<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787801779700

10位ISBN编号：7801779703

出版时间：2007-8

出版时间：《计算机网络安全》编委会、刘三满、孙学农、 李大友 中国计划出版社 (2007-08出版)

<<计算机网络安全>>

内容概要

《计算机网络安全》覆盖内容包括硬件安全、操作系统安全、数据加密安全、局域网安全、防火墙及VPN技术、计算机病毒及安全防护等方面，其宗旨为从各个方面杜绝网络安全隐患，完善网络安全机制。
从个人、企业和世界发展方向论证了网络时代安全性的重要和对任何可能造成风险的因素进行初步的解析，增进对网络安全重要性和实用性的了解。
《计算机网络安全》即可作为高等院校相关课程的教材，也可作为高职高专、培训机构的教学用书。

<<计算机网络安全>>

书籍目录

章节摘录

版权页：插图：应用系统安全是动态的、不断变化的：应用的安全涉及面很广，以目前Internet上应用最为广泛的E-mail系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的Bug是很少有人能够发现的，因此一套详尽的测试软件是必须的。
但是应用系统是不断发展且应用类型是不断增加的，其安全漏洞也是不断增加且隐藏越来越深。
因此，保证应用系统的安全也是一个随网络发展不断完善的过程。
应用的安全性涉及到信息和数据的安全性：信息的安全性涉及到机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。
由于局域网跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。
对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。
5.管理安全风险分析管理是网络中安全最最重要的部分。
责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。
责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工，甚至外来人员进入机房重地，或者员工有意无意泄漏他们所知道的一些重要信息，而管理上却没有相应制度来约束。
当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。
同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。
这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。
建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

编辑推荐

《计算机网络安全》主要内容包括网络安全基础知识、操作系统安全、网络通信安全、Web安全、数据安全、病毒及其预防、黑客攻击与防范、防火墙技术、有关网络安全的法律法规。
系列教材特色：定位明确，有的放矢，在充分调研高等院校计算机教育现状与IT相关行业需求的基础上，明确以“实际应用能力”培养为目标。
校企结合，模式先进，由高等院校与IT企业的一线工程师／技师共同编写，将各院校已有教学经验与企业实际项目紧密结合。
资源丰富，方便教学，《计算机网络安全》配有电子教案、素材库、多媒体课件及模拟考试题等相关资源，建设立体化教材服务体系。

<<计算机网络安全>>

版权说明