《网络安全与管理实验教程》

图书基本信息

书名：《网络安全与管理实验教程》

13位ISBN编号：9787560620633

10位ISBN编号：7560620639

出版时间：2008-8

出版社：谢晓燕 西安电子科技大学出版社 (2008-08出版)

作者：谢晓燕 编

页数：385

《网络安全与管理实验教程》

前言

在计算机网络技术已被广泛应用的今天，各种网络安全威胁和网络管理问题使得人们不得不认真考虑如何加强计算机的系统安全性，采用什么样的安全通信方式更好，如何加强网络的安全防御措施，如何监控网络性能，如何及时发现网络故障，以及如何保证网络长期健壮运行等问题。目前，网络安全和管理技术经过了长期的迅速发展，出现了许多应用于网络安全与管理的软硬件产品，这就要求网络管理人员应具备运用相关技术对这些产品进行合理配置的能力。在本科培养阶段，许多高等院校已将“网络安全与管理技术”作为网络工程专业的必修课程。该课程具有理论深、抽象度高、实践性强等特点，初学者对于大量概念与原理的理解深度往往取决于实践操作的强度。编写本书旨在通过明确的实验目的和详细的实验过程，指导学生有目的、有步骤地完成各项实践操作，由浅入深地引导学生发现问题和解决问题，加强其实践动手能力和对理论知识的理解。本书就网络安全与管理方面的典型问题，在概括介绍理论知识的基础上，设计了相关实验，全书分为五章和三个附录。第1章通过对DES、RSA和MD5三种典型安全算法的介绍，分析了加密与认证技术的基本原理，说明了如何用C语言来实现这三种典型的算法，并在附录中给出了算法源程序。第2章就操作系统本身的安全问题，分别讲述了如何提高Windows、Linux两类典型操作系统的安全性，主要包括用户帐户、文件系统安全、端口安全、审核和日志等内容。第3章在简单介绍了网络协议分析软件SnifferPro的使用后，详细介绍了四种典型的安全通信应用，包括PGP、CA认证系统、IP安全（IPSec）和虚拟专用网络（VPN），并针对性地设计了相关实验项目。第4章首先简单介绍了ACL分类，并按不同类型设计相关实验，详细描述了针对不同通信要求在路由器上实现访问控制功能的基本方法；接着重点介绍了防火墙设备的配置，在简明阐述基本概念后，通过对实验过程的详细描述，讨论了防火墙的工作过程和控制原则，阐明了使用防火墙实现网络边界安全的基本方法。第5章基于SNMP的网络管理概念，结合实验首先描述了如何使用Snmputil工具进行SNMP基本操作；然后介绍了AT-SNMPc软件的基本操作以及路由器的SNMP配置；最后详细描述了各种SNMPPDU的格式，并对编码进行了分析。本书根据编者长期从事“网络安全与管理技术”课程的讲授以及相关实验指导所积累的经验，通过对内容的反复筛选以及对实验项目的精心设计，逐步编写而成。本书具有以下显著特点：理论与实践结合紧密；实验项目具有良好的可操作性，实验目的明确，需要的实验环境可根据实际的实验条件灵活调整；实验过程步骤清晰，内容翔实，图文并茂，在提高实验操作效率的同时，可有效降低初学者的学习难度。本书由谢晓燕担任主编，赵婧如、马素刚担任副主编。谢晓燕负责全书的定稿与审核任务，并编写了第1章和附录A、B、C。赵婧如编写了第4章和第5章，马素刚编写了第2章和第3章。限于编者的水平，书中难免有疏漏之处，恳请广大读者批评指正。

《网络安全与管理实验教程》

内容概要

《网络安全与管理实验教程》

书籍目录

《网络安全与管理实验教程》

章节摘录

第1章　数据加密算法及Hash算法加密算法可以保护机密数据不被窃取或篡改。Hash算法能够用来对报文的完整性进行认证。有时为了很好地解决数据传输的机密性、完整性及不可否认性等问题，需要将二者结合使用。DES、RSA分别是对称和非对称两种密码体制的典型算法，而MD5是一种典型的Hash算法。本章分别对DES、RSA、MD5三种算法进行详细分析，并通过示例程序说明如何使用C语言来实现这三种算法。1.1　数据加密概述在互联网上进行文件、电子商务往来等信息传输时存在许多不安全因素，尤其是一些机密文件在网络上传输时，信息安全显得尤为重要。不安全性是互联网的存在基础——TCP／IP协议所固有的，因此解决这一问题的方案就是加密，加密后的数据被别人获得后，在解密之前是不可读的。数据加密是所有数据安全技术的核心。加密在网络上的作用是，防止重要的或私有化信息在网络上被截获和篡改。需要说明的是，文件加密不只应用于电子邮件等网络上的传输，也可应用于静态文件的保护。数据加密是指对原来被称为“明文”的数据按某种算法进行处理，使其成为不可读的一段代码的过程。通常把通过加密得到的代码称为“密文”。数据加密的逆过程称为数据解密，即将密文转化为明文的过程。只有利用相应的密钥对密文进行解密，才能显示出明文的内容，通过这样的途径能够保护数据不被非授权的访问者非法窃取。加密技术通常分为两大类：常规密钥密码体制和公开密钥密码体制。所谓常规密钥密码体制，是指加密密钥与解密密钥相同的密码体制。这种加密系统又称为对称密钥系统。美国政府采用的DES加密标准就是一种典型的对称式加密方法。

《网络安全与管理实验教程》

编辑推荐

《网络安全与管理实验教程》

版权说明