<<计算机网络安全实用技术>>

图书基本信息

书名：<<计算机网络安全实用技术>>

13位ISBN编号：9787508469584

10位ISBN编号：7508469585

出版时间：2010-1

出版时间：水利水电出版社

作者：葛彦强，汪向征　主编

页数：282

前言

随着计算机网络安全技术的广泛应用，社会对网络安全技术人才的需求量增加，培养网络安全技术人才成为高等教育的重要任务之一。
学校培训需要实用型教材，要将枯燥难以理解的网络安全理论和技术变得容易掌握，充分体现学以致用的原则。
本教材就是基于这一原则编写的，并且还能满足广大读者的自学需求。
在保留足够的理论知识的基础上，密切联系实际应用，着重强调实用性和操作性，让读者既能通过本书学到实战经验，又能充分理解网络安全技术原理，轻松地掌握网络知识和技能，更好地促进有效性学习。
本教材共分为12章，主要内容介绍如下：第1章首先介绍了网络安全的基本概念；然后分别介绍了网络所面临的各种威胁，以及导致网络不安全的因素；接着介绍了网络安全的策略、服务与机制；还介绍了网络安全的体系机构，其中重点说明TCP／IP的安全体系结构；最后介绍了网络安全的不同级别，并举例说明各个级别。
第2章首先简单介绍了密码学发展历史、概念和分类；然后详细介绍了对称加密技术和非对称加密技术：最后介绍了网络加密中的三种方法：链路加密、结点加密和端对端加密。
第3章首先介绍了Hash算法的定义、分类、安全性、结构和MD5算法及SHA算法；然后详细介绍了数字签名技术，包括基本原理、加密算法、问题及改进等；接着又详细介绍了身份认证，包括Kerberos认证协议和认证体系x.509；还介绍了标准的密钥管理平台PKI，包括PKI概念、PKI提供的服务、PKI的组成、PKI的功能、密钥管理、信任模型和PKI的应用；最后简单介绍了授权管理基础架构（PMI）。
第4章首先简单介绍了防火墙的基本概念、作用、优点和缺点；然后详细介绍了防火墙的各种分类；接着又详细介绍防火墙的组成；还介绍了防火墙所采用的技术及三种体系结构；之后介绍了防火墙的实现以及常用的防火墙软件；最后简单介绍了网闸技术的概念、发展、对比及应用。
第5章首先介绍了入侵检测系统的定义、模型、功能和分类；然后介绍了入侵检测系统的原理，包括异常检测、误用检测以及特征检测等；接着分别介绍了基于主机的入侵检测系统、基于网络的入侵检测系统和基于分布式的入侵检测系统等三种不同的入侵检测系统；还介绍了Snort和ISS Real Secure的安装和使用；最后介绍了入侵检测系统目前的发展以及入侵检测的标准和功能评估。
第6章介绍了端口扫描和嗅探技术的基本原理和常用的工具。
第7章首先介绍了黑客攻击的基本步骤和拒绝服务的攻击与防御方法，最后介绍一些其他的攻击方式和防范方法。
第8章介绍了计算机病毒的定义、特征、分类、危害、传播途径、表现和发展趋势，还介绍了计算机病毒的基本机制以及网络蠕虫和木马的原理和防范。

<<计算机网络安全实用技术>>

内容概要

本书结合作者多年从事网络安全技术课程教学和实践工作的经验，针对应用型人才培养特点和社会需求编写，内容充实、思路清晰、实例丰富，突出了学以致用的原则，注重读者基本技能、创新能力和综合应用能力的培养，体现了高等教育的特点和要求。

全书共分12章，主要内容包括：网络安全概述、密码学基础和加密技术、数字签名和认证、防火墙技术和网闸技术、入侵检测技术、端口扫描与嗅探技术、黑客攻击和防范技术、计算机病毒及恶意代码、电子邮箱的使用及安全防范、网络操作系统安全、因特网服务的安全及安全网站的建设。能满足读者对服务器和个人电脑防护、安全配置和安全管理的需要。

本书介绍了大量的网络安全实用软件，包括各种技术中常用的软件。在各章后面配有课后习题，对每章的知识进行复习和巩固。

本书具有教材和技术资料双重特征，既可作为高等学校计算机及相关专业学生计算机网络安全技术课程的教材，也可作为网络安全技术人员的技术参考资料。

<<计算机网络安全实用技术>>

书籍目录

章节摘录

插图：（2）网络上系统信息的安全：包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。
（3）网络上信息传播的安全：即信息传播后果的安全。
包括信息过滤、不良信息的过虑等。
它侧重于防止和控制非法、有害的信息进行传播后的后果。
避免公共通信网络上大量自传输的信息失控。
本质上是维护道德、法则和国家利益。
（4）网络上信息内容的安全：即我们讨论的狭义的“信息安全”。
它侧重于保护信息的机密性、真实性和完整性。
避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。
本质上是保护用户的利益和隐私。
显而易见，网络安全与其所保护的信息对象有关。
本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。
显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。
1.1.4 计算机网络安全的属性网络安全有自己特定的属性，主要有机密性、完整性、可用性和可控性这四个方面。
（1）机密性是为了使信息不泄露给非授权用户、非授权实体或非授权过程，或供其利用，防止用户非法获取关键的敏感信息或机密信息。
通常采用加密来保证数据的机密性。
（2）完整性是为了使数据未经授权不能被修改，即信息在存储或传输过程中保持不被修改、不被破坏和不被丢失。
它主要包括软件的完整性和数据的完整性两个方面的内容。
·软件完整性是为了防止对程序的修改，如病毒。
·数据完整性是为了保证存储在计算机系统中或在网络上传输的数据不受非法删改或意外事件的破坏，保持数据整体的完整。
（3）可用性是为了被授权实体访问并按需求使用，即当用户需要时能够在提供服务的服务器上进行所需信息的存取。
例如：网络环境下拒绝服务、破坏网络和破坏有关系统的正常运行等，都属于对可用性的攻击。
（4）可控性是为了对信息的传播及内容具有控制能力。
任何信息都要在一定传输范围内可控，如密码的托管政策等。
1.2 网络面临的威胁计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。

<<计算机网络安全实用技术>>

编辑推荐

《计算机网络安全实用技术》特色：紧扣教学(考试)大纲，精心设计教学内容着眼热点、难点、疑点问题，把握网络安全未来发展趋势系统阐述网络安全理论、网络安全防护基本方法和成熟技术以常用网络安全软件使用和工程实践项目为中心，手把手教学结合主要知识点，精选200多道习题(选择、填空、问答、操作等)，供读者练习与自测提供丰富相关资源(电予教案、案例源程序代码等)

<<计算机网络安全实用技术>>

版权说明