<<网络安全技术理论与实践>>

图书基本信息

书名：<<网络安全技术理论与实践>>

13位ISBN编号：9787302281924

10位ISBN编号：7302281920

出版时间：2012-6

出版时间：清华大学出版社

作者：廉龙颖 编

页数：278

字数：446000

<<网络安全技术理论与实践>>

内容概要

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》全面地介绍了计算机网络安全的总体情况和发展趋势。
全书分为15章，全面讲述网络安全的基础知识（网络安全概述和网络安全编程基础），网络安全攻击技术（黑客与隐藏ip技术，网络扫描与网络监听，网络攻击，网络后门与清除日志，计算机病毒的防治），网络安全防御技术（操作系统安全配置方案，防火墙技术，入侵检测，信息加密与认证技术，无线网络安全）及网络安全工程（网络安全管理，网络安全方案设计）。

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》基本概念清晰，表达深入浅出，内容翔实，重点突出，理论与实践相结合，实用性强，易于教学。

《21世纪高等院校计算机网络工程专业规划教材·网络安全技术理论与实践》可作为信息安全、计算机、网络工程等专业本科生的教科书，也可供从事相关专业教学、科研和工程的人员参考。

<<网络安全技术理论与实践>>

书籍目录

章节摘录

版权页：插图：1.5 网络安全的评估标准为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在20世纪90年代提供了网络安全性标准（DoD5200.28-STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria，TCSEC），也叫橘黄皮书（Orange Book）。
该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。
安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序进行了安全描述。
目前，TCSEC已经成为了现行的网络安全标准。
TCSEC将网络安全性等级划分为A、B、C、D4类共7级，其中，A类安全等级最高，D类安全等级最低。
1.D级D级也称为酌情安全保护，是可用的最低安全形式。
该标准说明整个系统都是不可信任的。
对硬件来说，没有任何保护，操作系统容易受到损害，对于用户和他们对存储在计算机上信息的访问权限没有身份认证。
2.C1级C级有两个安全子级别，即Cl和C2，也称为自选安全保护系统，它描述了一个UNIX系统上可用的级别。
对硬件来说，存在某种程度的保护，因为它不再那么容易受到损害，尽管这种可能性存在。
用户必须通过用户注册名和口令系统识别自己，用这种方式来确定每个用户对程序和信息拥有什么样的访问权限。
3.C2级除Cl级包含的特征外，C2级还包括其他的创建受控访问环境的安全特性，该环境具有进一步限制用户执行某些命令或访问某些文件的能力。
这不仅基于许可权限，而且基于身份验证级别，另外，这种安全级别要求对系统加以审核，审核可用来跟踪记录所有与安全有关的事件，比如哪些是由系统管理员执行的活动。
4.B1级B级也称为被标签的安全性保护，分为三个子级别。
Bl级或称为标准安全保护，是支持多级安全的第一个级别，这一级说明了一个处于强制性访问控制之下的对象，不允许文件的拥有者改变其许可权限。
5.B2级B2级也称为结构保护，要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别。
这是提出的较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。
6.B3级B3级也称为安全域级别，使用安装硬件的办法来加强域，例如，内存管理硬件用来保护安全域免遭无授权访问或其他安全域对象的修改。

编辑推荐

《21世纪高等院校计算机网络工程专业规划教材:网络安全技术理论与实践》由清华大学出版社出版。

版权说明