

<<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

出版单位：北京大学出版社

作者：陈昶，杨艳春 主编

页数：280

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>



## <<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。

。

## &lt;&lt;计算机网络安全案例教程&gt;&gt;

## 书籍目录

第1章 计算机网络安全概述 1.1 信息安全简介 1.1.1 信息安全的发展历程 1.1.2 信息安全的3个最基本的原则 1.1.3 信息安全的知识体系 1.2 网络安全简介 1.2.1 网络安全的定义 1.2.2 网络安全案例 1.2.3 网络安全所涉及的内容 1.2.4 网络安全的特征 1.3 研究网络安全的必要性 1.4 网络安全相关法规 1.4.1 网络安全的相关政策法规 1.4.2 关于保密和网络安全管理的相关法规条例 (摘录) 本章小结 练习题第2章 黑客常用的系统攻击方法 2.1 黑客概述 2.1.1 黑客与骇客 2.1.2 著名黑客 2.1.3 黑客守则 2.1.4 黑客行为的发展趋势 2.2 网络扫描工具原理与使用 2.2.1 ping 2.2.2 X.Scan 2.2.3 nessus 2.2.4 nmap 2.3 网络监听原理与工具 2.3.1 网络监听的原理 2.3.2 网络监听工具 2.3.3 网络监听的防范 2.4 木马 2.4.1 什么是木马 2.4.2 木马的种类 2.4.3 木马系统的组成 2.4.4 木马攻击原理 2.4.5 木马的清除 2.5 拒绝服务攻击 2.5.1 DoS 2.5.2 DDoS 2.5.3 DRDoS 2.6 缓冲区溢出 2.6.1 缓冲区溢出的概念和原理 2.6.2 缓冲区溢出漏洞攻击方式 2.6.3 缓冲区溢出的防患 本章小结 练习题第3章 网络防病毒 3.1 计算机病毒的基本概念 3.1.1 计算机病毒的由来 3.1.2 计算机病毒的定义 3.2 计算机病毒的特征 3.3 计算机病毒的分类 3.3.1 按照计算机病毒存在的媒体进行分类 3.3.2 按照计算机病毒传染的方法进行分类 3.3.3 按照病毒破坏的能力进行分类 3.3.4 按照病毒特有的算法进行分类 3.3.5 按照病毒名进行分类 ..... 第4章 数据加密第5章 防火墙技术第6章 入侵检测技术第7章 Windows 2000的安全第8章 Web的安全性第9章 VPN技术第10章 数据库系统安全第11章 实验指导及综合实训部分习题参考答案参考文献

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 Security）。

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 Security）。

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）即确保未经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。

<<计算机网络安全案例教程>>

编辑推荐

<<计算机网络安全案例教程>>

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>