<<计算机网络安全技术教程>>

图书基本信息

书名：<<计算机网络安全技术教程>>

13位ISBN编号：9787508473017

10位ISBN编号：7508473019

出版时间：2010-4

出版时间：水利水电出版社

作者：刘华春，蒋志平 编著

页数：299

前言

随着政府上网、企业上网、教育上网及家庭上网的普及，计算机网络在经济、军事及文教等诸多领域得到了广泛应用。
计算机网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。
计算机网络存储、传输和处理政府宏观调控决策、商业经济、银行资金转账、股票证券、能源资源、国防和科研等大量关系国计民生的重要信息。
如何保护个人、企业和国家的机密信息不被黑客和间谍入侵，如何保证网络系统安全、不间断地工作，是国家和单位信息化建设必须考虑的重要问题。
因此，使计算机网络系统免遭破坏，提高系统的安全可靠性，已成为人们关注和亟须解决的问题。
每个单位的网络管理与维护人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全稳定地运行并提供正常而安全的服务。
本教程全面介绍了网络安全基础理论和网络安全应用技术，以面向应用为主线，以解决实际网络安全问题为内容进行内容组织。
全书分为4大部分，第1部分（1、2章）为计算机网络安全技术基础，主要介绍了网络安全技术的基础理论和网络安全程序设计的常用方法。
第2部分（3章）为信息加密技术，这部分对网络安全核心的基础设施——信息加密技术进行了的讲解，读者学习后面章节才能达到“知其然，还能知其所以然”的目的。
第3部分（4-7章）为网络安全，主要面向实际的计算机网络安全应用，对各种网络安全中的应用问题进行专门的分析和讲解。
第4部分（8-10章）为系统安全，主要介绍操作系统的安全、病毒防范和数据安全。
在编者多年的网络安全课程的教学中，使用了多本网络安全的教材和参考书，发现目前市面上的网络安全书籍主要有两类：一类是纯粹面向高校教学的，多见于一些重点本科高校使用的教材，这部分教材的特点就是理论翔实，适合于深入学习和研究网络安全使用。
而另一类，则是完全面向市场的网络安全技术的纯粹应用性书籍，这些书籍以介绍网络安全攻防工具的使用为主，以培养网络安全方面的速成人才为目标。
其实，网络安全作为一门有一定技术难度又与现实应用结合紧密的学科，只有在理论基础与实际应用这两者之间找到最佳结合点，才能让学生真正学好这门课程，这就是我们编写本教材的目的。
总体来讲，本教程的特点可以归纳为如下几点。

<<计算机网络安全技术教程>>

内容概要

本书系统地介绍了计算机网络的安全体系，将安全理论，攻、防技术，安全程序设计，网络安全工具等有机地结合起来。
全书从网络安全体系上共分为4个部分10章。
第1部分是计算机网络安全技术基础，介绍计算机网络安全的基本概念和网络安全程序设计的内容。
第2部分是信息加密技术，介绍密码学和信息加密原理。
第3部分是网络安全技术，主要介绍网络入侵与攻击技术、防火墙与入侵检测系统、身份认证与访问控制、IP安全与VPN技术。
第4部分是系统安全，介绍操作系统的安全、系统安全策略、病毒的分析与防范等内容。
本书可作为普通高等院校（尤其是应用型本科院校）、高等职业技术学院电子信息相关专业的网络安全课程教材，也可供各个企事业单位的网络管理维护人员和计算机工程技术人员作为自学参考书。

<<计算机网络安全技术教程>>

书籍目录

第1部分 计算机网络安全技术基础 第1章 网络安全概述 1.1 网络安全介绍 1.2 计算机网络面临的威胁 1.3 网络安全的基本技术与策略 1.4 常用的网络协议 1.5 常用的网络服务 1.6 常用的网络命令 1.7 环境配置 本章小结 习题 第2章 网络安全程序设计基础 2.1 Windows程序设计基础 2.2 Socket通信程序设计 2.3 网络安全程序设计 本章小结 习题 第2部分 信息加密技术 第3章 信息加密原理与技术 3.1 密码学概述 3.2 DES对称加密技术 3.3 RSA公钥加密算法 3.4 PGP加密技术 3.5 单向散列函数 3.6 数字签名与数字信封 3.7 数字证书 3.8 公钥基础设施 本章小结 习题 第3部分 网络安全技术 第4章 网络入侵与攻击技术 4.1 黑客攻击概述 4.2 网络扫描技术 4.3 网络监听 4.4 口令攻击 4.5 ARP欺骗攻击 4.6 拒绝服务攻击 4.7 缓冲区溢出攻击 4.8 IP地址欺骗攻击 4.9 DNS欺骗攻击 4.10 Web攻击 4.11 木马攻击技术 4.12 网络后门 本章小结 习题 第5章 防火墙与入侵检测系统 5.1 防火墙概述 5.2 防火墙技术的分类 5.3 防火墙的体系结构 5.4 防火墙系统的设计 5.5 防火墙产品介绍 5.6 入侵检测系统概念 5.7 入侵检测的分类 5.8 入侵检测的步骤 5.9 入侵检测工具介绍 本章小结 习题 第6章 IP安全与VPN技术 6.1 IP安全概述 6.2 IPSec协议 6.3 IPSec协议的优点及应用 6.4 VPN 本章小结 习题 第7章 WWW安全 7.1 WWW安全概述 7.2 Web的安全漏洞与检测 7.3 Web服务器的安全配置 7.4 增强Web的安全陆的相关措施 7.5 SSL安全协议 本章小结 习题 第4部分 系统安全 第8章 操作系统安全 8.1 操作系统安全概述 8.2 操作系统的安全机制 8.3 操作系统的安全性评测 8.4 Windows操作系统安全性分析 8.5 Windows操作系统的安全配置 本章小结 习题 第9章 计算机病毒分析与防治 9.1 计算机病毒概述 9.2 计算机病毒的工作机制 9.3 典型计算机病毒分析 9.4 计算机病毒的防治技术 9.5 杀毒软件介绍 本章小结 习题 第10章 数据与数据库安全 10.1 数据安全 10.2 数据库系统安全 10.3 SQL Server 2005数据库系统安全管理 本章小结 习题 参考文献

章节摘录

插图：1.2.1 人为因素的威胁1.人为的无意失误（1）安全配置不当造成的安全漏洞。
系统管理员设置资源访问控制的失误，而导致一些资源被偶然或故意地破坏，造成对网络信息保密性的破坏。
（2）无意的信息泄露。
合法用户进入安全进程后中途离开而给非法用户提供可乘之机，口令、密钥等保管不善而为他人非法获得，用户安全意识不强、口令选择不慎、将自己的账号随意转借或与别人共享等都会给网络安全造成威胁。
（3）操作失误。
删除文件、格式化硬盘、线路拆除等操作失误，系统掉电，“死机”等系统崩溃引起信息缺失，从而造成对网络信息完整性和可用性的破坏。
2.人为的恶意攻击这是计算机网络所面临的最大威胁，对手的攻击和计算机犯罪同属此类。
此类攻击又可以分为两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，是纯粹的信息破坏。
这类积极攻击者通常截取网上信息包，对其进行更改使之失效，故意篡改信息，或者登录系统占用大量网络资源从而导致资源消耗，损害合法用户的利益。
这类攻击者的破坏作用最大。
另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，这类攻击者称为消极攻击者。
两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。
人为恶意攻击具体可表现在以下几个方面：（1）非授权访问。
未经同意而使用网络或计算机资源被看做非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或者擅自扩大权限，越权访问信息等。
其主要表现形式有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

编辑推荐

《计算机网络安全技术教程》：21世纪高等院校精品规划教材

版权说明