

<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787115124982

10位ISBN编号：7115124981

出版时间：2004-9

出版时间：人民邮电出版社

作者：邓亚平

页数：376

字数：588000

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>>

内容概要

本书详细地介绍计算机网络安全的基础理论、原理及其实现方法。

主要内容包括网络安全概论、数据加密、计算机病毒的防治、操作系统的安全、数据库系统的安全、黑客入侵技术、网站的安全、网络协议的安全、防火墙技术、入侵检测技术、安全评估和安全法规等。

本书可作为高等院校本科计算机专业、通信工程专业和信息安全专业等相关专业的教材，也可作为计算机网络安全或信息安全课程的研究生教材，还可作为网络工程技术人员、网络管理员和信息安全管理的技术参考书。

<<计算机网络安全>>

书籍目录

- 第1章 网络安全概论 11.1 网络安全面临的威胁 11.1.1 物理安全威胁 11.1.2 操作系统的安全缺陷 31.1.3 网络协议的安全缺陷 61.1.4 应用软件的实现缺陷 131.1.5 用户使用的缺陷 151.1.6 恶意代码 171.2 网络安全体系结构 201.2.1 网络安全总体框架 201.2.2 安全控制 211.2.3 安全服务 211.2.4 安全需求 251.3 PDRR网络安全模型 261.3.1 防护 271.3.2 检测 311.3.3 响应 321.3.4 恢复 321.4 网络安全基本原则 331.4.1 普遍参与 331.4.2 纵深防御 331.4.3 防御多样化 341.4.4 阻塞点 351.4.5 最薄弱链接 351.4.6 失效保护状态 361.4.7 最小特权 371.4.8 简单化 381.5 本章小结 38习题 38
- 第2章 数据加密 402.1 数据加密概述 402.1.1 保密通信模型 412.1.2 经典加密方法 422.1.3 现代密码体制 462.2 对称密码体制 472.2.1 美国数据加密标准(DES) 472.2.2 国际数据加密算法(IDEA) 522.2.3 高级加密标准(AES) 552.3 非对称密码体制 602.3.1 非对称密码体制的原理 602.3.2 RSA算法 622.3.3 LUC算法 642.3.4 椭圆曲线算法 672.4 密钥的管理 712.4.1 密钥的管理 712.4.2 密钥的分配 732.4.3 公钥的全局管理体制(PKI) 792.5 散列函数与数字签名 812.5.1 散列函数 812.5.2 报文摘要 822.5.3 安全散列函数(SHA) 832.5.4 数字签名算法(DSA) 862.6 本章小结 87习题 89
- 第3章 计算机病毒及防治 903.1 计算机病毒概述 903.1.1 计算机病毒的概念和发展史 903.1.2 计算机病毒的特征 933.1.3 计算机病毒的种类 943.2 计算机病毒的工作机理 963.2.1 引导型病毒 973.2.2 文件型病毒 983.2.3 混合型病毒 993.2.4 宏病毒 1003.2.5 网络病毒 1013.3 计算机病毒实例 1033.3.1 CIH病毒 1033.3.2 红色代码病毒 1043.3.3 冲击波病毒 1053.4 计算机病毒的检测和清除 1063.4.1 计算机病毒的检测 1063.4.2 计算机病毒的消除 1093.5 本章小结 110习题 111
- 第4章 操作系统的安全 1124.1 操作系统安全性概述 1124.1.1 操作系统安全的重要性 1124.1.2 操作系统的安全服务 1144.1.3 操作系统安全性的设计原则与一般结构 1174.1.4 安全操作系统的发展状况 1184.2 Windows NT/2000的安全 1214.2.1 Windows NT/2000的安全模型 1214.2.2 Windows NT/2000的登录控制 1234.2.3 Windows NT/2000的访问控制 1254.2.4 Windows NT/2000的安全管理 1274.3 UNIX/Linux的安全 1314.3.1 UNIX用户账号与口令安全 1314.3.2 UNIX的文件访问控制 1344.3.3 UNIX安全的管理策略 1364.3.4 UNIX网络服务的安全管理 1384.3.5 UNIX的安全审计 1404.4 本章小结 141习题 142
- 第5章 数据库系统的安全 1435.1 数据库安全概述 1435.1.1 简介 1435.1.2 数据库系统的特性 1445.1.3 数据库系统的安全性要求 1445.1.4 数据库系统安全的含义 1465.1.5 数据库系统的安全架构 1465.1.6 数据库安全系统特性 1475.1.7 多层数据库系统的安全 1485.2 数据库安全的威胁 1495.2.1 数据篡改 1495.2.2 数据损坏 1505.2.3 数据窃取 1505.3 数据库的数据保护 1515.3.1 数据库的故障类型 1515.3.2 数据库的数据保护 1535.4 数据库的备份和恢复 1595.4.1 数据库的备份 1595.4.2 系统和网络完整性 1605.4.3 数据库的恢复 1615.5 本章小结 163习题 163
- 第6章 黑客入侵技术 1646.1 端口扫描 1646.1.1 端口扫描简介 1646.1.2 端口扫描的原理 1656.1.3 端口扫描的工具 1666.2 网络监听 1696.2.1 网络监听的原理 1696.2.2 网络监听的检测 1726.3 IP电子欺骗 1746.3.1 关于盗用IP地址 1746.3.2 IP电子欺骗的原理 1756.3.3 IP电子欺骗的实施 1766.3.4 IP电子欺骗的防范 1786.4 拒绝服务攻击 1796.4.1 概述 1796.4.2 拒绝服务攻击的原理 1806.4.3 分布式拒绝服务攻击及其防范 1846.5 特洛伊木马 1876.5.1 特洛伊木马程序简介 1876.5.2 特洛伊木马程序的位置和危险级别 1896.5.3 特洛伊木马的类型 1896.5.4 特洛伊木马的检测 1906.5.5 特洛伊木马的防范 1926.6 E-mail炸弹 1956.6.1 E-mail炸弹的原理 1956.6.2 邮件炸弹的防范 1966.7 缓冲区溢出 1986.7.1 缓冲区溢出简介 1986.7.2 制造缓冲区溢出 1996.7.3 通过缓冲区溢出获得用户shell 2006.7.4 利用缓冲区溢出进行的攻击 2026.7.5 缓冲区溢出攻击的防范 2046.8 本章小结 205习题 205
- 第7章 网站的安全 2067.1 口令安全 2067.1.1 口令破解过程 2067.1.2 安全口令的设置 2127.2 Web站点的安全 2137.2.1 构建Web站点的安全特性 2157.2.2 检测和排除安全漏洞 2187.2.3 监控Web站点的信息流 2257.3 DNS的安全 2277.3.1 DNS的安全问题 2277.3.2 增强的DNS 2327.3.3 安全DNS信息的动态更新 2347.4 本章小结 237习题 237
- 第8章 网络协议的安全 2388.1 IP的安全 2388.1.1 IPSec协议簇 2388.1.2 AH协议 2478.1.3 ESP协议 2508.1.4 IKE

<<计算机网络安全>>

协议 2528.2 传输协议的安全 2558.2.1 SSL协议 2568.2.2 TLS协议 2648.3 应用协议的安全
2718.3.1 FTP的安全 2728.3.2 Telnet的安全 2758.3.3 S-HTTP 2788.3.4 电子商务的安全协议
2798.4 本章小结 282习题 282第9章 防火墙技术 2849.1 防火墙概述 2849.1.1 防火墙的基本
概念 2849.1.2 防火墙的作用与不足 2849.2 防火墙的设计策略和安全策略 2879.2.1 防火墙的
设计策略 2879.2.2 防火墙的安全策略 2889.3 防火墙的体系结构 2929.3.1 包过滤型防火墙
2929.3.2 多宿主主机(多宿主网关)防火墙 2949.3.3 屏蔽主机型防火墙 2969.3.4 屏蔽子网型防
火墙 2979.3.5 堡垒主机 3009.4 防火墙的主要技术 3019.4.1 数据包过滤技术 3029.4.2 代理技
术 3089.4.3 状态检查技术 3119.4.4 地址翻译技术 3149.4.5 内容检查技术 3179.4.6 VPN技术
3179.4.7 其他防火墙技术 3239.5 本章小结 325习题 325第10章 入侵检测技术 32610.1 入
侵检测概述 32610.1.1 网络安全的目标 32610.1.2 研究入侵检测的必要性 32710.1.3 网络安全体
系结构 32910.2 入侵检测原理 33010.2.1 异常入侵检测原理 33010.2.2 误用入侵检测原理
33110.2.3 入侵检测模型 33210.3 入侵检测系统的关键技术 33910.3.1 多用于异常入侵检测的
技术 33910.3.2 多用于误用入侵检测的技术 34710.3.3 基于Agent的入侵检测 34810.3.4 入侵检
测的新技术 35310.3.5 入侵检测系统面临的挑战和发展前景 35610.4 基于数据挖掘的智能化入侵
检测系统设计 35710.4.1 入侵检测系统体系结构以及模型 35810.4.2 数据预处理 35810.4.3 基于
协议分析的检测方法 35910.4.4 数据挖掘规则生成模块 36010.5 本章小结 362习题 362第11章
网络安全评估和安全法规 36311.1 安全评估的国际通用准则 36311.1.1 可信计算机系统安全评
估准则 36311.1.2 信息系统技术安全评估通用准则 36511.2 安全评估的国内通用准则 36611.2.1
信息系统安全划分准则 36611.2.2 信息系统安全有关的标准 36911.3 网络安全的法律和法规
36911.3.1 网络安全相关的法规 36911.3.2 网络安全相关的法律 37011.3.3 网络安全管理的有关
法律 37011.3.4 电子公告服务的法律管制 37311.4 本章小结 374习题 374参考文献 375

<<计算机网络安全>>

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>