<<计算机网络安全案例教程>>

图书基本信息

书名：<<计算机网络安全案例教程>>

13位ISBN编号：9787301140840

10位ISBN编号：7301140843

出版时间：2008-8

出版时间：北京大学出版社

作者：陈昶，杨艳春　主编

页数：280

前言

<<计算机网络安全案例教程>>

内容概要

本书从网络安全的概述引入，从网络安全的角度出发，全面介绍网络安全的基本理论以及网络安全方面的管理、配置和维护。

全书共分为11章，主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、网络防病毒、数据加密、防火墙技术、入侵检测技术、Windows 2000的安全、Web的安全性、虚拟专用网（VPN）技术、数据库系统安全、实验指导及综合实训，各章节内容都包括引例、教学目标、教学要求、正文、本章小结、练习题。

本书注重实习性，实例丰富典型，实验内容和案例融合在课程内容中，将理论知识与实践操作很好地结合起来，最后一章的“实验指导及综合实训”注重培养实践操作能力，并作为全书内容的一个综合实训。

本书可作为高职高专计算机、电子商务等相关专业学生的教材，也可作为技术参考书或培训教材。

<<计算机网络安全案例教程>>

书籍目录

章节摘录

第1章　计算机网络安全概述1.1 信息安全简介信息安全（InfoSec）是一门交叉学科，涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。
1.1.1 信息安全的发展历程信息安全在其发展过程中经历了3个阶段。
1.通信安全阶段早在20世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即COMSEC（Communication Secul7ity）。
2.信息安全阶段 20世纪80年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即INFOSEC（Information Securiity）。
3.信息保障阶段20世纪90年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到了极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性3个原则了，并衍生出了诸如抗否定性、可控性、真实性等其他原则，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段，即IA（Information Assurance）。
信息保障的核心思想是对系统或数据的4个方面的要求：保护（Protect）、检测（Detect）、反应（React）和恢复（Restore），即PDRR。
1.1.2　信息安全的3个最基本的原则信息安全的3个最基本原则是保密性、完整性和可用性，即C.I.A三元组。
1.保密性保密性（Confidentiality）即保护信息的内容免遭有意的、无意的或未授权的泄漏。
有许多方法可以损害保密性，如有意泄露公司的私有信息或滥用网络特权。
2.完整性完整性（Integrity）即确保未授权的人员或过程不能修改数据；已授权的人员或过程未经授权不能修改数据；数据的内部与外部相一致。

编辑推荐

<<计算机网络安全案例教程>>

版权说明