<<CISSP认证考试权威指南>>

图书基本信息

书名：<<CISSP认证考试权威指南>>

13位ISBN编号：9787302215370

10位ISBN编号：7302215375

出版时间：2010-1

出版时间：清华大学出版社

作者：（美）迈克尔，（美）泰特尔，（美）查佩尔 著，梁志敏 译

页数：635

译者：梁志敏

前言

本书为读者提供了信息系统安全专家认证(Certified lnformation Systems SecurityProfessional，CISSP)考试的完备基础知识。
购买本书表示你愿意学习和进一步了解CISSP考试要求掌握的技能。
本部分概述了本书与CISSP考试的内容。
本书是专门为参加CISSP认证考试的读者和学生编写的。
如果你有志成为一名通过认证的安全专家，那么CISSP认证和这本学习指南就非常适合你。
本书的目的就是要帮助你为通过CISSP认证考试做好充分的准备。
在开始阅读本书之前，你需要先独自完成一些工作。
你应当对IT及安全性有大致的了解，应当在CISSP考试所覆盖十个领域中的某个领域具有5年的工作经历(或4年的工作；经历加上大学学位)。
根据(ISC)2，如果你具有参加CISSP考试的资格，那么可以使用本书充分地准备CISSP考试。
接下来将介绍有关(ISC)2的更多信息。
(ISC)2 CISSP考试由国际信息系统安全认证协会(International Information Systems SecurityCertification Consortium，(ISC)2)管理。
(ISC)2是一个全球性的非赢利性组织，该组织具有四个主要的目标：为信息系统安全领域维护公共知识体系(CommonBodyofKnowledge，CBK)。
为信息系统安全专业人士和从业人员提供认证。
指导认证培训和管理认证考试。
通过连续的教育培训，对有资格的认证候选人的鉴定工作进行管理。
(ISC)2由董事会运作，董事会成员从通过认证的从业人员中按级别选举产生。

<<CISSP认证考试权威指南>>

内容概要

获得CISSP认证将显示您的职业资历，增强您在IT安全领域的可信度和职场竞争力。
本书由三位安全认证专家联袂撰写，通过列举多个真实场景、提供书面练习并全面介绍CISSP考试的公共知识体系，使您不仅拥有了应试利器，还可以掌握得心应手地履行本职工作所需的技能。
这本最新的必备指南涵盖访问控制、业务连续性、密码术、生物测定学和软件安全测试等重要主题，还列出了如何顺利通过考试的实用建议。
本书内容如下：　　全面系统地覆盖所有考试目标，是您必备的优秀考试指南。
实用的“动手练习”帮您巩固关键技能。
“真实场景”将您所学的理论知识运用于实际工作中。
每章的“复习题”极富挑战性，可用于为考试热身。
每章的“应试要点”列出参试前必须熟练掌握的要点，这是本书的一个鲜明特色。
本书末尾的易撕考点卡详细列出所有官方考试目标，指出每个目标对应的章号，以便您对照每个目标跟踪备考情况。

作者简介

James Michael Stewart，信息系统安全认证专家，从事写作与培训工作已有14年之久，其作品始终与最新的安全热点相结合。
他教授许多CISSP培训课程，此外，还参加众多与Windows安全性和Certified Ethical Hacker认证相关的会议。
Michael的一些著作和教材主要涉及安全认证、Microsoft专题以及网络管理。
读者可以在其Web站点www．impactonline．com上了解到Michael的更多信息。
Ed TiEel，从事自由职业的作家、培训师和顾问，精通信息安全、标记语言与网络连接技术的相关知识。
他是许多Tech Target站点的定期撰稿人，与HP. Sony和Motorola等许多公司合作，讲授联机安全和技术课程，并且定期为Tom's Hardware站点提供稿件。
读者可以在其Web站点www.edtittel.com上了解到Ed的更多信息。
Mike Chapple，信息系统安全认证专家，Notre Dame大学的IT安全专家。
曾任Brand Institute的首席信息主管以及美国国家安全局和美国空军的信息安全研究员。
Mike的主要专业领域包括网络入侵检测和访问控制，他是Tech Target Search Security站点的长期撰稿人，Information Security杂志的技术编辑。
Mike编著了一些与信息安全相关的著作，包括Wiley出版社发行的The GSEC Prep Guide以及Jonesand Bartlett Publishers出版社发行的Information Security Illuminated。

<<CISSP认证考试权威指南>>

书籍目录

章节摘录

插图：（1）“操作者的动作”和“操作者的位置”除了上述三种常见的身份验证因素之外，至少还有其他两个因素值得注意。
第一个因素是“操作者的动作（something you do）”，例如，书写签名、键入密码短语（击键力度）或者讲出短语。
“操作者的动作”常常包含在“操作者的身份”或类型3中。
另外一个值得注意的因素是“操作者的位置（somewhere you are）”，例如，操作者登入的计算机终端、操作者进行连接操作的电话号码（通过呼叫者的ID标识）或国家（通过IP地址标识）。
通过物理位置控制访问时，主体必须存在而非远程连接。
“操作者的位置”常常包含在“操作者所具有的物品”或类型2中。
（2）逻辑位置逻辑位置能够将“操作者的位置”、“操作者所拥有的物品”和“操作者知道的内容”这几种概念结合在一起。
逻辑位置（logical location）访问控制在某些逻辑身份标识（如IP地址、MAC地址、客户类型或所用协议1的基础上约束访问。
不过请注意，因为使用黑客工具能够伪造任何类型的地址信息，所以逻辑位置访问控制应当不是唯一的身份验证因素。
我们还可以在日期和时间的基础上约束访问，也可以按照事务类型约束访问。
前者阻止指定时间周期之外的访问；后者则是一种与内容或上下文相关的访问控制，此时访问基于主体尝试的事务而动态变化。
（3）多因素身份验证当需要使用两个不同的因素都来提供身份验证时，就会出现双因素身份验证（two factor authentication）。
例如，你在杂货店用支票付账时，通常需要提供你的驾照（“操作者所拥有的物品”）和你的电话号码（“操作者知道的内容”）。
强身份验证只不过是需要两个或多个因素的任何身份验证，而且这些因素不必属于不同的类型。
不过一般说来，如果组合不同类型的因素，那么合成的身份验证就更安全。
双因素身份验证背后的概念是：如果组合使用两个相同的因素，那么系统的强度并不会超过只单独使用其中一个因素的系统的强度。
更确切地说，只要攻击能够窃取或获得特定因素的一个实例，那么相同的攻击就能够窃取或获得特定因素的所有实例。
例如，同时使用两个密码并不比只使用一个密码更安全，这是由于如果密码破解攻击能够成功破解一个密码，那么这种攻击就能够破解两个密码。
不过，使用两个或多个不同的因素时，两个或多个不同的攻击类型或攻击方法要想成功，就必须收集所有相关的身份验证元素。
例如，如果一个令牌、一个密码和一个生物测定学因素共同被用于身份验证，那么只有在偷窃物品、破解密码与生物测定学复制攻击同时成功的情况下才能进入指定系统。
一旦提供的身份标识和身份验证因素的登录凭证被提交给系统，那么系统就会将它们与系统中的身份标识数据库进行核对。
如果定位到身份标识并且提供的身份验证因素也正确，那么主体就通过了身份验证。

编辑推荐

《CISSP认证考试权威指南(第4版)》提供包括多个真实场景，提供丰富的习题，还配备了光盘。
光盘中的前沿备考软件包含：自定义测验引擎PDF格式的英文版电子书两套包含250道题的标准模拟试题可以运行在PC、掌上电脑或Palm掌上设备上的用于辅助记忆的电子抽认卡

版权说明