<<计算机网络安全基础与技能训练>>

图书基本信息

书名：<<计算机网络安全基础与技能训练>>

13位ISBN编号：9787560620435

10位ISBN编号：7560620434

出版时间：2008-7

出版时间：西安电子科技大学出版社

作者：吴献文 编

前言

计算机技术的飞速发展促进了网络的发展。
网络已经普遍存在于我们的生活、学习和工作环境中。
计算机网络的安全是网络可靠、稳定运行的保证，因此必须掌握网络的安全基础知识，学会如何安全使用，如何有效地保证、维护网络的安全，才能建立和维护一个有效的、满足要求的、安全的网络系统。
本书介绍了计算机网络安全的基础知识和常用的安全技术、安全策略，适应“以学生为中心”的教育思想，遵循学生的认知规律，由浅入深，由基础到专业、到实践，层层深入，并结合高职教育的特点，增强了实践动手的内容，弱化了理论部分，让学生在“学中做”，在“做中学”，更加适应学生自主学习和能力的培养。
编者总结多年的“计算机网络安全技术”课程教学经验，以安全技术案例为核心，采用引入、讲述、应用、疑难解析、知识拓展的模式，由浅入深，围绕实际案例展开对安全技术知识的介绍。
本书遵循“项目驱动＋案例教学”的教学模式，在案例的支持下展开对知识点的介绍。
本书在编写过程中十分注意教材内容的取舍和安排，具有以下主要特点：第一，教材内容以应用为中心。
采用“项目驱动”的编写方式，以实际项目引出相关的原理和概念；在实训过程中融入知识点，并通过实训思考、实训总结进行分析归纳，解决实训中出现的问题，提高学生动手能力以及发现问题、分析问题、解决问题的能力。
第二，教材内容以实用为目标。
不追求面面俱到，力求突出重点。
第三，采用“层次化”策略。
在项目驱动下，采用由浅入深、层次递进的方式，兼顾不同层次学生的需求，设有基本掌握部分和拓展部分。
第四，“模块化”教学。
教材编写时采用“模块化”思想，由基础知识和实训内容组成一个知识模块，真正实现“一体化教学”，边讲边练、讲练结合，而且学习节奏紧凑，老师讲完某一项技能或知识点，学生马上就练，练中出现了问题再看原理和知识点，然后再练，形成一个“讲—练—发现问题—再讲—再练—解决问题”的小循环，有利于学生自主学习能力的培养，增强学生学习的成就感，提高学习兴趣。
第五，面向课堂教学全过程设置教学环节，将知识讲解、技能训练和能力的提高有机结合起来。
除了第一章外，其余每一章都设有知识讲解与示范、实例、疑难解析、知识拓展、本章小结、思考与习题、实训等环节。
参与本书编写工作的人员都是长期从事计算机网络技术和计算机网络安全技术课程教学的一线教授和长期从事网络安全管理和维护的网络工程师，具有丰富的教学经验和实践经验。
本书由湖南铁道职业技术学院吴献文任主编，刘志成、毛春丽、龚娟任副主编。
第1章由龚娟编写，第2章由谢树新编写，第3章由言海燕编写，第4章由吴献文编写，第5章由薛志良编写，第6章由毛春丽编写，第7章由刘志成编写。
另外，张杰、颜谦和、周进等也参与了本书的校对、整理和修改工作，并提出了许多宝贵意见。
本书写作过程中也得到了西安电子科技大学出版社杨？
[编辑的大力支持和帮助，在此一并表示感谢。
由于作者水平有限，书中难免有不足之处，恳请读者批评指正。

内容概要

本书介绍了计算机网络安全的基础知识和常用的安全技术、安全策略，适应“以学生为中心”的教育思想，遵循学生的认知规律，由浅入深，由基础到专业、到实践，层层深入，并结合高职教育的特点，增强了实践动手的内容，弱化了理论部分，让学生在“学中做”，在“做中学”，更加适应学生自主学习和能力的培养。

本书共分为七个章节。

第1章是整本书的基础部分，从网络的脆弱性入手，介绍了网络安全的概念、策略、标准、基本模型、体系结构、安全机制与技术和网络安全法律法规等理论基础知识。

第2～7章分别介绍了病毒技术、黑客技术、加密技术、数字签名技术、防火墙技术和入侵检测技术等各项安全领域的专业技术，通过实例操作的方式详细阐述了每一种技术的应用。

本书可作为高职高专院校计算机专业的教材，也可供计算机爱好者参考借鉴。

本书配有电子教案，有需要的老师可与出版社联系，免费提供。

<<计算机网络安全基础与技能训练>>

书籍目录

章节摘录

3.网络管理人员的安全意识问题（1）保密观念不强或不懂保密规则，随便泄露机密。
例如，打印、复制机密文件，随便打印出系统保密字或向无关人员泄露有关机密信息。
（2）业务不熟练，因操作失误使文件出错或误发，或因未遵守操作规程而造成泄密。
（3）因规章制度不健全造成人为泄密事故。
如网络上的规章制度不严，对机密文件管理不善，各种文件存放混乱。
（4）素质差，缺乏责任心，没有良好的工作态度，明知故犯或有意破坏网络系统和设备。
（5）熟悉系统的工作人员故意改动软件或用非法手段访问系统或通过窃取他人的口令字和用户标识码来非法获取信息。
（6）身份被窃取，一个或多个参与通信的用户身份被别人窃取后非法使用。
（7）否认或冒充，否认参加过某一次通信，或冒充别的用户获得信息或额外的权力。
（8）担任系统操作的人员以超越权限的非法行为来获取和篡改信息。
（9）利用硬件的故障部位和软件的错误非法访问系统或对系统进行破坏。
（10）利用窃取系统的磁盘、磁带或纸带等记录载体或利用废弃的打印纸、复写纸来窃取系统或用户的信息。

编辑推荐

版权说明