

<<计算机网络安全工程师宝典>>

图书基本信息

书名：<<计算机网络安全工程师宝典>>

13位ISBN编号：9787229030438

10位ISBN编号：7229030439

出版时间：2010-11

出版时间：重庆

作者：陈庄//巫茜

页数：520

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>

<<计算机网络安全工程师宝典>>

前言

随着计算机技术、现代通信技术和网络技术的发展，尤其是Internet的广泛应用，计算机的应用更加广泛与深入，计算机网络和人们的工作与生活的联系也越来越密切。

在受益于计算机网络便利的同时，人们也发现自己的计算机信息系统不断受到侵害，其形式多样、技术先进且复杂，令人防不胜防。

因此，伴随着计算机网络在政治、经济、文化、教育、通信、军事等方面的作用日益增大，社会对计算机网络依赖的日益增强，网络安全问题成了一个热点。

计算机网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏篡改和泄露，保证网络系统的正常运行、网络服务不中断。

它是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合学科。

影响网络安全的因素很多，保护网络安全的技术手段也很多，主要包括防火墙技术、入侵检测技术、安全评估技术、防病毒技术、加密技术、身份认证技术等等。

<<计算机网络安全工程师宝典>>

内容概要

本书密切结合我国计算机网络安全技术和设计的前沿知识，全面系统地介绍了计算机网络安全技术和设计的内涵、意义、方法和原理。

全书共分为三篇，第1篇介绍网络安全技术相关内容，共分9章，主要内容包括计算机网络基础、网络安全技术概述、密码技术、防火墙技术、入侵检测技术、虚拟专用网、反病毒技术、无线网络安全技术、常用系统的网络安全策略等；第2篇介绍网络安全设计相关内容，共分7章，主要内容包括网络安全设计概论、物理安全设计、网络安全设计、主机安全设计、应用安全设计、数据安全设计和网络安全系统设计方案等；第3篇为实验篇，包括网络信息探测、入侵检测、网络监听、邮件加密、虚拟机安装、SSL软件、密码学等实验项目。

本书内容深入浅出，既注重理论研究，又注重实际操作应用，而且包含丰富的习题和实验题目，特别适合作为高等院校计算机网络安全类专业学生的教材，也可作高职高专和有关培训机构的教材，还可供企事业单位从事网络安全设计和管理的专业技术人员阅读、参考。

书籍目录

计算机网络安全技术篇 第1章 计算机网络基础 1.1 计算机网络概念 1.1.1 计算机网络的定义 1.1.2 计算机网络的发展概况 1.1.3 计算机网络的基本功能 1.2 计算机网络体系结构 1.2.1 计算机网络体系结构特点 1.2.2 ISO/OSI开放系统互联参考模型 1.3 计算机网络互联部件 1.3.1 计算机与外部设备 1.3.2 网络连接设备 1.3.3 传输介质 1.3.4 网络协议 1.3.5 网络协议 1.4 TCP/IP网络协议和服务 1.4.1 TCP/IP的概念 1.4.2 TCP/IP的层次结构 1.4.3 TCP/IP协议与安全服务 思考题 第2章 网络安全技术概述 2.1 网络安全技术概念 2.1.1 网络安全定义及特征 2.1.2 威胁网络安全的主要因素 2.1.3 网络攻击 2.1.4 网络安全的基本技术 2.2 网络安全技术特征 2.2.1 网络安全层次结构模型 2.2.2 ISO/OSI网络安全体系结构 2.2.3 其他网络安全转型 2.2.4 网络安全技术评估标准 2.3 网络安全技术分类 2.3.1 被动的网络安全技术 2.3.2 主动的网络安全技术 2.4 网络安全技术发展趋势 2.4.1 防火墙技术发展趋势 2.4.2 入侵检测技术发展趋势 2.4.3 防病毒技术发展趋势 思考题 第3章 密码技术 3.1 密码技术概论 3.1.1 密码技术基本概念 3.1.2 密码技术的数学表述 3.1.3 密码技术发展历程 3.2 对称密码技术 3.2.1 对称密码技术概论 3.2.2 古典对称密码技术 3.2.3 现代对称密码技术——DES算法 3.3 非对称密码系统 3.3.1 非对称密码技术概论 3.3.2 著名非对称加密技术——RSA算法 3.3.3 PKI系统 思考题 第4章 防火墙技术 4.1 防火墙概念 4.1.1 防火墙的定义 4.1.2 防火墙的原理与组成 4.1.3 防火墙的分类 4.1.4 防火墙的功能及重要性 4.1.5 防火墙技术发展动向和趋势 4.2 防火墙体系结构 4.2.1 双重宿主主机体系结构 4.2.2 被屏蔽主机体系结构 4.2.3 被屏蔽子网体系结构 4.3 防火墙设计及实现 4.3.1 防火墙主要性能指标 4.3.2 防火墙安全设计策略 4.3.3 典型防火墙的设计与实现 4.4 防火墙应用案例 4.4.1 防火墙的选择原则 4.4.2 防火墙的部署方法和步骤 4.4.3 典型的防火墙产品 4.4.4 典型防火墙产品的应用 思考题 第5章 入侵检测技术 5.1 入侵检测概念 5.1.1 入侵检测的定义 5.1.2 入侵检测系统的分类 5.1.3 入侵检测的发展动向和趋势 5.2 入侵检测原理 5.2.1 入侵检测系统的标准模型 5.2.2 入侵检测系统的分析方法 5.2.3 入侵检测系统的部署 5.3 入侵检测应用案例 5.3.1 入侵检测系统的选择原则 5.3.2 典型的入侵检测系统介绍 思考题 第6章 虚拟专用网(VPN)技术 6.1 VPN概述 6.1.1 VPN的概念 6.1.2 VPN的体系结构 6.1.3 VPN的应用领域 6.2 VPN隧道协议 6.2.1 VPN隧道技术的概念 6.2.2 VPN隧道技术对比 6.3 VPN加密方案 6.4 VPN过滤规则 6.5 VPN技术应用 6.5.1 VPN技术应用概况 6.5.2 VPN技术应用案例 思考题 第7章 反病毒技术 第8章 无线网络安全技术 第9章 常用系统的网络安全策略 计算机网络安全设计篇 第10章 网络安全设计概论 第11章 物理安全设计 第12章 网络安全设计 第13章 主机安全设计 第14章 应用安全设计 第15章 数据安全设计 第16章 网络安全系统设计 方案编写及案例参考文献

章节摘录

插图：被动意味着一旦检测到安全破坏，特定的信息安全技术才会采取保护措施试图保护数据或者资源。

常见的被动的网络安全技术主要有以下7种。

防火墙：用一个或一组网络设备（计算机系统或路由器等），在两个或多个网络间加强访问控制，以保护一个网络不受来自另一个网络攻击的安全技术。

它是被动的网络安全技术。

一旦出现特定的安全事件，才会使用防火墙抵御它们。

接入控制：目的是确保主体有足够的权利对系统执行特定的动作。

主体可以是一个用户、一群用户、服务或者应用程序主体对系统中的特定对象有不同的接入级别。

对象可以是文件、目录、打印机或者进程。

一旦有接入请求就会使用接入控制技术允许或者拒绝接入系统，所以它是被动的信息安全技术。

口令：它是必须输入才能获得进入或者接入信息（例如文件、应用程序或者计算机系统）的保密字、短语或者字符序列。

口令是被动的网络安全技术，一旦有人或进程想登录到应用程序、主机及网络，才会使用它们允许或拒绝接入系统。

生物特征识别：它是指通过计算机利用人类自身的生理或行为特征进行身份认定的一种技术。

包括指纹、虹膜、掌纹、面相、声音、视网膜和DNA等人体的生理特征，以及签名的动作、行走的步态、击打键盘的力度等行为特征。

生物特征的特点是人各有异、终生不变（几乎）、随身携带。

一旦某个人想使用他/她人体的一部分的几何结构登录到应用程序，主机或者网络就会使用生物特征识别技术允许或者拒绝他/她接入系统。

所以该技术是被动的网络安全技术。

<<计算机网络安全工程师宝典>>

编辑推荐

《计算机网络安全工程师宝典》：最前沿、最权威、最完整、最实用的网络安全解决方案

<<计算机网络安全工程师宝典>>

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>