

<<计算机网络安全技术>>

图书基本信息

书名：<<计算机网络安全技术>>

13位ISBN编号：9787508408910

10位ISBN编号：7508408918

出版时间：2002-01

出版时间：中国水利水电出版社

作者：蔡立军

页数：337

字数：484000

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>

<<计算机网络安全技术>>

内容概要

本书详细地介绍了计算机网络安全技术的基础理论、原理及其实现方法。

内容包括：计算机网络安全技术概论、实体安全与硬件防护技术、计算机软件安全技术、网络安全防护技术、备份技术、密码技术与压缩技术、数据库系统安全、计算机病毒及防治、防火墙技术和系统平台与网络站点的安全。

全书涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实例技术。

本书从工程应用角度出发，立足于“看得懂、学得会、用得上”，在内容安排上将理论知识与工程应用有机结合，突出适应性、实用性和针对性。

书中介绍的许多安全配置实例都来自作者多年的实践，读者可在今后工作中直接应用。

本书可以作为高职高专计算机专业及相近专业和本科计算机相近专业的教材，也可作为计算机网络安全培训、自学教材；也是网络工程技术人员、网络管理员、信息安全管理技术人员的技术参考书。

本书还为授课教师免费提供电子教案，此教案用PowerPoint制作，可以任意修改。

<<计算机网络安全技术>>

书籍目录

序

前言

第一章 计算机网络安全技术概论

本章学习目标

1.1 计算机网络安全的概念

1.2 计算机网络系统面临的威胁

1.2.1 计算机网络系统面临的威胁

1.2.2 安全威胁的来源

1.2.3 威胁的具体表现形式

1.3 计算机网络系统的脆弱性

1.3.1 操作系统安全的脆弱性

1.3.2 网络安全的脆弱性

1.3.3 数据库管理系统安全的脆弱性

1.3.4 防火墙的局限性

1.3.5 其他方面的原因

1.4 计算机网络安全技术的研究内容和发展过程

1.4.1 研究内容

1.4.2 发展过程

1.5 计算机网络安全的三个层次

1.5.1 安全立法

1.5.2 安全管理

1.5.3 安全技术措施

1.6 网络安全的设计和基本原则

1.6.1 安全需求

1.6.2 网络安全设计应考虑的问题

1.6.3 网络安全系统设计的基本原则

1.6.4 网络安全设计的关键

1.7 安全技术评价标准

本章小结

习题一

第二章 实体安全与硬件防护技术

本章学习目标

2.1 实体安全技术概述

2.1.1 影响实体安全的主要因素

2.1.2 实体安全的内容

2.2 计算机房场地环境的安全防护

2.2.1 计算机房场地的安全要求

2.2.2 设备防盗

2.2.3 机房的三度要求

2.2.4 防静电措施

2.2.5 电源

2.2.6 接地与防雷

2.2.7 计算机场地的防火、防水措施

2.3 安全管理

2.3.1 硬件资源的安全管理

<<计算机网络安全技术>>

2.3.2 信息资源的安全与管理

2.3.3 健全机构和岗位责任制

2.3.4 完善的安全管理规章制度

2.4 电磁防护

2.5 硬件防护

2.5.1 存储器保护

2.5.2 虚拟存储保护

2.5.3 输入/输出通道控制

本章小结

习题二

第三章 计算机软件安全技术

本章学习目标

3.1 计算机软件安全技术概述

3.2 文件加密技术

3.2.1 数据文件加密原理

3.2.2 可执行文件的加密方式

3.3 软件运行中的反跟踪技术

3.3.1 跟踪工具及其实现

3.3.2 软件运行中的反跟踪技术

3.3.3 实例：编制具有反跟踪功能的加密盘

3.4 防止非法复制软件的技术

3.4.1 软件加密的必要性

3.4.2 常用的防止非法复制软件的技术

3.4.3 实例：几种加密软件的使用原理及方法

3.5 保证软件质量的安全体系

3.5.1 概述

3.5.2 软件故障的分类

3.5.3 软件测试工具

本章小结

习题三

第四章 网络安全防护技术

本章学习目标

4.1 网络安全概述

4.1.1 网络安全的定义

4.1.2 网络安全的研究内容

4.1.3 Internet安全面临的威胁

4.1.4 个人上网用户面临的网络陷阱

4.2 计算机网络的安全服务和安全机制

4.2.1 计算机网络的安全服务

4.2.2 计算机网络的安全机制

4.2.3 安全服务和安全机制的关系

4.2.4 安全服务机制的配置

4.2.5 安全服务与层的关系的实例

4.3 网络安全防护措施

4.3.1 网络的动态安全策略

4.3.2 网络的安全管理与安全控制机制

4.3.3 网络安全的常规防护措施

<<计算机网络安全技术>>

4.3.4 网络安全控制措施

4.3.5 网络安全实施过程中需要注意的一些问题

本章小结

习题四

第五章 备份技术

本章学习目标

5.1 备份技术概述

5.1.1 备份的基本知识

5.1.2 网络备份

5.1.3 数据失效与备份的意义

5.1.4 与备份有关的概念

5.2 备份技术与备份方法

5.2.1 硬件备份技术

5.2.2 软件备份技术

5.2.3 双机互联硬件备份方法

5.2.4 利用网络资源备份

5.2.5 系统备份软件——Norton Ghost

5.2.6 同步动态备份软件——Second Copy 2000

5.2.7 多平台网络备份系统——Amanda

5.2.8 重新认识Windows 98的备份技术

5.3 备份方案的设计

5.3.1 系统备份方案的要求及选择

5.3.2 日常备份制度设计

5.3.3 灾难恢复措施设计

5.4 典型的网络系统备份方案实例

5.4.1 基于CA ARC Serve的备份方案设计

5.4.2 一个证券网络系统的备份方案

本章小结

习题五

第六章 密码技术与压缩技术

本章学习目标

6.1 密码技术概述

6.1.1 密码通信系统的模型

6.1.2 密码学与密码体制

6.1.3 加密方式和加密的实现方法

6.2 加密方法

6.2.1 加密系统的组成

6.2.2 四种传统加密方法

6.3 密钥与密码破译方法

6.4 常用信息加密技术介绍

6.4.1 DES算法

6.4.2 IDEA算法

6.4.3 RSA公开密钥密码算法

6.4.4 典型HASH算法——MD5算法

6.4.5 信息认证技术

6.5 Outlook Express下的安全操作实例

6.6 数据压缩

<<计算机网络安全技术>>

6.6.1 数据压缩概述

6.6.2 ARJ压缩工具的使用

6.6.3 WinZip的安装和使用

本章小结

习题六

第六章 数据库系统安全

本章学习目标

7.1 数据库系统简介

7.2 数据库系统安全概述

7.2.1 数据库系统的安全性要求

7.2.2 数据库系统的安全的含义

7.2.3 数据库的故障类型

7.2.4 数据库系统的基本安全架构

7.2.5 数据库系统的安全特性

7.3 数据库的数据保护

7.3.1 数据库的安全性

7.3.2 数据库中数据的完整性

7.3.3 数据库并发控制

7.4 死锁、活锁和可串行化

7.4.1 死锁与活锁

7.4.2 可串行化

7.4.3 时标技术

7.5 数据库的备份与恢复

7.5.1 数据库的备份

7.5.2 数据库的恢复

7.6 攻击数据库的常用方法

7.7 数据库系统安全保护实例

7.7.1 SQL Server数据库的安全保护

7.7.2 Oracle数据库的安全性策略

本章小结

习题七

第八章 计算机病毒及防治

本章学习目标

8.1 计算机病毒概述

8.1.1 计算机病毒的定义

8.1.2 计算机病毒的发展历史

8.1.3 计算机病毒的分类

8.1.4 计算机病毒的特点

8.1.5 计算机病毒的隐藏之处和入侵途径

8.1.6 现代计算机病毒的流行特征

8.1.7 计算机病毒的破坏行为

8.1.8 计算机病毒的作用机制

8.2 DOS环境下的病毒

8.2.1 DOS基本知识介绍

8.2.2 常见DOS病毒分析

8.3 宏病毒

8.3.1 宏病毒的分类

<<计算机网络安全技术>>

- 8.3.2 宏病毒的行为和特征
- 8.3.3 宏病毒的特点
- 8.3.4 宏病毒的防治和清除方法
- 8.4 网络计算机病毒
 - 8.4.1 网络计算机病毒的特点
 - 8.4.2 网络对病毒的敏感性
 - 8.4.3 网络病毒实例——电子邮件病毒
- 8.5 反病毒技术
 - 8.5.1 计算机病毒的检测
 - 8.5.2 计算机病毒的防治
 - 8.5.3 计算机感染病毒后的修复
- 8.6 软件防病毒技术
 - 8.6.1 防、杀毒软件的选择
 - 8.6.2 反病毒软件
 - 8.6.3 常用反病毒软件产品
- 8.7 典型病毒实例——CIH病毒介绍
 - 8.7.1 CIH病毒简介
 - 8.7.2 恢复被CIH病毒破坏的硬盘信息
 - 8.7.3 CIH病毒的免疫
- 本章小结
- 习题八
- 第九章 防火墙技术
 - 本章学习目标
 - 9.1 防火墙技术概述
 - 9.1.1 防火墙的定义
 - 9.1.2 防火墙的发展简史
 - 9.1.3 设置防火墙的目的和功能
 - 9.1.4 防火墙的局限性
 - 9.1.5 防火墙技术发展动态和趋势
 - 9.2 防火墙技术
 - 9.2.1 防火墙的技术分类
 - 9.2.2 防火墙的主要技术及实现方式
 - 9.2.3 防火墙的常见体系结构
 - 9.3 防火墙设计实例
 - 9.3.1 防火墙产品选购策略
 - 9.3.2 典型防火墙产品介绍
 - 9.3.3 防火墙设计策略
 - 9.3.4 Windows 2000环境下防火墙及NAT的实现
 - 本章小结
 - 习题九
- 第十章 系统平台与网络站点的安全
 - 本章学习目标
 - 10.1 Windows NT系统的安全性
 - 10.1.1 Windows NT的Registry的安全性
 - 10.1.2 NT服务器和工作站的安全漏洞及解决建议
 - 10.1.3 NT与浏览器有关的安全漏洞及防范措施
 - 10.1.4 基于Windows NT操作系统的安全技术

<<计算机网络安全技术>>

10.1.5 Windows操作系统的安全维护技术

10.2 UNIX系统的安全性

10.2.1 UNIX以系统安全

10.2.2 UNIX网络安全

10.3 Web站点的安全

10.3.1 Web站点安全概述

10.3.2 Web站点的安全策略

10.4 反黑客技术

10.4.1 黑客的攻击步骤

10.4.2 黑客的手法

10.4.3 防黑客技术

10.4.4 黑客攻击的处理对策

本章小结

习题十

附录

附录A 常用备份工具软件

附录B 黑客与计算机安全站点

参考文献

<<计算机网络安全技术>>

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>