

<<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：9787030119896

10位ISBN编号：7030119894

出版时间：2009-4

出版时间：科学出版社

作者：叶忠杰 编

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>>

前言

网络技术的发展和给现代社会带来了巨大的推动和冲击，但由于计算机操作系统和网络协议的缺陷，加上层出不穷的计算机病毒和黑客攻击，使得网络的安全问题越来越突出。

人们在工作、学习、生活各方面越来越依赖网络的同时，也对安全问题深感担忧。

随着Internet / Intranet的大量应用，安全问题面临重大的挑战。

事实上，资源共享和信息安全历来就是一对矛盾，而TCP / IP协议的开放性决定了安全问题是先天存在的，肆虐的病毒、黑客的攻击更是加剧了安全问题的严重性。

随着人们对计算机网络安全问题的关注，有关计算机网络安全问题的专著、教材和读物也逐渐增多，这些书各有各的特点，为各层次读者提供了宝贵的资料，也指导着国内计算机网络安全技术的应用与研究。

本书的特点如下。

首先，通俗易懂。

计算机网络的技术性很强，网络安全的技术也晦涩难懂，使初学者很难入门。

本书以通俗的语言和清晰的叙述方式，向读者介绍计算机网络安全的基本理论、基本知识和常用技术。

其次，注重实用。

阅读本书，可使读者掌握计算机网络安全的基本概念，并了解设计和维护网络及其应用系统安全的基本手段和方法。

尽可能减少原理性和理论性的介绍，突出应用的实际需求，多数章节安排了“案例分析”和“建议实验”，能直接满足网络安全的基本需求。

本书介绍了许多实用的安全工具软件，多数是社会上主流的产品和技术。

第三，技术新颖。

计算机和网络技术的发展非常迅速，为了使本书能反映较新的理论和技术，我们参考了大量的国内外最新资料，以尽量靠近新知识、新技术的前沿。

全书共分10章。

第1、2、5和6、7章分别由浙江交通职业技术学院的叶忠杰和戎成编写，第3、4章由浙江金融职业学院的陈月波编写，第8、9章由天津石油职业技术学院的徐建功编写，第10章由浙江吉利汽车销售有限公司网络总监胡乃翔编写，柳州运输职业技术学院黄锋老师承担了本书的审稿工作。

为了方便教学，本书配有电子课件，课件可到科学出版社网站（www.sciencep.com）下载或发邮件至主编邮箱yehongjie@zjvtit.edu.ca索取。

在向读者推荐本书的同时，也深感计算机网络安全技术的精深和发展，以我们的现有水平很难在本书中全面、准确和及时反映，因此，书中难免会有疏漏甚至错误之处，在此恳请广大读者批评指正。

<<计算机网络安全技术>>

内容概要

《计算机网络安全技术》介绍了计算机网络安全的基本知识和技术，包括计算机网络安全概论、信息加密技术基础、局域网安全技术及应用、操作系统安全技术、网络防火墙技术及应用、数字签名与CA认证技术、Internet安全技术及应用、计算机病毒与网络安全、网络黑客与入侵检测、常用网络安全软件及使用等内容。

多数章节安排了“案例分析”和“建议实验”，能直接满足网络安全的基本需求；在各章节中还介绍了相关的安全工具，多数属于社会主流的产品和技术。

《计算机网络安全技术》结构合理、概念清晰、内容新颖，突出实际应用，可读性强。

《计算机网络安全技术》适合作为高职高专院校相关专业课程的教材，也可供各行各业从事计算机网络应用和管理的读者参考。

<<计算机网络安全技术>>

书籍目录

第1章 计算机网络安全概论

1.1 网络安全概述

1.1.1 网络安全形势与安全事例

1.1.2 计算机和网络安全的含义

1.1.3 安全网络的特征

1.1.4 网络的安全威胁与安全网络的实现

1.2 网络安全的体系结构

1.2.1 OSI安全服务

1.2.2 OSI安全机制

1.2.3 OSI安全服务的层配置

1.2.4 TCP / IP网络的安全体系结构

1.3 网络与信息安全的相关法规

1.3.1 国外网络与信息安全法规

1.3.2 我国网络与信息安全法规

1.4 计算机网络的安全评估

1.4.1 计算机网络安全评估的目的和意义

1.4.2 制定计算机网络安全评估标准的基本策略

1.4.3 安全标准的制定

1.4.4 计算机系统的安全等级

1.4.5 网络系统的安全评估方法

习题

第2章 信息加密技术基础

2.1 信息加密技术的发展

2.2 信息加密的基本原理

2.3 对称加密算法

2.3.1 基本原理

2.3.2 数据加密标准算法

2.3.3 其他对称加密算法

2.4 不对称加密算法

2.4.1 RSA算法

2.4.2 E1 - Gamal算法

2.5 信息摘要算法

2.5.1 MD5算法

2.5.2 其他MD算法

2.6 密码分析与密钥管理

2.6.1 密码分析与攻击

2.6.2 密钥管理与交换技术

2.7 信息加密技术在网络中的实现

2.7.1 链路加密

2.7.2 节点加密

2.7.3 端端加密

建议实验

习题

第3章 局域网安全技术及应用

3.1 局域网的安全问题

<<计算机网络安全技术>>

- 3.1.1 局域网安全特性
- 3.1.2 局域网安全问题分析
- 3.1.3 局域网的结构安全
- 3.2 局域网常用的安全技术
 - 3.2.1 局域网安全技术概述
 - 3.2.2 VLAN安全技术及应用
 - 3.2.3 VPN安全技术及应用
- 3.3 无线局域网的安全问题与安全技术
 - 3.3.1 无线局域网的安全问题
 - 3.3.2 无线局域网的安全技术
- 3.4 企业局域网的安全解决方案
 - 3.4.1 网络系统概况
 - 3.4.2 安全风险分析
 - 3.4.3 安全需求与安全目标
 - 3.4.4 网络安全方案的总体设计

建议实验

习题

第4章 操作系统安全技术

- 4.1 操作系统安全概述
 - 4.1.1 操作系统安全及其特点
 - 4.1.2 计算机操作系统的安全评估
- 4.2 自主访问控制与强制访问控制
 - 4.2.1 访问控制的基本概念
 - 4.2.2 自主访问控制
 - 4.2.3 强制访问控制
- 4.3 WindowsServer2003操作系统的安全技术
 - 4.3.1 WindowsServer2003的安全模型
 - 4.3.2 WindowsServer2003新增或加强的安全功能
 - 4.3.3 WindowsServer2003的安全策略与安全操作
- 4.4 Linux操作系统的安全技术
 - 4.4.1 UNIX / Linux系统的安全性
 - 4.4.2 Linux系统常用的安全技术
- 4.5 WindowsServer2003安全配置实践

建议实验

习题

第5章 网络防火墙技术及应用

- 5.1 网络防火墙概述
 - 5.1.1 网络防火墙的基本概念
 - 5.1.2 网络防火墙的目的与作用
- 5.2 网络防火墙的类型
 - 5.2.1 包过滤型防火墙
 - 5.2.2 代理服务器型防火墙
 - 5.2.3 其他类型的防火墙
- 5.3 网络防火墙的设计与实现
 - 5.3.1 防火墙设计的安全要求与准则
 - 5.3.2 防火墙的设计步骤
 - 5.3.3 防火墙的安全体系结构

<<计算机网络安全技术>>

5.4 防火墙的管理与维护

5.4.1 网络防火墙的日常管理与监控

5.4.2 网络防火墙的维护

5.4.3 防火墙使用的注意事项

5.5 典型的防火墙产品与技术发展趋势

5.5.1 防火墙相关标准

5.5.2 CheckPoint公司的FireWall防火墙

5.5.3 其他典型防火墙产品

5.5.3 防火墙技术的展望

建议实验

习题

第6章 数字签名与CA认证技术

6.1 数字签名

6.1.1 数字签名概述

6.1.2 数字签名的实现

6.2 数字证书

6.2.1 数字证书的基本概念

6.2.2 数字证书在电子邮件中的应用

6.3 CA认证及应用

6.3.1 CA认证的基本概念

6.3.2 CA认证产品及应用实例——招商银行网上个人银行

6.4 数字签名案例分析

6.4.1 使用Office2003的签名工具保护Office文档

6.4.2 使用AdobeAcrobat数字签名工具保护.PDF文档

建议实验

习题

第7章 Internet安全技术及应用

7.1 Internet安全概述

7.1.1 Internet安全隐患

7.1.2 TCP / IP的安全威胁

7.2 FTP安全

7.2.1 FTP概述

7.2.2 FTP协议的安全问题及防范措施

7.3 电子邮件安全

7.3.1 电子邮件概述

7.3.2 电子邮件服务协议

7.3.3 电子邮件的安全问题

7.3.4 电子邮件的安全技术

7.3.5 OutlookExpress安全电子邮件

7.3.6 PGF安全电子邮件

7.4 wcb安全

7.4.1 Web概述

7.4.2 Web客户端安全

7.4.3 Web服务器安全—— S6.O安全配置实例

7.5 代理技术及应用

7.5.1 代理的概念及用途

7.5.2 代理服务器简介

<<计算机网络安全技术>>

7.5.3 Windows代理实现：Internet共享实例

7.5.4 设置IE的代理服务器

建议实验

习题

第8章 计算机病毒与网络安全

8.1 计算机病毒概述

8.1.1 病毒的基本概念

8.1.2 病毒的分类及命名规则

8.2 蠕虫病毒

8.2.1 蠕虫病毒概述

8.2.2 蠕虫病毒的检测与防范

8.3 特洛伊木马

.....

第9章 网络黑客与入侵检测

第10章 常用网络安全软件及使用

参考文献

章节摘录

插图：4.设计代理服务器代理服务器接受外部网络节点提出的服务请求，如服务请求被接受、代理服务器再建立与实现服务器的连接。

由于它作用于应用层，故可利用各种安全技术，如身份验证、日志登录、审计跟踪、密码技术等来加强网络安全性，解决包过滤所不能解决的问题。

5.严格定义功能模块，分散实现防火墙由各种功能模块组成，如包过滤器、代理服务器、认证服务器、域名服务器、通信监控器等。

这些功能模块最好由路由器和单独的主机实现。

功能分散减少实现的难度，增加了系统的可靠程度。

6.防火墙维护和管理方案的考虑防火墙的日常维护是对访问记录进行审计，发现入侵和非法访问情况，据此对防火墙的安全性进行评价，需要时进行适当改进。

管理工作要根据网络拓扑结构的改变或安全策略的变化，对防火墙进行硬件和软件的修改和升级。

通过维护和管理进一步优化其性能，以保证网络及其信息的安全性。

5.3.3防火墙的安全体系结构网络防火墙的安全体系结构基本上分5种：过滤路由器结构、双宿主主机结构、主机过滤结构、子网过滤结构、吊带式结构等。

1.过滤路由器防火墙结构在传统的路由器中增加分组过滤功能就能形成这种最简单的防火墙。

这种防火墙的好处是完全透明的，但由于在单机上实现，会形成了网络中的“单失效点”。

由于路由器的基本功能是转发分组，一旦过滤机能失效，被入侵者就会形成网络直通状态，任何非法访问都可以进入内部网络。

因此，这种防火墙的失效模式不是“失效—安全”型，也违反了阻塞点原理。

因此，我们认为这种防火墙尚不能提供有效的安全功能，仅在早期的Internet中应用。

过滤路由器防火墙的基本结构如图5.1所示。

<<计算机网络安全技术>>

编辑推荐

《计算机网络安全技术》由科学出版社出版。

<<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>