概述4.5.1 入侵检测的概念4.5.2 入侵检测系统的功能及分类4.5.3 常见入侵检测的方法4.5.4 入侵检测及防御系统4.5.5 入侵检测及防御技术的发展趋势4.6 Sniffer检测实验4.6.1 实验目的4.6.2 实验要求及方法4.6.3 实验内容及步骤4.7 本章小结4.8 练习与实践四第5章 身份认证与访问控制5.1 身份认证技术概述5.1.1 身份认证的概念5.1.2 身份认证系统5.2 认证系统与数字签名5.2.1 认证系统5.2.2 数字签名5.3 访问控制5.3.1 访问控制概述5.3.2 访问控制的模式与分类5.3.3 访问控制的安全策略5.3.4 认证服务与访问控制系统5.3.5 准入控制与身份认证管理5.4 安全审计5.4.1 安全审计概述5.4.2 系统日志审计5.4.3 审计跟踪5.4.4 安全审计的实施5.5 访问列表与Telnet访问控制实验5.5.1 实验目的5.5.2 实验要求及方法5.5.3 实验内容及步骤5.6 本章小结5.7 练习与实践五第6章 密码与加密管理6.1 密码技术概述.....第7章 数据库系统安全管理第8章 计算机病毒的防治第9章 防火墙安全管理第10章 操作系统与站点安全管理第11章 电子商务的安全管理第12章 网络安全管理方案及应用参考文献

章节摘录

插图：1.4.3 网络安全管理的发展趋势网络安全管理的发展趋势主要体现在以下几个方面：（1）安全管理技术不断更新为了适应网络安全威胁的发展和变化，不断出现一些新的安全理论和技术，如云安全、网络隔离、智能检测、可信服务、虚拟技术、信息隐藏技术和软件安全扫描等技术。

（2）安全管理技术集成化 统一威胁管理（Unified Threat Management, UTM）是集多种网络安全防护技术一体化的解决方案，可保障网络安全的同时大量降低运行维护成本，因此，受到广大用户的欢迎。

网络安全技术优化集成已成趋势，如杀毒软件与防火墙集成、虚拟网（VPN）与防火墙的集成、入侵检测系统（IDS）与防火墙的集成，以及安全网关、主机安全防护系统、网络监控系统等集成技术。

（3）新型网络安全管理平台统一协调管理是实现网络安全管理的重要手段，也是安全技术发展的一大趋势。

其主要包括网络安全管理平台、统一威胁管理工具和日志审计分析系统等。

（4）高水平的人才和服务网络安全威胁严重性及发展变化，要求更高的解决网络安全问题的技术和经验，急需高水平的网络安全人才和服务。

网络安全服务也将随着网络安全产业和业务的发展而扩展，作为一种技术也需要工具和规范的支持。对网络系统进行定期的风险评估，通过各种措施对网络系统进行安全加固，逐渐交给网络安全服务公司或团队将成为一种趋势。

为用户提供有效的网络安全管理方案是网络安全服务的基本手段，对网络系统建设方案的安全评估、对人员安全培训也是网络安全服务的重要内容。

<<网络安全管理及实用技术>>

编辑推荐

《网络安全管理及实用技术》是教育部高等学校管理科学与工程类学科专业教学指导委员会推荐教材

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>