<<计算机系统安全教程>>

图书基本信息

书名：<<计算机系统安全教程>>

13位ISBN编号：9787302226185

10位ISBN编号：7302226180

出版时间：2010-11

出版时间：清华大学出版社

作者：曹天杰　等编著

页数：262

<<计算机系统安全教程>>

前言

随着计算机的广泛应用，以计算机为核心的信息系统安全问题越来越突出，如何采取有效的措施保护计算机系统安全，是目前各国都面临的问题。
本书具有完善的知识体系，概念清晰，讲解详细。
本书具有以下特色：（1）内容全面，层次分明。
从计算机系统的不同层次，介绍了各层次中的安全威胁及防范措施，覆盖了计算机系统安全涉及的各方面内容。
主要包括系统安全（操作系统安全、数据库安全）、网络安全（漏洞检测、攻击与防范、防火墙、系统入侵检测与防御）、应用安全（电子邮件安全、IP安全、web安全）。
（2）强调信息保障与纵深防御。
无论攻击和防守，对信息安全来说都是过程，信息安全是否成功关键在于对过程的把握。
从纵深防御保护的角度分析了信息保障中的保护、检测、响应和恢复。
如认证、防火墙起到边界保护的作用，扫描器、入侵检测系统、蜜罐则是检测工具，入侵防御系统属于响应工具。
（3）注重理论与实践相结合，强调实用。
在介绍理论知识的基础上，注重实践能力的培养，如第5章从理论到实践，介绍了漏洞的概念、漏洞的分类、漏洞标准库、漏洞扫描的原理、漏洞扫描的工具、扫描器的实现。
本书共分为11章：第1章是绪论；第2章介绍实现安全服务的各种方法；第3章与第4章分别介绍了操作系统安全、数据库安全；第5章介绍系统漏洞及检测；第6章介绍网络攻击与防范；第7章与第8章分别介绍了防火墙、系统入侵检测与防御；第9～第1l章介绍了电子邮件安全、IP安全、Web安全。
其中第3～第5章由李琳编写，第9～第11章由黄石编写，其余各章由曹天杰编写，全书由曹天杰负责统稿。

<<计算机系统安全教程>>

内容概要

本书全面而又系统地讲述了计算机系统安全的基本知识。
本书注重理论与实践相结合，条理清晰。
围绕认证、访问控制、机密性、完整性、可用性、不可否认性、安全审计与报警等安全服务的实现，介绍了系统安全、网络安全、应用安全各个层次计算机系统可能面临的威胁与防范措施，从纵深防御的角度分析了信息保障中的保护、检测、响应和恢复等方面的知识。

本书主要内容包括：绪论、实现安全服务、操作系统安全、数据库安全、漏洞检测、攻击与防范、防火墙、系统入侵检测与防御、电子邮件安全、ip安全、web安全。

本书可以作为信息安全专业、信息对抗专业、计算机科学与技术专业、网络工程专业或其他相关专业的本科生和研究生教材，也可以作为信息系统安全领域的从业人员参考书。

<<计算机系统安全教程>>

书籍目录

章节摘录

插图：1.2.1 安全策略安全策略是指在一个特定的环境里（安全区域），为了保证提供一定级别的安全保护所必须遵守的一系列条例和规则。
例如，可以将安全策略定义为：系统中的用户和信息被划分为不同的层次，一些级别比另一些级别高。
当且仅当主体的级别高于或等于客体的级别，主体才能读访问客体；当且仅当主体的级别低于或等于客体的级别，主体才能写访问客体。
一种安全策略实质上表明所涉及的系统在进行一般操作时，在安全范围内什么是允许的，什么是不允许的。
策略通常不作具体规定，它只是提出什么是最重要的，而不确切地说明如何达到所希望的这些结果。
安全策略都建立在授权的基础之上，一般按授权性质的不同区分不同的策略。
在安全策略中包含对“什么构成授权”的说明。
在一般性的安全策略中可能写有“未经适当授权的实体，信息不得给予、不被授权、不允许引用、任何资源也不得为其使用”。
按照所涉及的授权的性质可将策略分为三种，基于规则的策略、基于身份的策略、基于角色的策略。
基于身份的安全策略使用建立在不多的一般属性或敏感类之上的规则，它们通常是强加的。
它的基础是用户的身份和属性以及被访问的资源或客体的身份和属性。
在一定程度上与“必须认识”的安全观念相当。
它的目的是过滤对数据或资源的访问。
基本上有两种执行基于身份的策略的方法，将有关访问权的信息视为访问者所拥有，或是视为被访问数据的一部分。
前者的例子为特权标识或权力，给予用户并为代表该用户进行活动的进程所使用，后者的例子为访问控制表。
这两种情况下，数据项的大小可以有很大的变化（从完整的文件到数据元素），这些数据项可以按权力命名，或带有它自己的访问控制表。
基于规则的安全策略涉及建立在特定的、个体化属性之上的授权准则，假定某些属性与被应用实体永久相关联，而其余属性可以是某种占有物（如权力），它们可传送给另外的实体。
它的基础是强加于全体用户的总安全策略，是为了以最小的代价，保证信息系统的安全，使信息系统发挥最大的效益。
基于规则的安全策略中的授权通常依赖于敏感性。
在一个安全系统中，数据或资源应该标注安全标记。
代表用户进行活动的进程可以得到与其原发者相应的安全标记。

编辑推荐

《计算机系统安全教程》：21世纪高等学校信息安全专业规划教材。

<<计算机系统安全教程>>

版权说明