

# 《信息安全实用技术》

## 图书基本信息

书名：《信息安全实用技术》

13位ISBN编号：9787562433613

10位ISBN编号：7562433615

出版时间：2005-5

出版社：重庆大学出版社

作者：戴宗坤

页数：344

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《信息安全实用技术》

## 内容概要

本书采用理论与工程实际相结合的方法对信息安全的若干实用技术进行了简明通俗的介绍，包括身份鉴别的原理、方法，Kerberos系统和用于建立网络信任体系的PKI，防火墙技术原理、配置方法和拓扑结构，入侵检测技术，VPN、Ipsec和网络安全，在公共网络上使用VPN技术构建安全网络平台的原理、方法和工程实现，Internet应用安全，审计与报警技术，病毒和恶意代码的技术原理及病毒防范体系，黑客技术分析等内容，并根据编著者研究成果和经验，对网络信息系统的安全解决方案给出了具体的方法和案例。

本书作为全国信息技术人才培养工程信息安全专业技术指定培训教材，亦可作为信息安全和计算机应用本专科教材，并对从事信息安全管理、信息系统管理以及信息安全咨询服务的专业技术人员具有参考价值。

## 书籍目录

1 身份鉴别技术	1.1 身份鉴别	1.1.1 鉴别的基本概念	1.1.2 鉴别的方法	1.1.3 人类用户鉴别	1.1.4 鉴别的阶段	1.1.5 可信任第3方的参与	1.2 身份鉴别系统Kerberos	1.2.1 Kerberos介绍	1.2.2 Kerberos的目的	1.2.3 Kerberos协议	1.2.4 Kerberos模型	1.2.5 Kerberos工作原理	1.2.6 Kerberos第5版与第4版的区别	1.2.7 Kerberos的安全性	1.3 公开密钥基础设施	1.3.1 概述	1.3.2 PKI提供的服务	1.3.3 PKI构成	1.3.4 PKI标准	1.3.5 基于PKI的信任模型	1.3.6 PKI的运行模型	1.3.7 MS Windows 2000公钥基础设施2																																																																																																																														
防火墙技术	2.1 基本概念	2.2 防火墙的基本类型	2.2.1 包过滤	2.2.2 应用网关	2.2.3 电路网关	2.2.4 混合型防火墙	2.2.5 状态检测防火墙	2.3 防火墙的配置形式	2.3.1 包过滤路由器防火墙	2.3.2 双穴机网关防火墙	2.3.3 主机过滤防火墙	2.3.4 子网过滤防火墙	2.3.5 跨越公共网络的基于VPN的内联网防火墙系统	2.4 防火墙的局限性	2.5 防火墙的应用示例	2.5.1 主要特性	2.5.2 典型应用配置实例3	入侵检测	3.1 入侵检测系统概述	3.1.1 入侵检测系统的功能	3.1.2 入侵检测的发展	3.1.3 入侵检测系统的分类	3.2 入侵检测系统的系统结构	3.2.1 CIDF模型	3.2.2 简单的分布式入侵检测系统	3.2.3 基于智能代理技术的分布式入侵检测系统	3.3 入侵检测分析技术	3.3.1 入侵分析概述	3.3.2 异常检测分析方法	3.3.3 滥用检测分析方法	3.4 入侵检测系统的实际应用	3.4.1 IDS的部署	3.4.2 入侵检测系统存在的问题和发展方向	3.4.3 典型入侵检测系统简介4	VPN与网络安全	4.1 前言	4.2 VPN技术及其应用	4.2.1 VPN概念	4.2.2 VPN技术的发展	4.2.3 VPN的应用领域	4.3 VPN技术及其管理	4.3.1 VPN在TCP/IP协议栈的实现	4.3.2 VPN的管理问题	4.4 VPN与网络安全	4.4.1 网络安全的要素	4.4.2 安全VPN与网络安全	4.5 链路层隧道封装技术	4.5.1 L2F协议	4.5.2 L2TP协议	4.5.3 PPTP协议	4.6 因特网协议安全	4.6.1 概述	4.6.2 设计Ipsec的目的	4.6.3 Ipsec的体系结构	4.7 SSL和TLS	4.7.1 SSL	4.7.2 TLS	4.7.3 SSL的应用5	因特网应用安全	5.1 WWW的安全	5.1.1 WWW安全分析	5.1.2 Web安全防护技术	5.1.3 主页防黑技术	5.2 电子商务的安全	5.3 因特网信息过滤技术	5.3.1 内容阻塞	5.3.2 内容定级和自我鉴定	5.3.3 RSACi	5.3.4 使用内容定级和自我鉴定的例子	5.3.5 其他一些客户端封锁软件	5.4 电子邮件的安全	5.4.1 概述	5.4.2 PGP	5.4.3 S/MIME	5.4.4 垃圾邮件	5.5 网上数据库安全	5.5.1 数据库系统	5.5.2 数据库基本安全架构	5.5.3 数据库的安全控制	5.5.4 数据库加密	5.5.5 Oracle数据库的安全措施6	安全审计和报警	6.1 基本概念	6.2 安全审计线索	6.3 开放系统互联的安全审计和报警通则	6.4 审计事件的时间注册	6.5 安全审计和报警功能及实现	6.5.1 安全审计和报警准则	6.5.2 安全审计和报警模型的实现	6.5.3 安全审计和报警设施概览	6.5.4 安全审计的日常管理	6.5.5 安全审计与反制	6.5.6 审计实现和应用时的若干考虑7	病毒与恶意代码	7.1 概述	7.1.1 病毒的由来	7.1.2 计算机病毒在中国	7.2 计算机病毒的特点与种类	7.2.1 计算机病毒的特点	7.2.2 关于计算机病毒的分类	7.3 病毒的产生、传播途径和寄生软件	7.3.1 病毒的产生	7.3.2 病毒的传播途径	7.3.3 病毒的寄生软件	7.4 计算机病毒的结构和形式描述	7.4.1 计算机病毒的结构	7.4.2 计算机病毒的形式描述	7.5 病毒的表现行为	7.6 典型病毒简介	7.7 计算机病毒的动态特性	7.8 反病毒的斗争	7.8.1 提高认识	7.8.2 建立、健全法律法规和管理制度, 加强教育和宣传	7.8.3 病毒防范的技术措施8	黑客、黑客技术及其防范措施	8.1 什么是黑客	8.1.1 黑客的定义和分类	8.1.2 黑客对网络信息系统的影响	8.1.3 相关法律	8.2 黑客常用的攻击方法和防范措施	8.2.1 黑客攻击的一般过程	8.2.2 信息探测	8.2.3 网络嗅探攻击技术	8.2.4 缓冲区溢出攻击	8.2.5 SQL注入式攻击	8.2.6 特洛伊木马攻击技术	8.3 黑客技术的可利用性	8.3.1 利用黑客技术对信息系统进行监管	8.3.2 促进对黑客技术的研究和利用9	信息系统安全方案设计方法	9.1 信息系统基本结构及资源分析	9.1.1 网络结构	9.1.2 资源分析	9.2 安全风险分析	9.2.1 安全事件发生可能性(概率)分析	9.2.2 攻击者及其目的分析	9.2.3 攻击地点及其工具分析	9.2.4 脆弱性分析	9.2.5 攻击结果分析	9.2.6 用户风险分析	9.2.7 支持系统风险分析	9.2.8 残余风险分析	9.3 安全需求分析	9.3.1 按对信息的保护方式进行安全需求分析	9.3.2 按与风险的对抗方式进行安全需求分析	9.4 安全规则与设计原则	9.5 系统安全体系	9.5.1 技术体系

# 《信息安全实用技术》

9.5.2 组织体系    9.5.3 管理体系    9.6 安全解决方案    9.6.1 安全方案总成    9.6.2 物理  
安全和运行安全    9.6.3 网络规划与子网划分    9.6.4 网络隔离与访问控制    9.6.5 操作系统  
安全增强    9.6.6 应用系统安全    9.6.7 重点主机防护系统    9.6.8 连接与传输安全    9.6.9  
安全综合管理与控制附录    附录1 信息安全常用缩略语    附录2 名词与术语参考文献

# 《信息安全实用技术》

## 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:[www.tushu000.com](http://www.tushu000.com)