第一图书网, tushu007.com

<<网络安全原理与应用>>

图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787512303416

10位ISBN编号：7512303416

出版时间：2010-7

出版时间：中国电力出版社

作者：闫大顺，石玉强　主编

页数：341

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

前言

随着信息技术的广泛应用和发展，人们对计算机和网络的依赖性越来越大，信息被暴露和非法使用、网络受到攻击的可能性也变得越来越大。
随着经济全球化、军事指挥网络化，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱。
一个国家的网络信息获取能力和网络信息安全保障能力已成为21世纪的综合国力、经济竞争能力和生存能力的重要组成部分，呈上升趋势的网络安全事件已成为信息社会十分突出的问题。
网络安全本质上就是计算机网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。
通过网络安全原理的分析，结合网络安全的实践技术，能够给个人或企业用户使用计算机网络时提供数据传递的机密性、完整性、真实性，保护用户的利益和隐私；也能够给网络运行和管理者提供有效的、安全的网络访问、读写等操作，保护网络资源和服务。
网络安全的概念是与时俱进的，历经了可靠性、保密、保护，而发展到今天的网络信息保障。
本书从技术的角度介绍了网络安全保障体系，从应用的角度介绍了提高网络安全的各种措施和技术，并进一步强调网络安全是一个动态的整体安全。
本书力图全面、系统、深入地介绍网络安全原理及其应用的相关知识，主要体现在以下几个方面。
（1）体系完整，内容全面。
本书内容全面，突出知识体系的完整性，并用通俗易懂的语言讲述抽象的理论。
（2）图文并茂，示例丰富。
本书图文并茂，精心选取常见示例帮助读者理解相关理论概念。
（3）循序渐进、深入浅出。
本书内容讲解循序渐进，深人浅出，概念清晰，条理性强，符合读者学习网络安全原理的认识规律。
（4）理论与技术联系密切。
全书围绕网络安全原理与应用技术两个核心点展开。
叙述基础理论时易懂易学；介绍应用技术时详尽周密。
理论与技术的密切结合是本书的一大特色。
本书由闫大顺、石玉强主编，负责全书内容的取材和组织，闫大顺编写了第1章和第14章的第l、第2节，石玉强编写了第4章的第1、第2节和第8章，刘磊安编写了第4章的第3、第4节和第12章，杜淑琴编写了第2、第3章，邹莹编写了第5、第6章，刘佳编写了第7、第9章，邹娟编写了第10章，谢芳清编写了第11章，李晟编写了第13章及第14章的第3节，参编的还有王洁、高杨、张海强、陈滢生等。
另外，编者感谢曹天杰教授、沈玉利教授、吴家培副教授给予的指导和各种不同形式的帮助。
本书由赵春晓主审。

内容概要

本书为21世纪高等学校规划教材。
　　本书主要从网络安全的基本原理和实践技术两个方面，系统分析了网络安全各种常见的安全威胁，提出了网络安全原理的本质，给出了网络安全的各种主要防御技术。
全书从网络安全体系上分三部分：第一部分，计算机网络安全基础，介绍网络安全概述、物理安全、网络协议安全和网络攻击；第二部分，主动防御技术，包括密码编码学基础、数字认证、PKI与PMI、身份认证、VPN技术、Web安全、操作系统及软件平台安全；第三部分，被动防御技术，包括计算机病毒及其防范、防火墙、入侵检测等。
本书既注重基本原理的阐述，又关注网络安全的新动向，适时增加了实践的新技术。
每章最后都配有习题，用来检查学习效果。
本书重点突出、难易适当、实例丰富、实用性强。
　　本书可作为高等院校计算机科学与技术等专业网络安全、计算机系统安全等课程的教材，也可供从事网络安全研究和计算机系统安全管理等领域的人员参考。

书籍目录

第1章　网络安全概述　1．1　网络安全问题　1．2　网络安全体系　1．3　网络安全设计　1．4　网络安全的措施　1．5　网络安全的发展方向　小结　习题第2章　物理安全　2．1　物理安全　2．2　交换机安全　2．3　路由器安全　小结　习题第3章　网络协议安全　3．1　OSI参考模型　3．2　TCP／IP参考模型　3．3　TCP／IP协议簇　3．4　链路层协议漏洞分析　3．5　网络层协议漏洞分析　3．6　传输层协议漏洞分析　3．7　常用应用层协议及安全性分析　小结　习题第4章　网络攻击　4．1　攻击概述　4．2　网络侦查技术　4．3　缓冲区溢出攻击　4．4　拒绝服务攻击　小结　习题第5章　病毒　5．1　病毒概述　5．2　Windows病毒　5．3　网络蠕虫　5．4　特洛伊木马　小结　习题第6章　密码编码学基础　6．1　密码学概述　6．2　传统加密技术　6．3　分组密码　6．4　公钥密码体制　小结　习题第7章　数字认证　7．1　消息认证　7．2　数签名　7．3　数字水印　小结　习题第8章　PKI和PMI　8．1　PKI的概念　8．2　信任模型　8．3　PKI体系结构　8．4　数字证书　8．5　PMI　8．6　CA系统的安全设计　小结　习题第9章　身份认证　9．1　认证的基本原理　9．2　认证协议　小结　习题第10章　防火墙　10．1　防火墙概述　10．2　防火墙的设计策略和安全策略　10．3　防火墙的技术　10．4　防火墙的体系结构　……第11章　入侵检测第12章　VPN技术第13章　Web安全第14章　操作系统及软件平台安全参考文献

章节摘录

插图：随着社会经济和科学技术的飞速发展，信息技术和计算机网络正大幅度对传统行业的生产、营销和管理模式产生改变，同时也促使相关的新产业诞生号陕速成长，以计算机网络进行交流的信息已成为国家和社会发展的重要战略资源。
迄今为止，信息技术与计算机网络已经更深地融合到国家的政治、经济、军事、交通、通信、卫生、文教等诸多领域，以电子商务、电子政务、电子税务、电子银行、电子海关、电子证券、网络书店、网上拍卖、网络购物、网络防伪、远程教育、远程医疗、网上交易、网络监控、网络营销、网上选举、网上娱乐等形式发挥越来越大的作用。
为此在计算机网络中存储、传输和处理的海量信息中有许多是商业经济信息、银行转账、股票证券、军事国防数据、科研数据等敏感信息或机密信息，开放式的计算机网络自然吸引各式各样怀有不同目的攻击，来窃取信息、泄露信息、修改和删除信息，每年都带来极大的损失。
因此计算机网络安全是一个关系到国家的安全、社会的稳定、民族文化的继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快而变得越来越重要。
随着Internet的广泛应用，网络上出现的安全问题越来越多、越来越严重。
第一起网络安全事件是1986年初在巴基斯坦的拉合尔（Lahore），巴锡特（Basit）和阿姆杰德（Am jad）两兄弟编写的Pakistan病毒（Brain）在一年内流传到了世界各地。
从此之后爆发了众多的网络攻击事件，如网络蠕虫病毒感染、主机被控制、数据库被非法访问’Web服务器网页被更改、非法电子银行转账等。
事实上，相当多的网络入侵或攻击并没有被发现。
即使被发现了，由于这样或那样的原因，人们并不愿意公开它。
这说明世界上没有绝对安全的网络，只要用户使用联网的计算机或其他接入设备以及网络连接了Internet，它就存在危险，要使用网络就必须考虑它的安全问题。

编辑推荐

《网络安全原理与应用》：21世纪高等学校规划教材

第一图书网, tushu007.com

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