<<网络安全防御技术实践教程>>

图书基本信息

书名：<<网络安全防御技术实践教程>>

13位ISBN编号：9787302209836

10位ISBN编号：7302209839

出版时间：2010-1

出版时间：清华大学出版社

作者：黄传河，喻涛，王昭顺 编著

页数：311

前言

随着21世纪的到来，人类步入信息社会，信息产业成为全球经济发展的主导产业，计算机科学与技术在信息产业中占据了重要的地位。
随着互联网技术的普及和推广，网络技术更是信息社会发展的推动力，人们在日常学习、生活和工作中都越来越依赖于网络，因此关于信息技术、信息安全技术、网络安全技术的发展成为越来越重要的学科。
互联网技术的发展改变了人们的生活，信息安全的内涵已发生了根本变化。
安全已从一般性的安全防卫，变成了一种非常普通的安全防范；从一种研究型的学科，变成了无处不在，影响人们学习、生活和工作的安全技术。
技术的普及也推动了社会对人才的需求，因此建立一套完整的网络安全课程教学体系，提供体系化的安全专业人才培养计划，培养一批精通安全技术的专业人才队伍，对目前高校计算机网络安全方向专业人才培养来说，显得尤为重要。
关于教材开发背景结合国家十二五本科计算机专业课程规划体系，深入领会教育部计算机科学与技术教学指导委员会编制的“计算机科学与技术专业规范的知识体系和课程大纲”文件精神，为及时反映目前网络安全专业学科发展动态，创新网络教材编辑委员会组织编写了本书。
希望本书中的网络安全知识内容，既重视理论、方法和标准的介绍，又兼顾技术、系统和应用分析，在内容结构和知识点布局上能有所创新。
此外，随着互联网技术的普及和推广，人们日常学习和工作依赖网络的比重增加，计算机网络安全的实施和防范技术，成为目前最为瞩目的学习内容。
因此，创新网络教材编辑委员会选择网络安全技术在生活中的具体应用作为教材开发主线，规划出面向实际工程案例，可操作、可应用、可实施的网络安全技术教程。
同时希望策划的安全技术直观、形象、具体、可实施，选编和策划的安全知识具有专业化、体系化、全面化特征，能体现和代表当前最新的网络安全技术发展方向。

<<网络安全防御技术实践教程>>

内容概要

本书主要针对高等院校计算机科学与技术、通信工程、计算机网络等相关专业，在计算机网络基础理论、网络安全基础理论学习完成之后，配套使用的网络安全实验教程。
本书介绍了在局域网组建过程中，使用的多项安全产品及相关技术，包括网络防火墙、IDS入侵检测系统、USG统一网关和综合网络安全实践教程。

本书分为4篇，按照局域网组建中使用到的网络安全产品，详细讲述了使用这些网络安全设备，解决实际生活中遇到的各种安全问题，包括网络防火墙应用技术、入侵检测系统应用技术、统一网关应用技术等，以及针对这些问题的解决方法。
本书在每个章节中对所使用到的相关安全产品的基本配置、基本界面、功能配置都给予了详细的讲解，以帮助读者熟悉产品的使用，并进一步诠释其在工程项目中的实施方法。

本书可作为高等院校计算机科学与技术、通信工程、计算机网络等相关专业本科生或研究生学习和研究网络安全产品及技术的实验教材，还可作为网络安全专业认证的培训教材，以及网络设计师、网络工程师、系统集成工程师以及其他专业技术人员在工作中遇到网络安全问题时的技术参考用书。

作者简介

黄传河，博士，武汉大学计算机学院教授、博士生导师。
主要研究方向为计算机网络（移动互联网、移动Ad Hoc网络、无线传感器网络、无线Mesh网络、WDM网络、网络互联），网络安全，分布并行处理，量子计算。

<<网络安全防御技术实践教程>>

书籍目录

章节摘录

插图：防火墙可以监控进出网络的通信量，从而完成看似不可能完成的任务：仅让安全通过验证的信息进入，同时又抵制对企业网络构成威胁的数据。
随着网络上安全性问题的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或选择了不合适的口令。
因此，防火墙的作用是防止恶意的、未授权的通信进出被保护的网络，迫使企业强化自己的网络安全政策。
防火墙的功能在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和Internet之间，或者内部网络之间的任何活动。
防火墙可以对网络之间的通信进行扫描，关闭不安全的端口，阻止外来的DOS攻击，封锁木马的传播路径等，以保证网络安全。
典型意义上的防火墙设备具有三个方面的基本特性：内部网络和外部网络之间的所有数据流都必须经过防火墙；只有符合安全策略的数据流才能通过防火墙；防火墙自身具有非常强的抗攻击免疫力。
内部网络和外部网络之间的所有网络数据流都必须经过防火墙。
这是防火墙所处网络位置的特性，同时也是一个前提。
因为只有当防火墙是内、外部网络之间通信的唯一通道，才可以全面、有效地保护企业网络不受侵害。
根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。
所谓网络边界即是采用不同安全策略的两个网络连接处，例如用户网络和互联网之间连接、和其他业务往来单位的网络连接、用户内部网络不同部门之间的连接等。
防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。
典型的防火墙体系网络结构如图1—2所示。
从图1—2中可以看出，防火墙的一端连接企事业单位内部的局域网，而另一端则连接互联网。
所有的内、外部网络之间的通信都要经过防火墙。
只有符合安全策略的数据流才能通过防火墙。
防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速地从一条链路转发到另外的链路上去。
从最早的防火墙模型开始谈起，原始的防火墙是一台“双穴主机”，即具备两个网络接口，同时拥有两个网络层地址。
防火墙将网络上的流量通过相应的网络接口接收上来，按照OSI协议栈的七层结构顺序上传，在适当的协议层进行访问规则和安全审查，然后将符合通过条件的报文从相应的网络接口送出，而对于那些不符合通过条件的报文则予以阻断。

编辑推荐

《网络安全防御技术实践教程》：教育部高等学校信息安全类专业教学指导委员会，中国计算机学会教育专业委员会共同指导。
通过全书提供的近40个安全技术实验的训练，帮助学生熟练掌握网络安全工程师所需要的基本实践技能。
书中全部内容都来自实际工程案例，所有实验操作都用日常安全需求作为主线串接知识，以问题解决过程作为核心，因此《网络安全防御技术实践教程》可以作为相关安全理论学习完成之后的实验补充，帮助学生加强对抽象安全理论的直观理解，也可以根据教学的实际情况，从中选择部分实验教学内容，要求学生完成适当数量和难度的实验来补充理论诠释知识的不足；还可以作为学生工作前专门的实训教学内容。

版权说明