

<<计算机网络安全技术>>

图书基本信息

书名：<<计算机网络安全技术>>

13位ISBN编号：9787301153994

10位ISBN编号：7301153996

出版时间：2009-8

出版单位：北京大学出版社

作者：宋西军

页数：300

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>

<<计算机网络安全技术>>

前言

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，越来越多的企业将经营的各种业务建立在Internet / Intranet环境中。

一旦网络系统安全受到严重威胁，不仅会对个人、企业造成不可避免的损失，严重时将会给企业、社会乃至整个国家带来巨大的经济损失。

因此，提高对网络安全重要性的认识，增强网络安全防范意识，强化网络安全防范措施，不仅是各个企业组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

本书共9章，比较全面地介绍了计算机网络安全涉及的各个方面的技术。

第1章概述了计算机网络安全技术；第2章介绍了进行网络攻击的常用技术；第3章介绍了防火墙的基本概念、分类及防火墙的应用实例；第4章介绍了VPN技术的基本概念与分类，对各种VPN实现的技术原理进行了简单比较，并讲解了基于Windows Server2003平台的VPN连接的实现；第5章介绍了公钥基础结构（PKI）技术，并基于Windows Server 2003讲解了密钥证书的管理实现；第6章介绍了入侵检测系统与入侵防御系统；第7章介绍了数据安全，对实现数据完整性的方法给出了详细的介绍，包括在线技术、备份、归档、分级存储管理、容灾技术和方案等；第8章介绍了流行的网络操作系统的安全性实现；第9章介绍了计算机常见的病毒及其防范方法。

<<计算机网络安全技术>>

内容概要

计算机网络安全主要包括数据的传输安全和数据的存储安全两大方面，其保障技术涉及计算机科学、计算机网络、计算机通信、密码技术等多方面的知识。

本书主要内容包括计算机网络安全的概况、常见的网络攻击技术、防火墙技术、VPN技术、公钥基础结构(PKI)技术、入侵检测系统与入侵防御系统、数据安全、网络操作系统的安全性、计算机病毒及其防范9个部分。

本书涵盖了常见的计算机网络安全的实现技术，在内容安排上遵循“实用、够用”的原则，将理论知识和实践技能掌握有机结合，并在Windows平台和Linux平台上给出了应用项目实现的步骤。

全书内容难度适中，实用性强。

本书可作为高职高专院校信息安全技术、计算机网络技术等专业的教材使用，也可作为信息安全管理、网络工程技术人员、网络管理人员的参考用书。

<<计算机网络安全技术>>

书籍目录

第1章 计算机网络安全概述 1.1 计算机网络安全含义 1.1.1 什么是网络安全 1.1.2 网络安全的特征
1.2 影响计算机网络安全因素 1.2.1 网络安全的根源 1.2.2 网络中潜在的威胁 1.3 网络攻击的类型
1.4 网络攻击的常见形式 1.5 计算机网络安全层次结构 1.5.1 物理安全 1.5.2 安全控制 1.5.3 安全服务
1.5.4 安全机制 1.6 计算机网络安全的评价标准 1.6.1 国际标准 1.6.2 国内标准 1.7 网络安全的关键技术
1.8 计算机网络安全的研究意义 1.8.1 计算机网络安全与经济 1.8.2 计算机网络安全与政治
1.8.3 计算机网络安全与社会 1.8.4 计算机网络安全与军事 本章小结 习题第2章 网络攻击技术 2.1
密码破解技术 2.2 网络嗅探技术 2.2.1 嗅探原理 2.2.2 嗅探造成的危害 2.2.3 嗅探器的安全防范 2.3
网络端口扫描技术 2.3.1 TCP/IP相关问题 2.3.2 端口扫描及其分类 2.3.3 常用端口扫描工具 2.4 缓冲区溢出
2.5 拒绝服务攻击技术 2.5.1 拒绝服务概述 2.5.2 典型的拒绝服务攻击 2.5.3 分布式拒绝服务攻击的原理及防范
本章实训 本章小结 习题第3章 防火墙 3.1 防火墙基本概述 3.1.1 防火墙的概念 3.1.2 防火墙的功能
3.2 防火墙的分类 3.2.1 防火墙实现技术 3.2.2 防火墙体系结构 3.2.3 防火墙分类 3.3 防火墙应用实例
3.3.1 基础概念 3.3.2 应用实例 本章实训 本章小结 习题第4章 VPN技术 4.1 VPN概述 4.1.1 VPN的概念
4.1.2 VPN的特点 4.1.3 VPN的分类 4.2 VPN关键技术 4.2.1 隧道技术 4.2.2 加解密技术 4.2.3 密钥管理技术
4.2.4 使用者与设备身份认证技术 4.3 隧道协议与VPN实现 4.3.1 PPTP VPN 4.3.2 L2F VPN 4.3.3 L2TP VPN
4.3.4 MPLS VPN 4.3.5 IPsec VPN 4.3.6 SSL VPN 4.3.7 SOCKS v5 VPN 4.4 Windows Server 2003系统中VPN连接的实现
4.4.1 Windows Server 2003系统中VPN概述 4.4.2 远程访问VPN服务器 4.4.3 配置远程访问VPN服务器 4.4.4 远程访问客户端的配置
4.4.5 路由器到路由器VPN 4.5 VPN益处 4.6 VPN发展趋势 本章实训 本章小结 习题第5章 公钥基础结构(PKI)技术
5.1 公钥基础结构简介 5.1.1 网络传输的安全需求 5.1.2 PKI的定义 5.1.3 PKI的内容 5.1.4 PKI的相关标准
5.2 证书权威(CA) 5.2.1 CA的功能和组成 5.2.2 CA自身证书的管理 5.2.3 CA对用户证书的管理 5.2.4 密钥管理和KMC
5.2.5 时间戳服务 5.2.6 密钥硬件简介 5.2.7 CA产品简介 5.3 数字证书和CRI 5.3.1 数字证书的定义 5.3.2 数字证书的类型
5.3.3 证书的撤销列表 5.4 Windows Server 2003证书服务实现 5.4.1 部署证书服务 5.4.2 使用证书 5.4.3 管理证书
本章实训 本章小结 习题第6章 入侵检测系统与入侵防御系统 6.1 入侵检测概述 6.1.1 入侵检测系统简介
6.1.2 入侵检测系统的功用 6.1.3 入侵检测系统的分类 6.2 入侵检测系统的设计 6.2.1 CIDF模型 6.2.2 入侵检测系统的构建
6.3 入侵检测系统的弱点与局限 6.3.1 NIDS的弱点与局限 6.3.2 HIDS的弱点与局限 6.4 几种典型的入侵检测系统
6.4.1 启明星辰天阕入侵检测与管理系统 6.4.2 安氏领信网络入侵检测系统 6.5 入侵防御技术概述 6.5.1 入侵防御系统简介
6.5.2 入侵防御系统的功用 6.6 入侵防御系统的设计 6.7 入侵防御系统的弱点与局限 6.8 几种典型的入侵防御系统
6.8.1 H3C SecPath IPS(Intrusion Prevention System)入侵防御系统 6.8.2 启明星辰天清入侵防御系统(IPS) 6.8.3 安氏领信网络入侵防御检测系统
6.9 入侵检测技术与入侵防御技术的区别 本章实训 本章小结 习题第7章 数据安全 7.1 数据完整性简介 7.1.1 数据完整性丧失的原因
7.1.2 保障数据完整的方法 7.2 磁盘阵列 7.2.1 RAID技术规范简介 7.2.2 JBOD模式 7.2.3 IDE或SATA RAID 7.2.4 RAID常见故障及相关处理方式
7.3 备份 7.3.1 镜像备份 7.3.2 单机和网络备份 7.4 归档和分级存储管理 7.4.1 归档 7.4.2 分级存储管理(HSM)
7.5 容灾计划 7.5.1 容灾与备份 7.5.2 容灾的分类 7.5.3 容灾系统的组成 7.5.4 容灾等级 7.6 CDP技术 7.6.1 CDP技术简介
7.6.2 CDP产品 7.6.3 CDP应用 7.7 灾备方案的主要应用及发展 7.7.1 灾备系统应用误区 7.7.2 未来发展方向 本章实训 本章小结 习题第8章 网络操作系统的安全性
8.1 Windows XP操作系统的安全性 8.1.1 Windows XP的登录机制 8.1.2 Windows XP的屏幕保护机制 8.1.3 Windows XP的文件保护机制
8.1.4 利用注册表提高Windows XP系统的安全 8.2 Windows 2003的安全基础 8.2.1 Windows 2003的安全基础概念 8.2.2 Windows 2003的安全模型
8.2.3 Windows 2003的安全机制 8.2.4 Windows 2003的安全性 8.2.5 Windows 2003安全访问控制 8.2.6 在Windows 2003系统中监视和优化性能
8.2.7 Windows 2003的安全措施 8.3 Unix系统的安全性 8.3.1 Unix操作系统简介 8.3.2 Unix系统的安全性 8.4 Linux系统的安全性
8.4.1 Linux操作系统简介 8.4.2 Linux系统的常用命令 8.4.3 Linux系统的网络安全 本章实训 本章小结 习题第9章 计算机病毒及其防范 9.1 计算机病毒概述
9.1.1 计算机病毒的定义 9.1.2 计算机病毒的发展历史 9.1.3 计算机病毒的危害 9.2 计算机病毒

<<计算机网络安全技术>>

毒的特征与分类 9.2.1 计算机病毒的特征 9.2.2 计算机病毒的分类 9.3 计算机病毒的工作原理 9.3.1 计算机病毒的结构 9.3.2 引导型病毒的工作原理 9.3.3 文件型病毒的工作原理 9.4 常见计算机病毒介绍 9.4.1 特洛伊木马分析与防范 9.4.2 蠕虫病毒分析与防范 9.4.3 宏病毒分析与防范 9.4.4 ARP病毒分析与防范 9.5 反病毒技术 9.5.1 反病毒技术的发展 9.5.2 病毒防治常用方法 9.5.3 Windows病毒防范技术 9.6 常用杀毒软件介绍 9.6.1 瑞星杀毒软件 9.6.2 江民杀毒软件 本章实训 本章小结 习题 参考文献

章节摘录

插图：第1章计算机网络安全概述随着计算机和网络技术的迅猛发展和广泛普及，越来越多的企业将经营的各种业务建立在Internet / Intranet环境中。

于是，支持E-mail、文件共享、即时消息传送的消息和协作服务器成为当今商业社会中的极重要的IT基础设施。

然而，大部分企业在充分体会到了互联网的好处的时候，却较少关心网络互联带来的风险。

据报道，现在全世界平均每20秒就发生一次计算机网络入侵事件，而全球每年因网络安全问题造成的经济损失也达数千亿美金。

现在，人们日常使用的软盘、CD、VCD、DVD都可能携带恶性代码；E—mail、上网浏览、软件下载以及即时通讯都可能被黑客利用而受到攻击；一台新计算机在连接到网上不到15分钟即可能被扫描到

。

所以人们所处的网络环境已没有值得信任的了。

金陵晚报2009年5月4日报道：雇用黑客编写木马程序，再将其挂在网上兜售，用于窃取游戏玩家的账号和密码。

由一伙分工明确、制销一条龙的犯罪团伙组成的“木马帝国”，在不到一年的时间内侵入全国数万用户的计算机系统，从中牟利200多万元。

此案曾一度引发了全国网民的关注，被公安部列为重点挂牌督办大案。

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，一旦网络系统安全受到严重威胁，不仅会对个人、企业造成不可避免的损失，严重时将会给企业、社会乃至整个国家带来巨大的经济损失。

因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，不仅是各个企业组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

<<计算机网络安全技术>>

编辑推荐

《计算机网络安全技术》：全国高职高专应用型规划教材(信息技术类)

<<计算机网络安全技术>>

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>