

<<计算机安全技术>>

图书基本信息

书名：<<计算机安全技术>>

13位ISBN编号：9787564300982

10位ISBN编号：7564300981

出版时间：2008-10

出版时间：侯迎春 西南交通大学出版社 (2008-10出版)

作者：侯迎春

页数：227

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>

<<计算机安全技术>>

内容概要

《计算机安全技术》首先介绍了计算机安全的基础知识、计算机软件安全、计算机病毒，接着用了大量的篇幅介绍网络安全的相关内容，其中涉及访问控制与防火墙技术、加密与认证、网络监听与端口扫描、网络攻防、入侵检测、安全审计与系统恢复、Windows XP的安全、数据库安全等。

计算机安全主要包括操作系统安全、数据库安全和网络安全三部分，尤其是网络安全。

<<计算机安全技术>>

书籍目录

第1章 计算机安全基础知识1.1 计算机安全概述1.1.1 计算机系统面临的威胁和攻击1.1.2 计算机系统安全的重要性1.1.3 计算机安全技术的发展和现状1.1.4 计算机安全技术研究的内容和目的1.1.5 计算机安全系统的设计原则1.2 网络安全体系结构1.2.1 网络安全的含义1.2.2 网络安全存在的问题1.2.3 网络安全的层次体系1.2.4 对网络安全的攻击技术和类型1.2.5 网络安全机制应具有的功能1.2.6 网络安全常用技术1.2.7 安全协议1.3 网络安全标准及安全等级1.3.1 国际上的安全级别评价标准1.3.2 我国网络安全评价标准1.3.3 网络安全的相关法规1.4 计算机软件安全1.4.1 软件的安全技术概述1.4.2 软件分析技术1.4.3 常用的软件保护技术1.4.4 软件的加壳与脱壳1.4.5 软件安全保护建议1.5 计算机病毒及其防御1.5.1 计算机病毒基础知识1.5.2 计算机病毒的防御习题第2章 访问控制与防火墙技术2.1 实体安全概述2.1.1 物理安全策略2.1.2 信息存储的备份2.1.3 安全管理及其他问题的防范2.2 访问控制2.2.1 访问控制的概念和目标2.2.2 访问控制的策略和实现2.3 防火墙2.3.1 防火墙技术2.3.2 防火墙的体系结构2.3.3 防火墙设计及安全策略配置2.3.4 防火墙技术的发展趋势习题第3章 加密与认证3.1 密码技术3.1.1 私钥密码技术3.1.2 公钥密码技术3.1.3 PGP简介3.1.4 SSH安全协议3.2 数字证书、数字认证与公钥基础设施3.2.1 数字证书3.2.2 数字认证3.2.3 公钥基础设施3.3 加密与认证的应用3.3.1 虚拟专用网3.3.2 IP安全协议IPSec3.3.3 基于IPsec的虚拟专用网3.3.4 安全套接字层SSL及SSL VPN习题第4章 端口监听与扫描技术4.1 计算机网络监听概述4.1.1 网络监听的原理4.1.2 检测网络监听的手段4.2 网络监听工具——Sniffer (嗅探器) 4.2.1 Sniffer的工作环境4.2.2 Sniffer网络监听的工作原理4.2.3 怎样在网上发现Sniffer4.2.4 怎样防止被Sniffer4.2.5 Sniffer软件的安装4.2.6 使用Sniffer查询流量信息4.3 端口扫描技术4.3.1 端口扫描的概念4.3.2 端口扫描技术的原理4.3.3 端口号4.3.4 简单端口扫描技术4.3.5 秘密扫描技术4.3.6 SOCKS端口探测技术4.3.7 反弹扫描4.3.8 UDP扫描4.3.9 ICMP扫描4.3.10 端口扫描工具4.3.11 端口扫描侦察工具习题第5章 网络入侵与攻击5.1 初识黑客5.2 黑客攻击的目的及步骤5.2.1 黑客攻击的目的5.2.2 黑客攻击的一般步骤5.3 常见的黑客攻击技术5.3.1 口令攻击5.3.2 漏洞攻击5.3.3 拒绝服务攻击5.3.4 放置特洛伊木马程序5.3.5 缓冲区溢出攻击5.3.6 网络中的欺骗技术5.4 黑客工具5.4.1 木马程序5.4.2 扫描工具5.4.3 破解工具习题第6章 入侵检测技术与蜜罐技术6.1 网络入侵检测概述6.1.1 信息收集6.1.2 信号分析6.2 分层协议模型与TCP / IP协议6.2.1 TCP / IP协议模型6.2.2 TCP / IP协议报文格式6.3 网络数据包的截获6.3.1 以太网环境下的数据截获6.3.2 交换网络环境下的数据截获6.4 网络入侵检测系统6.4.1 入侵检测系统概述6.4.2 入侵检测技术6.4.3 入侵检测产品选择要点6.4.4 入侵检测技术发展方向6.5 蜜罐技术6.5.1 蜜罐技术6.5.2 蜜空间技术6.5.3 蜜网技术习题第7章 安全审计与系统恢复7.1 安全审计7.1.1 安全审计概述7.1.2 日志的审计7.1.3 安全审计的实施7.2 Windows NT中的访问控制与安全审计7.2.1 Windows NT中的访问控制7.2.2 Windows NT中的安全审计7.3 系统恢复7.3.1 系统恢复和信息恢复7.3.2 系统恢复的过程习题第8章 Windows XP的安全8.1 Windows XP的安全特性8.1.1 操作系统的安全8.1.2 Windows XP的安全特性8.1.3 Windows XP安全架构8.1.4 安全标识符8.2 Windows XP的安全配置8.2.1 Windows XP的安装8.2.2 Windows XP系统的两种不同登录方式8.2.3 Windows XP系统的安全策略8.2.4 Windows XP系统“本地安全策略”8.2.5 Windows XP的组策略8.3 Windows XP常用的系统进程和服务8.3.1 Windows XP常用的系统进程8.3.2 Windows XP的系统服务8.4 Windows XP的注册表8.4.1 注册表由来8.4.2 注册表基本知识8.4.3 Windows XP注册表的备份与恢复习题第9章 数据库及应用系统安全9.1 数据库系统安全概述9.1.1 数据库系统的组成9.1.2 数据库系统安全评估标准9.1.3 数据库系统安全性要求9.1.4 数据库系统安全框架9.2 数据库系统安全保护机制9.2.1 用户标识与鉴别9.2.2 存取控制9.2.3 数据库加密9.2.4 数据库审计9.2.5 数据库系统的备份与恢复9.3 SQL数据库的安全管理9.3.1 SQL Server安全管理概述9.3.2 SQL数据库安全性控制策略9.3.3 攻击数据库的常用方法9.3.4 SQL Server的安全配置习题第10章 计算机安全实验10.1 软件动态分析技术10.1.1 实验目的10.1.2 实验理论基础10.1.3 实验内容10.1.4 实验步骤10.2 PGP的原理与使用实验10.2.1 实验目的10.2.2 实验步骤10.2.3 思考题10.3 瑞星防火墙配置实验10.3.1 实验目的10.3.2 实验理论基础10.3.3 实验内容10.3.4 实验步骤10.4 使用Sniffer捕获加密包和非加密包10.4.1 实验目的10.4.2 实验步骤10.5 端口扫描实验10.5.1 实验目的10.5.2 实验原理10.5.3 实验内容10.5.4 思考题10.6 DoS攻击实验10.6.1 实验目的10.6.2 实验内容10.6.3 实验要求10.6.4 思考题10.7 缓冲区溢出实验10.7.1 实验目的10.7.2 实验要求10.7.3 实验内容10.7.4 思考题10.8 入侵检测原理与Snort的使用实验10.8.1 实验目的10.8.2 注意事项和预备工作10.8.3 实验原理10.8.4 实验内

<<计算机安全技术>>

容10.8.5 思考题10.9 剖析特洛伊木马10.9.1 实验目的10.9.2 实验背景10.9.3 实验内容10.9.4 思考题10.10
Windows XP用户帐户的管理10.10.1 实验目的10.10.2 实验步骤参考文献

<<计算机安全技术>>

编辑推荐

《计算机安全技术》适合作为高职高专计算机类专业及需要掌握计算机安全技术的相近专业的课程教材，配合《计算机安全技术》的课件，也可供自学者使用。

<<计算机安全技术>>

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>