第一图书网, tushu007.com

<<计算机网络安全教程>>

图书基本信息

书名：<<计算机网络安全教程>>

13位ISBN编号：9787302269625

10位ISBN编号：7302269629

出版时间：2012-1

出版时间：清华大学出版社

作者：石勇，卢浩，黄继军　编著

页数：338

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

内容概要

本书从网络安全的理论基础着手，同时兼顾实际工作中的应用，深入浅出地介绍了网络协议的基础知识、网络安全基础、计算机物理安全、操作系统安全基础、密码学基础、身份认证与访问控制、数据库安全、恶意软件概念及防范、Internet
安全协议、公钥基础设施——PKI、网络安全技术、无线网络安全技术、网络应用安全、数据备份、信息安全评测与风险评估和计算机网络安全管理等内容，书中通过大量实例、图文并茂的说明，使读者能在最短的时间内理解消化相关知识，并能学以致用，每章结尾均配有课后习题供读者练习巩固。
《计算机网络安全教程》的内容，逐步学习，并加以实践操作，即可掌握相关的技术内容。
《计算机网络安全教程》可作为高等学校计算机网络安全课程的教材，也可供广大网络管理员参考。

书籍目录

第1章 网络协议基础
1.1 网络发展概述
1.2 网络体系结构
1.2.1 OSI参考模型
1.2.2 TCP/IP参考模型
1.3 TCP/IP 协议基础
1.3.1 链路层协议
1.3.2 网络层协议
1.3.3 传输层协议
1.3.4 应用层协议
1.4 相关的基本概念
本章小结
课后练习
第2章 网络安全基础
2.1 网络安全概述
2.1.1 网络安全发展历程
2.1.2 网络安全的含义、要素
2.2 网络面临的安全威胁
2.2.1 非人为安全威胁
2.2.2 人为安全威胁
2.3 网络安全需求分析
2.3.1 网络物理安全需求
2.3.2 网络系统安全需求
2.3.3 网络应用安全需求
2.3.4 网络数据安全需求
2.3.5 网络安全管理
2.4 网络安全模型和体系结构
2.4.1 安全模型
2.4.2 安全体系结构
2.4.3 安全评估标准
本章小结
课后练习
第3章 计算机物理安全
3.1 环境安全
3.1.1 计算机设备的位置
3.1.2 自然灾害的防备
3.1.3 选址与建筑材料
3.2 机房安全及等级
3.2.1 适用范围
3.2.2 相关术语
3.2.3 计算机机房的安全分类
3.2.4 场地的选择
3.2.5 结构防火
3.2.6 计算机机房内部装修
3.2.7 计算机机房专用设备

3.2.8 火灾报警及消防设施
3.2.9 其他防护和安全管理
3.3 设备安全
3.3.1 计算机硬件物理安全
3.3.2 磁介质安全
3.3.3 信息的加密和解密
3.3.4 硬盘锁
3.3.5 电磁辐射泄漏
3.3.6 IC卡安全
3.4 突发应急计划
本章小结
课后练习
第4章 操作系统安全基础
4.1 Windows操作系统
4.1.1 Windows操作系统简介
4.1.2 Windows操作系统安全体系结构
4.1.3 Windows操作系统的基本安全设置
4.2 Windows NT/2000安全
4.2.1 Windows NT/2000文件系统
4.2.2 Windows NT安全漏洞及解决方案
4.2.3 Windows 2000分布式安全协议
4.3 UNIX系统安全基础
4.3.1 UNIX操作系统安全基础
4.3.2 UNIX操作系统登录过程
4.4 Linux操作系统
4.4.1 Linux操作系统简介
4.4.2 Linux网络安全
4.5 操作系统漏洞
4.5.1 操作系统脆弱性等级
4.5.2 操作系统漏洞
本章小结
课后练习
第5章 密码学基础
5.1 概述
5.1.1 密码学的历史
5.1.2 密码学的定义
5.2 密码学的基本概念
5.2.1 基本概念
5.2.2 密码系统的安全性
5.2.3 密码体制分类
5.2.4 对密码系统的攻击
5.3 古典密码学
5.3.1 凯撒密码

5.3.2 仿射密码
5.3.3 维吉尼亚密码
5.3.4 Playfair密码
5.3.5 Hill密码
5.4 对称密码算法
5.4.1 对称密码算法概述
5.4.2 DES算法
5.4.3 AES算法
5.4.4 分组密码工作模式
5.4.5 Java中的对称密码算法编程实例
5.5 非对称密码算法
5.5.1 非对称密码算法概述
5.5.2 RSA算法
5.5.3 Java中的非对称密码算法编程实例
5.6 数字签名
5.6.1 数字签名概述
5.6.2 基于RSA算法的数字签名
5.6.3 Java中的数字签名算法编程实例
5.7 PGP原理与应用
5.7.1 操作描述
5.7.2 加密密钥和密钥环
5.7.3 公开密钥管理
本章小结
课后练习
第6章 身份认证与访问控制
6.1 身份认证
6.1.1 身份认证概述
6.1.2 常用的身份认证技术
6.1.3 常用的身份认证机制
6.2 访问控制
6.2.1 访问控制概述
6.2.2 访问控制的基本要素
6.3 访问控制类型
6.3.1 自主型访问控制（DAC）
6.3.2 强制型访问控制（MAC）
6.3.3 基于角色的访问控制（RBAC）
6.4 访问控制机制
6.4.1 访问控制列表
6.4.2 能力机制
6.4.3 安全标签机制
本章小结
课后练习
第7章 数据库安全
7.1 数据库安全概述
7.1.1 数据库简介
7.1.2 数据库的安全特性
7.2 数据库安全威胁

7.3 数据库中的数据保护
7.3.1 数据库中的访问控制
7.3.2 数据库加密
7.3.3 数据库的完整性保护
7.4 备份与恢复数据库
7.4.1 数据库备份
7.4.2 数据库恢复
7.5 SQL Server数据库安全机制
7.5.1 SQL Server安全体系结构
7.5.2 SQL Server身份认证
7.5.3 SQL Server访问控制
7.5.4 SQL Server访问审计
本章小结
课后练习
第8章 恶意软件概念及防范
8.1 恶意软件的概念
8.2 恶意软件分类
8.2.1 获取目标系统远程控制权类（第一类）
8.2.2 维持远程控制权类（第二类）
8.2.3 完成特定业务逻辑类（第三类）
8.3 恶意软件的运行症状
8.4 恶意软件的防范
本章小结
课后练习
第9章 Internet安全协议
9.1 安全协议概述
9.2 IPSec协议
9.2.1 IPSec概述
9.2.2 IPSec安全体系结构
9.2.3 认证头协议
9.2.4 安全负载封装协议
9.2.5 因特网密钥交换协议
9.3 TLS
9.3.1 TLS概述
9.3.2 TLS工作原理
9.3.3 TLS的安全服务
9.3.4 TLS的特点与不足
9.4 Kerberos协议
9.4.1 Kerberos概述
9.4.2 Kerberos工作原理
9.4.3 Kerberos的安全服务
9.4.4 Kerberos的特点与不足
9.5 SET协议
9.5.1 SET概述
9.5.2 SET工作过程
9.5.3 SET的安全功能
9.5.4 SET与TLS协议的比较

本章小结
课后练习
第10章 公钥基础设施——PKI
10.1 PKI概述
10.1.1 理论基础
10.1.2 PKI使用的密码技术
10.1.3 PKI提供的安全服务
10.2 数字证书
10.2.1 数字证书的定义
10.2.2 数字证书的格式
10.2.3 数字证书的生命周期
10.2.4 使用Java工具生成数字证书
10.3 PKI的组成
10.3.1 概述
10.3.2 PKI认证机构
10.3.3 其他组成部分
10.4 PKI功能
10.4.1 证书管理
10.4.2 密钥管理
10.4.3 认证
10.4.4 安全服务功能
10.5 信任模型
10.5.1 层次结构模型
10.5.2 分布式网状结构模型
10.5.3 Web模型
10.6 相关的标准
10.6.1 X.509标准
10.6.2 PKIX标准
10.6.3 PKCS标准
10.6.4 X.500标准
10.6.5 LDAP标准
本章小结
课后练习
第11章 网络安全技术
11.1 网络数据加密技术
11.1.1 链路加密
11.1.2 端到端加密
11.2 防火墙
11.2.1 防火墙概述
11.2.2 防火墙的功能及其局限性
11.2.3 防火墙的分类
11.3 入侵检测系统
11.3.1 入侵检测系统概述
11.3.2 入侵检测系统模型及框架
11.3.3 入侵检测系统分类
11.3.4 入侵检测系统部署
11.4 VPN

11.4.1 VPN概述
11.4.2 VPN类型
11.4.3 VPN工作原理
11.4.4 VPN主要技术
本章小结
课后练习
第12章 无线网络安全技术
12.1 无线网络安全概述
12.1.1 无线网络基础知识
12.1.2 无线网络技术
12.2 无线网络安全性分析
12.2.1 移动通信网络安全性分析
12.2.2 Wi-Fi无线局域网安全性分析
12.3 无线网络安全防护
12.3.1 移动通信网络安全防护
12.3.2 Wi-Fi无线局域网安全防护
本章小结
课后练习
第13章 网络应用安全
13.1 网络攻击的步骤
13.1.1 搜集初始信息
13.1.2 确定攻击目标的IP地址范围
13.1.3 扫描存活主机、开放的端口
13.1.4 分析目标系统
13.2 口令安全
13.2.1 口令破解
13.2.2 设置安全的口令
13.3 网络监听
13.3.1 网络监听原理
13.3.2 网络监听实践
13.3.3 网络监听防范
13.4 网络扫描
13.4.1 网络主机扫描
13.4.2 主机端口扫描
13.5 IP欺骗攻击
13.5.1 IP欺骗攻击原理
13.5.2 IP欺骗攻击防范
13.6 网络钓鱼攻击
13.6.1 网络钓鱼攻击原理
13.6.2 网络钓鱼攻击防范
13.7 Web安全
13.7.1 Web安全威胁
13.7.2 Web安全防范基础
本章小结
课后练习
第14章 数据备份
14.1 数据备份概述

14.1.1 数据完整性概念
14.1.2 保护数据完整性的方法
14.1.3 数据备份系统的组成
14.1.4 数据备份分类
14.1.5 数据存储介质
14.2 数据存储技术
14.2.1 DAS
14.2.2 NAS
14.2.3 SAN
14.3 远程数据备份
14.3.1 同步数据复制
14.3.2 异步数据复制
14.4 个人数据备份
14.4.1 Windows自带的备份功能
14.4.2 Symantec Ghost备份功能
本章小结
课后练习
第15章 信息安全评测与风险评估
15.1 概述
15.2 信息安全风险评估
15.2.1 评估概述
15.2.2 评估步骤
15.2.3 评估分类
15.3 信息安全风险评估标准
15.3.1 评估前的决策
15.3.2 TCSEC
15.3.3 欧洲的安全评价标准（ITSEC）
15.3.4 加拿大的评价标准（CTCPEC）
15.3.5 美国联邦准则（FC）
15.3.6 国际通用标准（CC）
15.3.7 中国的安全标准
本章小结
课后练习
第16章 计算机网络安全管理
16.1 计算机网络安全管理概述
16.1.1 网络安全管理的重要性
16.1.2 网络安全管理的内容
16.1.3 网络安全管理的原则
16.2 安全管理标准
16.2.1 ISO 2700
16.2.2 ISO 2700
16.2.3 ISO 2700
16.3 安全立法
16.3.1 国际安全法律法规
16.3.2 国内安全法律法规
本章小结
课后练习

章节摘录

版权页：插图：TCP／TP体系的传输层提供了两类服务：可靠传输服务（TCP协议）及不可靠传输服务（UDP协议）。
TCP是面向连接的服务，用TCP通信，首先必须建立连接，并且在传输过程中，协议机制能保障数据按发送顺序可靠到达目的地。
TCP协议适合传输对可靠性要求高、连续的大量数据。
TCP连接的建立、释放过程都需要一定的开销，如果频繁建立、释放连接，会导致传输效率显著降低。
UDP是无连接服务，通信前无须建立连接，任何时候只需直接将数据发出即可。
UDP灵活、方便，不存在连接管理问题，适合传输间断、小块数据。
UDP提供的是一种不可靠的传输服务，如传输中数据出现丢失、乱序的问题，UDP都不会做处理。
TCP、UDP分别适应不同的应用场合，当需要传输连续、数据量很大、对可靠性要求高的数据时，应采用TCP协议，而在需要传输大量离散数据，且对可靠性要求不太高时，则适合用UDP协议。
基于网络层编址、寻址（即路由）功能，数据能从一台主机到达网络中任意其他主机，单数据到达目的主机后，由目的主机的哪个应用程序来处理，则不是网络层协议所能解决的，也就是说，网络层实现的是主机端到端的传输能力。
网络数据的发送、接收，最终都必须由特定的应用程序来完成，因此，必须引用新的机制，来实现网络数据与应用程序的关联，这就是传输层的端口（Port）所要做的，所以说，传输层提供的是应用程序端到端的传输能力。
端口，是一个16比特的数字，故端口号的最小值为0，最大值为65535。
其中，0～1023称为熟知端口（Well-KnownPort），熟知端口通常用于关联常用的网络服务。
例如，80端口常用于关联Web服务，以提供网页浏览服务；53端口常用于关联DNS服务，以提供域名解析服务。
需要注意的是，因为TCP/IP的网络层提供了两套服务-TCP和UDP，因此对应就有两套端口机制。
也就是说，TCP有一套端口，从0到65535，同样UDP也有一套端口，从0到65535。
在一些需要严密表述的场合，仅指出端口号是不够的，还应当指明是TCP端口还是UDP端口。
前文所述Web服务的80端口，是指TCP的80端口，而DNS服务的53端口，通常是指UDP的53端口。

编辑推荐

《计算机网络安全教程》：网络协议及网络安全基础、计算机物理安全、操作系统安全、密码学基础、身份认证与访问控制、数据库安全、恶意软件概念及防范、Internet安全协议、公钥基础设施-PKI、网络安全技术、无线网络安全技术、数据备份、信息安全评测与风险评估、计算机网络安全管理。
《计算机网络安全教程》从网络安全的理论基础着手，同时兼顾实际工作中的应用，深入浅出地介绍了计算机网络安全的方方面面，内容包括网络安全相关基础知识、密码学基础、身份认证与访问控制、数据库安全、恶意软件防范、Internet安全、无线网络安全技术、数据备份、网络安全管理等。
《计算机网络安全教程》可以作为高等学校计算机专业相关教材，也可作为广大网络管理员的参考书。
融合作者多年的教学和科研经验，理论与实践相结合，便于课堂讲授。
实例丰富，图文并茂，能够使读者深刻掌握相应知识，并学以致用。
明确的重点内容和丰富的课后习题，使学习有的放矢，学习效果得以强化。
提供实验软件和PPT等教学资料，便于教学和自学。

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