<<安全网络构建>>

图书基本信息

书名：<<安全网络构建>>

13位ISBN编号：9787121121678

10位ISBN编号：7121121670

出版时间：2010-11

出版时间：电子工业出版社

作者：沈才梁 编

页数：229

前言

教育部[2006]16号文件明确指出，课程建设与改革是提高教学质量的核心，也是教学改革的重点和难点。
高等职业院校要积极与行业企业合作开发课程，根据技术领域和职业岗位（群）的任职要求，参照相关的职业资格标准，改革课程体系和教学内容。
本书教材编写组深入浙江绍兴及周边地区的中小企业及网络安全技术服务与营销企业，以网络安全构建和管理的岗位需求出发，以工作任务为导向，通过对工作岗位能力要求深入调研后，多次召开技术专家访谈会，从中提炼出具体的工作任务作为课程的子学习领域。
第二至第五子学习领域包含案例导入、讲授单元、行动单元、思考及训练四个部分，以必要的理论知识介绍为基础，重点讲授具体工作任务的完成。
工作任务选取突出实用，结合实际。
通过与国内知名信息安全企业天融信公司合作，由天融信公司提供真实案例及具体工作任务等资料，教材编写组的教师与企业专家共同提炼、选取典型的案例及工作任务，使教材具有高度的真实性和实用性，实现课堂与工作岗位的并轨对接。
在教材编写过程中，编写组从实际课程教学的需要出发，将课程教学内容、教学方法和教学组织体现在教材中，以便能够帮助教师及学生合理安排教学。
本书由沈才梁副教授主编，其中第一、第六子学习领域由毛颉、沈才梁编写，第二、第三子学习领域由袁思达、陈建成编写，第四子学习领域由陈令编写，第五子学习领域由杜焕强、黄叶珏编写，附录由俞立峰和阮胜利编写，参加编写和审校等工作的人员还有唐科萍、许方恒。
在本书编写过程中，得到了天融信杭州分公司、华正信息科技有限公司、杭州电子科技大学、温州职业技术学院、浙江建设职业技术学院等企事业单位和兄弟院校的大力支持。
在这里，特别向范炳华工程师、华海军高级工程师、李永平教授、吴坚副教授表示感谢！
由于编者水平有限和时间仓促，书中难免存在疏漏和不足，希望同行专家和读者能给予批评和指正。

<<安全网络构建>>

内容概要

本书从安全网络构建的角度，全面介绍了中小企业网络安全规划、设计及主要网络安全设备的配置和管理。
全书共七个部分，包括安全网络的初步设计、硬件VPN配置管理、硬件防火墙配置管理、入侵检测系统配置管理、入侵防御系统配置管理、安全网络构建及附录。

本书通过介绍国内主流安全厂商的系列产品，以中小企业网络安全的真实应用为例，详尽描述了常用安全产品的应用、选型、配置、管理和典型的网络安全解决方案设计流程。

本书理论与实践融为一体，适合理实一体化教学。

本书可作为高职高专计算机网络及相关专业的教材，也可作为相关技术人员的参考书或培训教材。

<<安全网络构建>>

书籍目录

章节摘录

插图：3.入侵检测技术入侵检测技术就是通过对数据的采集与分析实现入侵行为的检测的技术。
入侵检测系统（IDS）是进行入侵检测的软件和硬件的组合。
入侵检测系统是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。
它从计算机网络系统中的若干关键点收集信息，并分析这些信息，判断网络中是否有违反安全策略的行为和遭到袭击的迹象。
入侵检测系统被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。
4.认证技术在数据通信中，认证技术是非常重要的一项技术，是证实信息交换过程有效性和合法性的一种手段。
常用的认证技术有身份认证和报文认证。
身份认证：验证信息通信的双方是否是合法用户，证实客户的真实身份与其所声称的身份是否相符的过程，如常见的用户名和密码认证。
报文认证：主要是通信双方对通信的内容进行验证，以保证数据在通信过程中没有被修改。
5.访问控制技术访问控制技术是实现既定安全策略的系统安全技术。
根据安全策略的要求，访问控制对每个资源请求做出许可或限制访问的判断，可以有效防止非法用户访问系统资源和合法用户非法使用资源。
6.VPN（Virtual Private Network）技术VPN又称虚拟专用网，顾名思义就是在公共网络上建立的一条虚拟的专用网络链路。
所谓专用是指只有通过身份验证的用户账户才有权使用，即客户端通过服务器端提供的用户账户名和密码拨叫到VPN服务器，从而建立一条私有安全链路。
VPN以安全和私有的方法在Internet上传输数据时使用了两种技术：隧道技术和加密技术。
隧道技术是一种封装数据的方式，以这种方式封装的数据在Internet上是不可识别的，只有对用户端的网络可以识别，也就是说隧道是专用的，以保护远程用户或主机和专用网络之间的链接。
加密技术保证链接的安全，使数据在传输中不被第三者看到。
7.防病毒软件技术防病毒软件是最常见、最普遍的安全技术方案，主要功能是查杀病毒。
防病毒软件主要有两种：一种是针对单机用户的单机版软件；另一种是针对网络用户的网络版软件。
8.漏洞扫描技术漏洞扫描是指对重要计算机信息系统进行检查，发现其中可被黑客利用的漏洞。
漏洞扫描的结果实际上就是对系统安全性能的一个评估，它指出了哪些攻击是可能的，因此成为安全方案的一个重要组成部分。
漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。
通过使用漏洞扫描器，系统管理员能够发现所维护的服务器的各种TCP端口的分配、提供的服务、服务软件版本和这些服务及软件呈现在Internet上的安全漏洞，从而在计算机网络系统安全防护中做到有的放矢，及时修补漏洞。

<<安全网络构建>>

编辑推荐

《安全网络构建》：行业、企业专家参与教材编写，选取工作任务项目及典型案例，实现课堂教学与未来工作岗位的“短距离”对接。

版权说明