<<计算机网络安全技术>>

图书基本信息

书名：<<计算机网络安全技术>>

13位ISBN编号：9787811238587

10位ISBN编号：7811238586

出版时间：2010-1

出版时间：清华大学出版社有限公司

作者：范荣真 编

页数：261

前言

计算机网络成为当前社会发展的重要推动力。
社会经济发展、国防信息建设以及与人们生活息息相关的各行各业，对计算机网络的依赖程度都不断增大。
计算机网络给人们带来便利的同时，也带来了保证信息安全的巨大挑战。
如何使信息不受黑客的入侵，如何保证计算机网络不间断地工作并提供正常的服务，是各个组织信息化建设必须考虑的重要问题。
本书着重于从应用的角度介绍计算机网络安全，使读者了解一般网络安全的基础理论及技术原理，从实训中认识、理解什么是网络安全，并掌握常用的安全应用技术。
全书共8章，第1章主要介绍计算机网络安全的相关概念及计算机网络的安全体系结构。
第2章主要介绍计算机操作系统的安全基础与防范措施，包括：操作系统的安全机制及安全级别、操作系统安全技术。
第3章主要介绍计算机病毒防范技术，包括：计算机病毒的工作原理和分类、计算机病毒的检测和防范技术、各种防治病毒软件的使用。
第4章主要介绍信息加密技术，包括：加密体系；单钥加密和双钥加密算法；链路、节点、端到端加密；公钥架构。
第5章主要介绍防火墙技术，包括：防火墙体系结构、包过滤防火墙和应用代理防火墙，以及防火墙的应用。
第6章主要介绍电子商务的安全性，包括电子商务的安全需求分析、电子商务采取的安全措施。
第7章主要介绍网络黑客的攻击与防范，包括：黑客常用的各种攻击工具及攻击步骤、各种常用的防黑客的方法与工具的使用。
第8章主要介绍常用网络安全的策略。
本书涉及的内容操作性比较强，在学习时，可多安排学生的实训操作课时，加强实训的监督，并要求学生认真写好实训报告。
对书中一些理论如需进一步加深理解的，应该指导学生参阅相应的参考书。
本书由范荣真任主编，王文、阚晓初任副主编。
范荣真编写第3章、第4章、第5章、第7章，王文编写第1章、第2章，阚晓初编写第6章、第8章。
本书在取材上着重培养和强化学生的实践能力与应用能力，加强了实训内容的编写，在理论上取精而且简单明了。
本书特别突出了各项技术的应用，希望能贴近高职高专学生的学习特点，从而激发起学习兴趣，在实践中提高其对计算机网络安全的应对与控制能力。
网络安全是一门涉及计算机科学、通信技术、密码技术、应用数学等多门学科的交叉学科。
在应用上由于网络安全技术和产品发展很快，因此这本书的编写思想是，理论讲解简洁化，应用实例新颖化，操作步骤详细化，以实训引导学生理解理论，从而达到应用的目的。
当然，在采用本书做实验时，也可根据具体情况采用熟悉的实例。
由于编写水平及时间所限，书中难免有疏漏之处，恳请广大专家和读者批评指正。

<<计算机网络安全技术>>

内容概要

本书全面介绍了计算机网络安全的基础知识、基本理论，以及计算机网络安全方面的管理、配置与维护。
全书共8章，包括：网络安全概述、操作系统安全配置、网络病毒与防治、信息加密技术、防火墙配置与管理、电子商务网站安全、黑客的攻击与防范、网络安全策略。
本书主要以网络安全技术实训为主，以操作应用软件来引导学习。
本书可作为高职高专计算机专业及相关专业教材，也可作为相关技术人员的参考书或培训教材。

<<计算机网络安全技术>>

书籍目录

章节摘录

插图：4.客体重用在计算机输出信息系统可信计算基的空闲存储客体空间中，对客体初始指定、再分配一个主体之前，撤销该客体所含信息的所有授权。
当主体获得对一个已释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。
5.审计计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它的访问或破坏活动。
可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（如打开文件、程序初始化）；删除客体；由操作员、系统管理员和（或）系统安全管理员实施的动作及其他与系统安全有关的事件。
对于每一事件，其审计记录包括：事件的日期和时间、用户事件类型、事件是否成功。
对于身份鉴别事件，审计记录包含来源（如终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。
对不能由计算机信息系统可信计算基独立辨别的审计事件，审计机制提供审计记录接口，可由授权主体调用。
这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录。
6.强制访问控制计算机信息系统可信计算基对所有主体及其所控制的客体（例如，进程、文件、段、设备）实施强制访问控制，为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的事实依据。
计算机信息系统可信计算基支持两种或两种以上成分组成的安全级别。
计算机信息系统可信计算基控制的所有主体对客体的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级非等级类别包含了客体安全级中的非等级类别，主体才能写一个客体。
计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。
7.标记计算机信息系统可信计算基应维护与主体及其控制的存储客体（例如，进程、文件、段、设备）相关的敏感标记，这些标记是实施强制访问的基础。
为了输入未加安全标记的数据，计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。
8.隐蔽信道分析系统开发者应彻底隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。
9.可信路径当连接用户时（例如，注册、更改主体安全级），计算机信息系统可信计算基提供它与用户之间的可信通道路径。
可信路径上的通信能由该用户或计算机信息系统激活，且在逻辑上与其他路径上的通信相隔离，并能正确地加以区分。

编辑推荐

《计算机网络安全技术》：面向“十二五”高职高专规划教材·计算机系列

<<计算机网络安全技术>>

版权说明