<<网络安全与管理>>

图书基本信息

书名：<<网络安全与管理>>

13位ISBN编号：9787121015717

10位ISBN编号：7121015714

出版时间：2005-8

出版时间：电子工业出版社

作者：林涛

页数：272

字数：454000

<<网络安全与管理>>

内容概要

本书是一本从实战出发，以应用为目的，防范手段为重点，理论讲述为基础的系统性、实战性、应用性较强的网络安全课程实用教材。
教材摒弃了传统网络安全教材理论过多、实用性不强的问题，是一本紧密跟踪网络安全领域最新问题和技术运用的教材。
教材从应用的角度，系统讲述了网络安全所涉及的理论及技术。
以阶段能力培养为目的，每个能力阶段为一个章节，开始为问题的背景介绍，然后讲述处理手段和方法，最后系统讲述涉及的理论问题。
在每章的最后设计了实训内容，规划了任务，通过实战演练使读者能够综合运用书中所讲授的技术进行网络信息安全方面的实践。
本书力求避免抽象的理论介绍，而是通过案例讲解相关的技术和知识。
本书可作为高等职业院校计算机应用与软件技术专业的教材，也可作为自学和急需了解计算机网络安全相关技术和知识的技术人员的参考书，中等技校也可以参考部分内容教学。

<<网络安全与管理>>

书籍目录

第1章 网络安全概述 1.1 引言 1.1.1 从用户角度看网络安全领域 1.1.2 从技术角度看网络安全领域 1.1.3 从产业角度看网络安全领域 1.2 网络安全面临的威胁 1.2.1 物理安全威胁 1.2.2 操作系统的安全缺陷 1.2.3 网络协议的安全缺陷 1.2.4 应用软件的实现缺陷 1.2.5 用户使用的缺陷 1.2.6 恶意代码 1.3 网络安全体系结构 1.3.1 网络安全总体框架 1.3.2 安全控制 1.3.3 安全服务 1.3.4 安全需求 1.4 网络安全模型 1.4.1 防护 1.4.2 检测 1.4.3 响应 1.4.4 恢复 1.5 网络安全防范体系及设计原则 习题1第2章 密码学基础 2.1 密码学的发展历史 2.2 古老的密码技术 2.2.1 加密与破译 2.2.2 恺撒大帝的秘密——替代之恺撒码 2.3 对称密码算法 2.4 DES算法 2.4.1 DES的算法框架 2.4.2 DES的算法描述 2.4.3 DES算法的应用误区 2.5 非对称密码算法 2.6 RSA算法 2.7 Hash算法 实训1 数据加密算法的应用 习题2第3章 Windows网络操作系统的安全 3.1 WINDOWS网络操作系统的安全性概述 3.1.1 Windows 2000的安全特性 3.1.2 Windows 2000的安全结构 3.1.3 Windows 2000的网络模式 3.1.4 Windows 2000安全管理工具 3.2 ACTIVE DIRECTORY的结构与功能 3.2.1 Active Directory的功能和特点 3.2.2 Active Directory组件 3.2.3 Active Directory的操作 3.3 ACTIVE DIRECTORY组策略 3.3.1 组策略简介 3.3.2 组策略的创建 3.3.3 管理组策略 3.3.4 应用组策略 3.4 用户和工作组的安全管理 3.4.1 Windows 2000的用户账户 3.4.2 用户账户安全设置 3.4.3 组管理 3.4.4 用户和组的验证、授权和审核 3.5 审核机制 3.5.1 Windows 2000审核概述 3.5.2 审核管理 3.5.3 使用审核的最佳操作 实训2 设计一个域和组织单元（OU）结构 习题3第4章 对WINDOWS网络操作系统的攻击与防护 4.1 WINDOWS网络漏洞分析 4.1.1 本地输入法漏洞 4.1.2 Telnet漏洞 4.1.3 NetBIOS的信息泄露 4.1.4 IIS服务漏洞 4.1.5 命名管道漏洞 4.1.6 ICMP漏洞 4.1.7 MIME邮件头漏洞 4.2 常见WINDOWS攻击手法及防范 4.2.1 口令攻击 4.2.2 特洛伊木马攻击 4.2.3 网络监听 4.2.4 拒绝服务攻击 4.2.5 电子邮件攻击 4.2.6 缓存区溢出攻击 4.3 WINDOWS 2000入侵检测技术 4.3.1 基于Web服务端口的入侵检测 4.3.2 基于安全日志的检测 4.3.3 文件访问日志与关键文件保护 4.3.4 进程监控 4.3.5 注册表校验 4.3.6 端口监控 4.3.7 终端服务的日志监控 4.3.8 陷阱技术 实训3 WINDOWS网络操作系统下的攻击防御实训 习题4第5章 LINUX网络操作系统的安全 5.1 LINUX简介 5.2 LINUX安全问题概述 5.3 LINUX系统的安全机制 5.3.1 C1/C2安全级设计框架 5.3.2 用户账号与口令安全 5.3.3 文件系统与访问控制 5.3.4 Linux的安全审计 5.3.5 网络监听与入侵检测 5.4 LINUX系统安全防范 5.4.1 系统漏洞扫描 5.4.2 查找后门与系统恢复 5.4.3 系统安全加固 实训4 利用密码猜测程序检测系统中的薄弱密码 习题5第6章 电子商务的安全 6.1 电子商务安全概论 6.1.1 电子商务安全服务 6.1.2 电子商务安全技术 6.2 公共密钥基础设施PKI 6.2.1 PKI的核心服务 6.2.2 PKI实体的组成 6.2.3 PKI的应用 6.3 安全的电子支付 6.3.1 电子支付概述 6.3.2 基于信用卡的电子支付方案 6.3.3 基于支票的电子支付方案 6.3.4 基于现金的电子支付方案 6.3.5 电子支付与电子钱包 6.4 电子商务安全实施细节 6.4.1 客户端安全性 6.4.2 服务器端安全性 6.4.3 应用程序的安全性 6.4.4 数据库服务器的安全性 6.4.5 电子商务站点实例 实训5 电子商务安全技术调研 习题6第7章 网络攻击与防护 7.1 关于黑客 7.2 黑客（HACKER）文化 7.3 IP欺骗 7.3.1 IP欺骗原理 7.3.2 一个源程序 7.4 端口扫描 7.4.1 端口扫描简介 7.4.2 端口扫描的原理 7.4.3 端口扫描的工具 7.5 网络监听 7.5.1 网络监听的原理 7.5.2 网络监听的检测 7.6 拒绝服务攻击 7.6.1 概述 7.6.2 拒绝服务攻击的原理 7.6.3 分布式拒绝服务攻击及其防范 7.7 特洛伊木马 7.7.1 特洛伊木马程序的位置和危险级别 7.7.2 特洛伊木马的类型 7.7.3 特洛伊木马的检测 7.7.4 特洛伊木马的防范 实训6 攻击防御实训 习题7第8章 防火墙技术 8.1 防火墙的基本知识 8.1.1 防火墙的概念及作用 8.1.2 防火墙的架构与工作方式 8.1.3 防火墙的体系结构 8.1.4 防火墙的基本类型 8.1.5 防火墙的发展史 8.2 防火墙的工作原理 8.2.1 什么是防火墙 8.2.2 服务器TCP/UDP端口过滤 8.2.3 TCP/UDP端口 8.2.4 双向过滤 8.2.5 检查ACK位 8.2.6 FTP带来的困难 8.2.7 UDP端口过滤 8.3 深入了解防火墙 8.4 一种典型防火墙产品 实训7 防火墙配置 习题8第9章 网络安全解决方案 9.1 政府机构网络安全解决方案 9.1.1 前言 9.1.2 政府网络安全隐患 9.1.3 解决方案 9.2 金融系统网络安全解决方案 9.2.1 前言 9.2.2 网络系统分析 9.2.3 网络安全风险分析 9.2.4 网络安全需求及安全目标 9.2.5 网络安全实现策略及产品选型原则 9.2.6 网络安全方案设计原则 9.2.7 网络安全体系结构 9.3 电子商务网络安全解决方案 9.3.1 前言 9.3.2 网络系统分析 9.3.3 网络安全风险分析

9.3.4 网络安全需求及安全目标 9.3.5 网络安全实现策略及产品选型原则 9.3.6 网络安全方案设计原则 9.4 网络防病毒解决方案 实训8 网络安全方案 习题9参考文献

<<网络安全与管理>>

版权说明