

<<网络与系统防御技术>>

图书基本信息

书名：<<网络与系统防御技术>>

13位ISBN编号：9787811142235

10位ISBN编号：7811142236

出版时间：2007-8

出版时间：电子科技大学出版社

作者：周世杰, 陈伟, 钟婷 著

页数：257

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>

<<网络与系统防御技术>>

内容概要

本书为普通高等学校信息安全“十一五”规划教材之一，内容丰富新颖，涵盖当前网络与系统防御领域内各主要技术。

涉及的主要网络与系统防御技术有：网络与系统防御基础理论、网络安全基础、网络隔离技术、网络安全技术、协议安全技术、操作系统与主机安全技术等。

本书可作为高等院校信息安全专业本科生和研究生的教材，也可作为相关领域专业技术人员的参考用书。

<<网络与系统防御技术>>

书籍目录

第1章信息安全概述 1.1 信息及信息安全 1.1.1 信息 1.1.2 信息技术 1.1.3 信息安全 1.2 信息安全体系 1.2.1 安全服务 1.2.2 安全机制 1.2.3 安全服务与安全机制的关系 1.3 安全服务的分层部署与实现 1.4 信息安全技术 1.5 网络安全威胁 1.6 小结第2章 信息安全中的数学基础 2.1 概率论基础 2.1.1 概率论基础 2.1.2 随机变量及其概率分布 2.1.3 概率论中的几个定理 2.1.4 信息安全中的概率论方法 2.2 信息论基础 2.2.1 自信息量 2.2.2 熵 2.2.3 条件熵与通信中的信息论 2.2.4 信息安全中的信息论 2.3 计算复杂性理论与计算模型基础 2.3.1 计算复杂性基础 2.3.2 计算复杂性在信息安全中的应用 2.4 初等数论基础 2.4.1 数的整除性 2.4.2 算术基本定理 2.4.3 同余与同余方程 2.4.4 欧拉定理与费尔马定理 2.4.5 中国剩余定理 2.4.6 有限域 2.4.7 欧几里得算法 2.4.8 指数模运算 2.4.9 小结第3章 密码学基础 3.1 密码学的理论基础 3.1.1 密码学的基本概念 3.1.2 密码分析与密码算法的安全性 3.1.3 对称算法和公开密钥算法的概念 3.2 古典密码技术 3.2.1 替换密码 3.2.2 置换密码 3.3 对称密码技术 3.3.1 DES算法 3.3.2 AES算法 3.3.3 其他对称加密算法 3.4 公开密码技术 3.4.1 公开密钥算法的基本思想 3.4.2 RSA算法 3.4.3 Ecc算法 3.4.4 其他公钥算法 3.5 序列密码技术 3.5.1 序列密码的基本概念 3.5.2 常见序列密码算法简介第4章 网络基础 4.1 概述 4.1.1 计算机网络的演变 4.1.2 计算机网络的概念 4.1.3 计算机网络协议 4.1.4 计算机网络分类 4.1.5 计算机网络的组成与结构 4.1.6 常见计算机网络拓扑结构 4.2 TCP/IP协议基础 4.2.1 TCP/IP协议模型 4.2.2 TCP/IP协议栈 4.2.3 TCP/IP协议数据封装 4.3 IP层协议 4.3.1 IP协议概述 4.3.2 IP协议规范 4.4 传输层协议 4.4.1 TCP协议 4.4.2 UDP协议 4.5 小结第5章 网络隔离技术 5.1 交换机与网络隔离 5.1.1 交换机与子网隔离 5.1.2 虚拟子网隔离 5.2 路由器与网络隔离 5.2.1 路由器作为唯一安全组件 5.2.2 路由器作为安全组件的一部分 5.3 防火墙与网络隔离 5.3.1 防火墙中的关键技术 5.3.2 防火墙的典型体系结构 5.3.3 防火墙在网络边界安全中的作用 5.4 网络地址转换 5.4.1 网络地址转换基本概念 5.4.2 网络地址转换与网络安全第6章 网络安全技术 6.1 安全检测技术 6.1.1 入侵检测技术 6.1.2 漏洞检测技术 6.1.3 扫描技术 6.2 安全保护技术 6.2.1 安全保护目的 6.2.2 安全保护方法及关键技术 6.3 安全响应技术 6.3.1 安全响应意义 6.3.2 安全响应的阶段 6.3.3 常见安全响应方法 6.4 安全恢复技术 6.4.1 灾难恢复的概念 6.4.2 灾难恢复定义及意义 6.4.3 容灾系统分类 6.4.4 容灾关键技术第7章 协议安全技术 7.1 协议安全基础 7.1.1 安全协议的概念 7.1.2 安全协议的分类 7.1.3 安全协议缺陷与安全协议模型 7.1.4 安全协议设计的基本原则 7.1.5 TCP/IP协议与安全协议 7.2 认证协议 7.2.1 用户口令认证协议 7.2.2 挑战-握手认证协议 7.2.3 Kerberos认证协议 7.2.4 X.509认证协议 7.2.5 小结 7.3 安全协议实例：传输层安全协议(TLS) 7.3.1 SSL和TLS协议概述 7.3.2 TLS协议框架 7.3.3 TLS加密规范修改协议： 7.3.4 TLS报警协议 7.3.5 TLS记录层协议 7.3.6 TLS握手协议 7.3.7 小结第8章 计算机安全 8.1 计算机系统安全基础 8.1.1 计算机系统的层次结构 8.1.2 硬件安全保护技术 8.1.3 操作系统安全与引用监视器 8.1.4 操作系统安全性的评估方法 8.2 计算机系统的物理安全 8.2.1 设备防盗 8.2.2 设备防毁 8.2.3 防电磁泄漏 8.2.4 防止线路窃听 8.2.5 抗电磁干扰 8.2.6 电源保护 8.3 计算机系统的可靠性 8.3.1 硬件冗余 8.3.2 软件冗余 8.3.3 数据冗余 8.3.4 时间冗余 8.4 操作系统安全 8.4.1 UNIX操作系统安全 8.4.2 Windows操作系统安全 8.5 操作系统加固技术 8.5.1 防止本地攻击的安全加固 8.5.2 抵御网络攻击的安全加固 8.5.3 抵御应用程序攻击的安全加固 8.6 软件安全技术 8.6.1 软件安全问题的严重性 8.6.2 安全编码基本原则参考文献

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>