<<计算机网络安全与应用>>

图书基本信息

书名：<<计算机网络安全与应用>>

13位ISBN编号：9787122125552

10位ISBN编号：7122125556

出版时间：2012-1

出版时间：化学工业出版社

作者：陈学平　主编

前言

本书注重实践技能的培养，以实验为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的教材，也可作为计算机网络安全类的技术参考书或培训教材。
本书从实战出发，以应用为目的，防范网络入侵为重点，是一本系统性、实战性、应用性较强的网络安全教程。
本书摒弃了传统网络安全课程理论过多、实用性不强的缺点，紧密跟踪网络安全领域最新问题和技术运用，从应用的角度，系统讲述了网络安全所涉及的理论及技术。
以阶段能力培养为目的，每个能力阶段为一个章节，通过实战演练，学生将具备综合运用所学的技术进行网络信息安全方面的实际工作能力。
本书首先系统介绍和分析了网络安全的定义、标准、模型，以及常见的网络安全威胁，然后从网络管理与安全防护入手，详细讲述和分析了入侵检测、数据加密、身份验证、防火墙以及无线网安全等多方面的理论与技术，同时结合现场工程应用，有机地将网络安全管理技术与主流系统软硬件结合，突出实践能力培养。
本书安排了多个实验，便于读者亲身体验企业网络安全管理与防护的实际应用。
本书内容系统全面，结构清晰，注重实用性和应用性，主要特色如下。
1．本书力求做到理论与实践相结合，课程内容与实验相结合。
通过实验，让读者加深对网络安全理论知识的理解，掌握网络安全管理的技能，以期达到活学活用的目的。
2．本书是一本内容丰富、特色鲜明、实用性强的信息安全理实一体化教材。
本书包含了主流网络安全测试仪器的操作和使用，同时安排了无线网络安全的实训内容，对于丰富读者的网络安全实践经验，提高读者的网络安全管理水平，具有非常重要的意义。
3．本书每个实验都要求填写实训报告，便于读者对实验过程和结果进行分析和总结，并对所提出的问题进行深入思考。
4．本书从企业网络安全应用和专业角度出发，立足于“看得懂、学得会、用得上”，重点突出最新网络安全技术的可操作性和实用性，强化读者的网络安全防护能力。
我们将为使用本书的教师免费提供电子教案，需要者可以到化学工业出版社教学资源网站免费下载使用。
本书由重庆电子工程职业学院陈学平担任主编，重庆电子工程职业学院李明担任副主编，陈学平编写了全书大纲，并统稿。
本书第1～3章由李明编写，第4章由河南省漯河市漯河职业技术学院吴雪毅编写，第5章由洛阳市第一职业中等专业学校于志博编写，第6章由吉林电子信息职业技术学院战忠丽编写，第7～13章由陈学平编写。
本书在编写和出版过程中得到了化学工业出版社的支持与帮助，也得到了编者家人的支持，在此一并表示感谢。
编者2011年9月

<<计算机网络安全与应用>>

内容概要

本书从网络系统安全管理和应用的角度出发，重点介绍网络安全技术及其应用，各章在介绍网络安全技术后均配以相应的实践内容或应用实例，体现培养读者网络安全及管理技术的应用能力和实践操作技能的特色。
本书对原理、技术难点的介绍适度，将理论知识和实际应用紧密地结合在一起，典型实例的应用性和可操作性强；章末配有练习题，便于学生学习和实践，内容安排合理，重点突出，文字简明，语言通俗易懂。

本书可作为普通高校计算机、通信、信息安全等专业的应用型本科、高职高专或成人教育学生的网络安全实践教材，也可作为网络管理人员、网络工程技术人员和信息安全管理人员的参考书。

<<计算机网络安全与应用>>

书籍目录

章节摘录

版权页：插图：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。
从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。
对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成巨大的经济损失。
从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。
因此，网络安全在不同的环境和应用会得到不同的解释。
①运行系统安全即保证信息处理和传输系统的安全。
包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。
它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏产生信息泄露，干扰他人（或受他人干扰），本质上是保护系统的合法操作和正常运行。
②网络上系统信息的安全包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。
③网络上信息传播的安全即信息传播后果的安全。
包括信息过滤，不良信息的过滤等。
它侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法律或国家利益。
④网络上信息内容的安全即我们讨论的狭义的“信息安全”。
它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。
显而易见，网络安全与其所保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。
显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。
下面给出本书所研究和讨论的网络安全的含义。
网络安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。
网络安全的结构层次包括：物理安全、安全控制和安全服务。

编辑推荐

《计算机网络安全与应用》重点介绍网络安全技术及其应用，各章均配以相应的实践内容或应用实例，将理论知识和实际应用紧密地结合在一起，典型实例的应用性和可操作性强，突出了实践操作技能的特色。
《计算机网络安全与应用》将课程内容与实验相结合，结合现场工程应用，安排了十多个实验，让读者加深对网络安全理论知识的理解，掌握网络安全管理的技能，以期达到活学活用的目的。
《计算机网络安全与应用》将网络安全管理技术与主流系统软硬什有机结合，介绍了主流网络安个测试仪器的操作和使用，同时安排了无线网络安全的实训内容，有利于读者全面掌握计算机网络安全技术。

<<计算机网络安全与应用>>

版权说明