(ISC)² Official Study Guide

安全技术经典译丛

CISSP

CISSP®

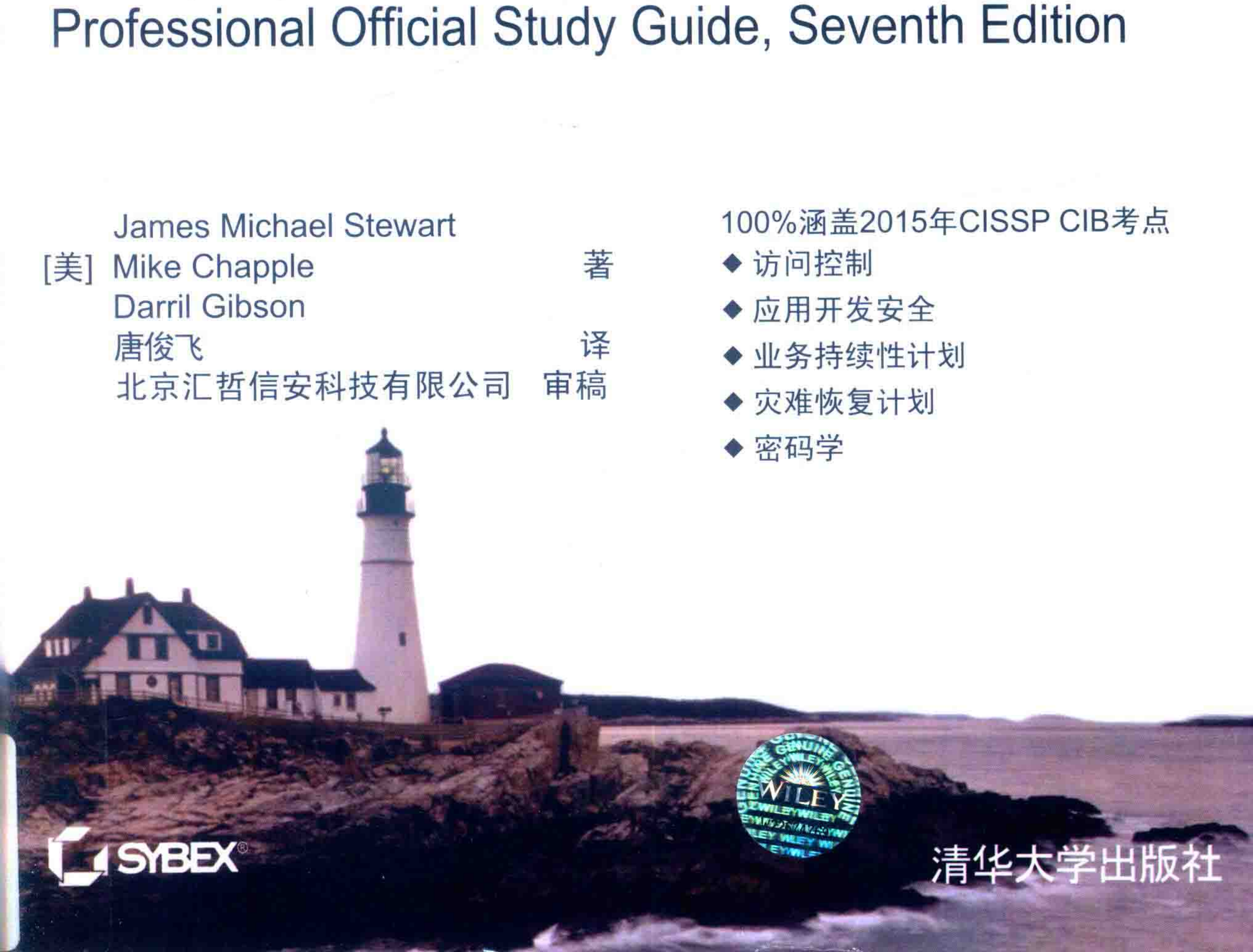
官方学习指南(第7版)

CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, Seventh Edition

James Michael Stewart
[美] Mike Chapple 著
Darril Gibson
唐俊飞 译
北京汇哲信安科技有限公司 审稿

100%涵盖2015年CISSP CIB考点

- ◆ 访问控制
- ◆ 应用开发安全
- ◆ 业务持续性计划
- ◆ 灾难恢复计划
- ◆ 密码学



SYBEX®
清华大学出版社

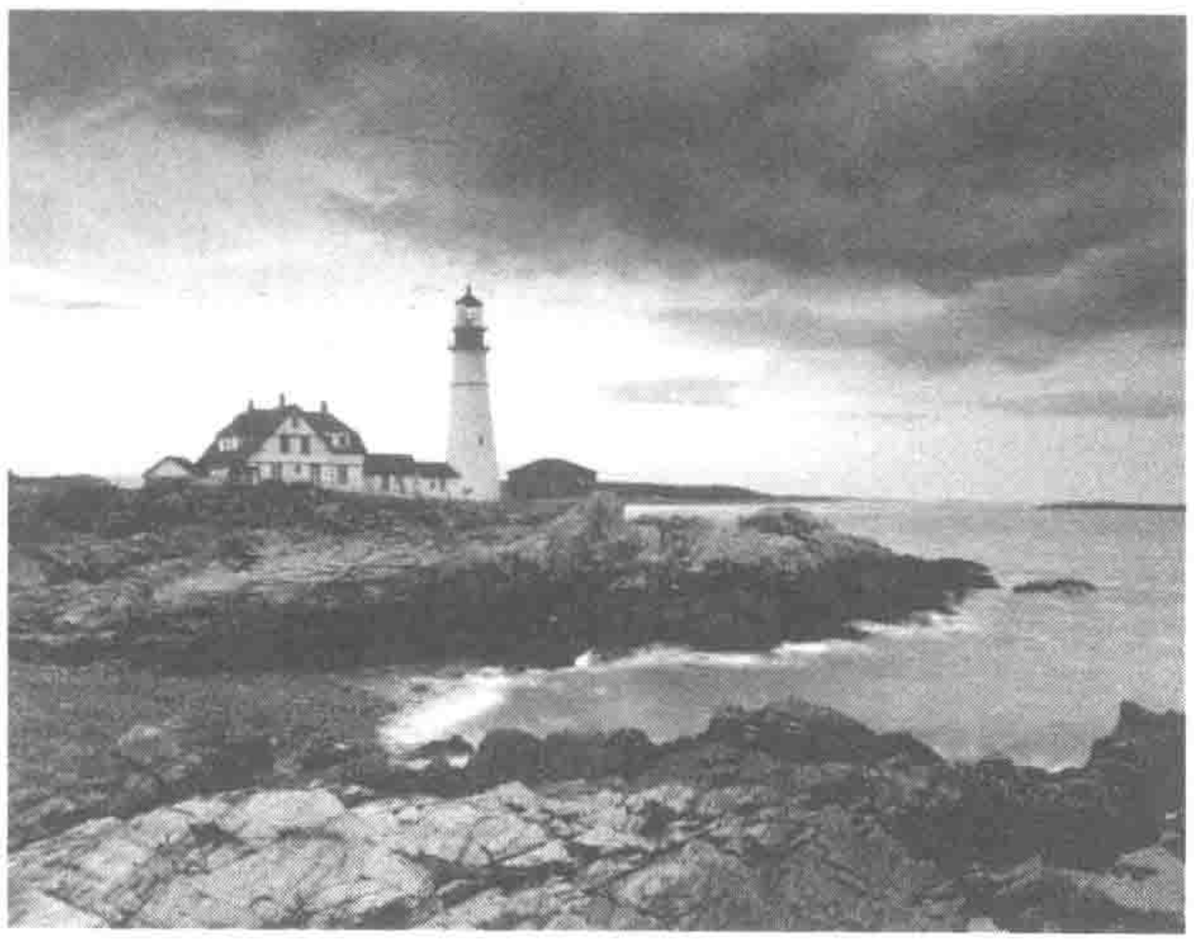
安全技术经典译丛

CISSP 官方学习指南

(第 7 版)

[美] James Michael Stewart
Mike Chapple
Darril Gibson 著

唐俊飞 译



清华大学出版社

北 京

James Michael Stewart, Mike Chapple, Darril Gibson
CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, Seventh Edition
EISBN: 978-1-119-04271-6

图书在版编目(CIP)数据

CISSP 官方学习指南：第 7 版 / (美)詹姆斯 • M. 斯图尔特(James M. Stewart)，(美)迈克 • 查普勒(Mike Chapple)，(美)戴瑞尔 • 吉布森(Darril Gibson) 著；唐俊飞 译. —北京：清华大学出版社，2017
(安全技术经典译丛)
书名原文：CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, Seventh Edition
ISBN 978-7-302-45933-0

Ⅰ. ①C… Ⅱ. ①詹… ②迈… ③戴… ④唐… Ⅲ. ①信息系统—安全技术—资格考试—指南
Ⅳ. ①TP309-62

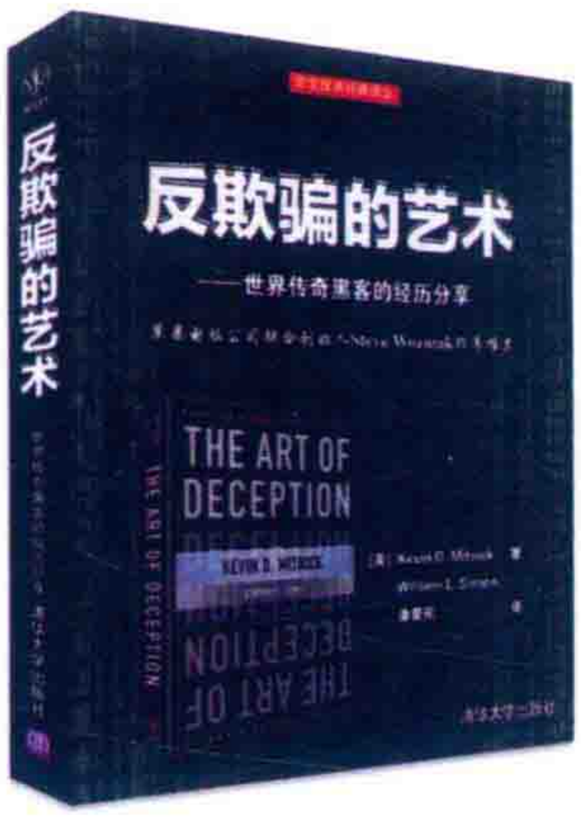
中国版本图书馆 CIP 数据核字(2017)第 040028 号

责任编辑：王　军　李维杰
装帧设计：孔祥峰
责任校对：曹　阳
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：51.5　　**字　　数**：1431 千字
版　　次：2017 年 4 月第 1 版　　**印　　次**：2017 年 4 月第 1 次印刷
印　　数：1～5000
定　　价：128.00 元

产品编号：070541-01

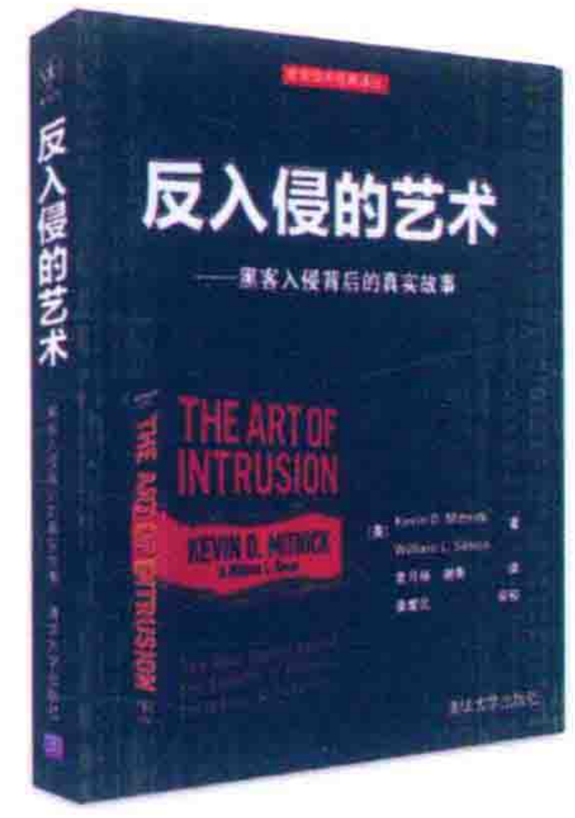
安全技术经典译丛



[美] Kevin D. Mitnick 著
William L. Simon
潘爱民 译

反欺骗的艺术——世界传奇黑客的经历分享

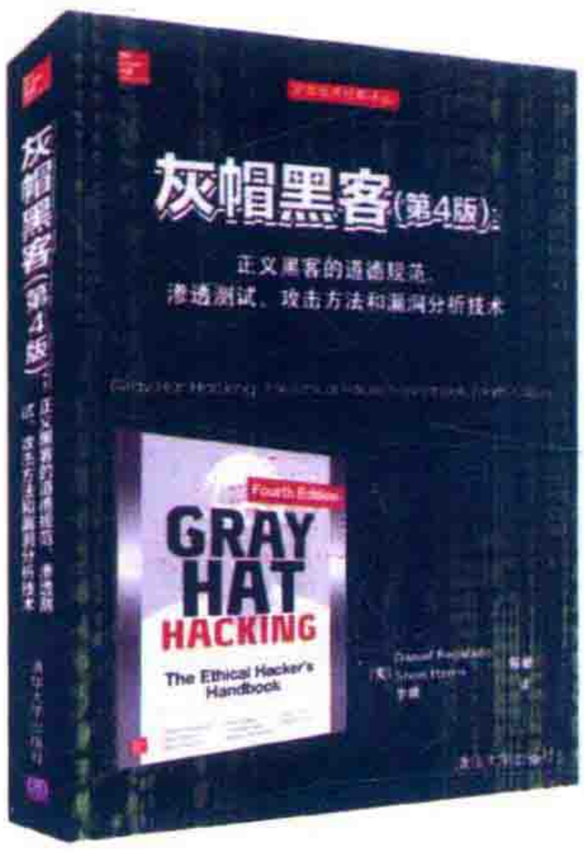
一部充满智慧的佳作！如同清晰的路标，可帮助政府、个人和企业弄清入侵者的手段，正确地检测、防范和应对威胁，并挫败其阴谋。本书还列出许多指导规则，为企业开发安全规程、培训计划和安全手册提供参考。



[美] Kevin D. Mitnick 著
William L. Simon
袁月杨 谢衡 译

反入侵的艺术——黑客入侵背后的真实故事

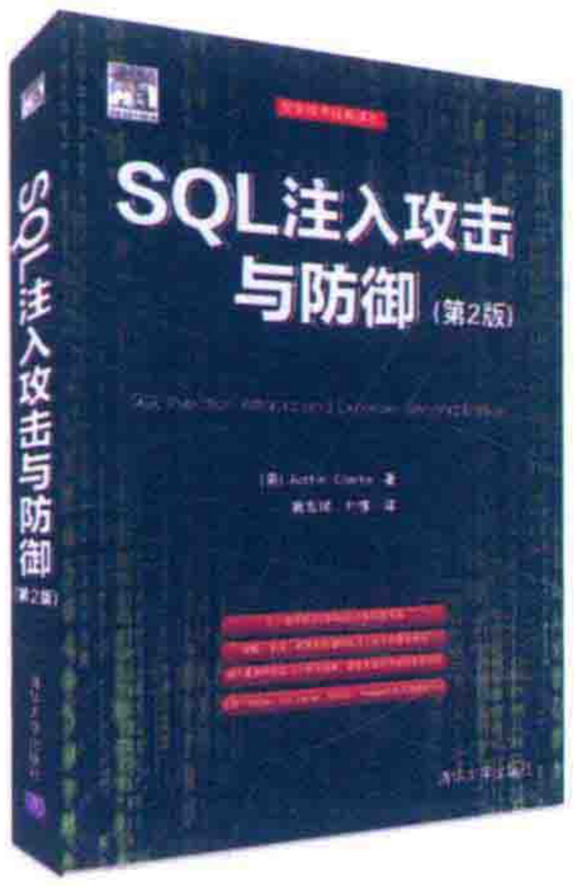
早已金盆洗手的著名黑客Kevin D. Mitnick将其一生积累下来的丰富技能汇集成书，使大家免受黑客攻击！本书列出入侵案例和对策，在每一个故事的后面，Mitnick都进行了专业的分析——攻击行为其实是可以防范的！



[美] Daniel Regalado 等著
Shon Harris
李枫 译

灰帽黑客(第4版)：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术

多位安全专家披露的久经考验的安全策略助你加固网络并避免数字灾难。本书分析敌方当前的武器、技能和战术，提供切实有效的补救措施、案例研究和可部署的测试实验，并揭示黑客们如何获取访问权限、攻击网络设备、编写和注入恶意代码及侵占Web应用程序和浏览器。这个与时俱进的知识宝库也透彻讲解Android漏洞攻击、逆向工程技术和网络法律等主题。



[美] Justin Clarke 著
施宏斌 叶愫 译

SQL注入攻击与防御(第2版)

本书深入探讨SQL注入问题。讲述一些最新研究成果，包括如何在移动设备上利用SQL注入漏洞，以及客户端SQL注入等。本书由一批SQL注入专家撰写，他们对Oracle、SQL Server、MySQL和PostgreSQL平台的SQL注入问题具有独到的见解。

译 者 序

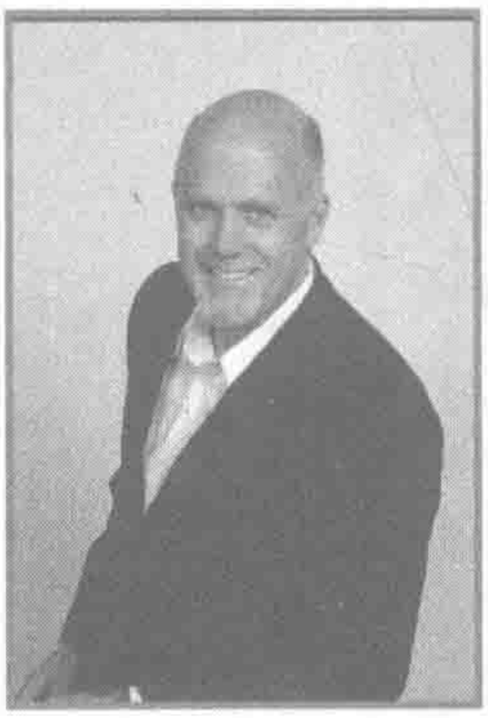
毫无疑问，CISSP(Certified Information Systems Security Professional)认证是信息安全领域最受全球广泛认可的 IT 安全认证，一直以来被誉为业界的“金牌标准”。CISSP 认证不仅是对个人信息安全专业知识的客观评估，也是全球公认的个人成就标准。

自 2015 年 4 月 CISSP 改版以来，国内一直缺乏配套的中文教材供大家学习。CISSP 备考学员大多是企业的中流砥柱，肩负着企业信息安全的重任，工作日程繁密，并且许多人也有了家庭的责任，学习时间非常之紧。我在汇哲科技任职 CISSP 主讲培训师多年，能深刻地体会到学习者的困境，并由此激发了要翻译一本优秀中文教材的决心。通过各方面的对比并结合多年的教学经验，我最终选择了《CISSP 官方学习指南(第 7 版)》(*CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide, Seventh Edition*)进行翻译。本书是(ISC)^2 出版的唯一官方 CISSP 备考辅导书，也是唯一紧贴 2015 年 CISSP 改版后 8 大知识域的“官方学习指南”，具有很强的权威性和指导性。

在图书的翻译和校勘过程中，得到了清华大学出版社的大力支持，也收到了汇哲科技 CISSP 学员提供的大量信息和建议。为此我对大家表达诚挚的感谢！最后，衷心希望本书能帮助大家自信而有效地完成 CISSP 备考，成功通过 CISSP 考试！

译 者

序



每当我们展望未来，我们必须先回头看看我们来自何处。早在 1989 年，(ISC)² 由少数充满激情的志愿者建立，他们想为新概念创建一组标准，目前还没有成熟的职业领域能被称为信息安全。在这些志愿者的心目中，让最初的 500 名申请者注册参加 CISSP 认证考试被认为是相当成功的。他们几乎没有想象到：26 年后不仅人数会从 500 名申请者增长为来自超过 160 个国家的 10 万名 CISSP 证书持有人，并且 CISSP 也将成为信息安全行业的标准认证。

技术的进步带来了更新的需要，而且我们不知疲倦地工作来确保我们的内容与行业密切相关。随着信息安全行业继续转型，以及网络安全成为全球焦点，CISSP 公共知识体系(CBK)与今天的挑战更加密切相关。

新版的(ISC)²《CISSP 官方学习指南(第 7 版)》是齐心合作以加强和提升我们的教育和培训水平的一部分。本书反映了我们不断变化的领域中最相关的主题，并且是(ISC)² 认证考试候选人的学习工具，针对 8 个 CISSP 知识域和行业中最新的主题提供了全面的学习指南。

如果正在获得认证的道路上，你毫无疑问听说过 CBK 的(ISC)²《CISSP 认证学习指南》。虽然是公共知识体系的权威参考，但本书是学习工具，集中于培训准备考试的读者。作为 ISO/IEC 17024 国际标准之下的 ANSI 认证认可机构，(ISC)² 没有教授 CISSP 考试。相反，我们努力生成或认可教授 CISSP 的 CBK 的内容。对 CBK 有深刻理解的候选人是考试和职业成功最好的准备。

(ISC)² 也通过与知名行业领先品牌 Wiley 合作，开辟了新的天地。与知名内容提供商 Wiley 建立合作伙伴关系，允许(ISC)² 以所需的规模增加产品，来保持我们的内容持续更新，并与不断变化的环境保持一致。 结合我们两个组织的专长和力量，对认证候选人和行业是同样有利的。

我期待你对(ISC)²《CISSP 官方学习指南(第 7 版)》的反馈。 恭喜你获得 *SC Magazine* 的名为“最佳专业认证计划”的认证的第一步。祝你学习好运！

最诚挚的问候

David P. Shearer、CISSP、PMP

CEO

(ISC)²

Cathy，你对世界和生活的看法经常让我感到惊讶，对我提出挑战，让我更爱你。

—James Michael Stewart

Dewitt Latimer，我的导师、朋友和同事。我非常想念你。

—Mike Chapple

Nimfa，感谢在过去 23 年来与我分享你的生活，也让我与你分享我的生活。

—Darril Gibson

作 者 简 介

James Michael Stewart，CISSP，从事写作与培训工作已有 20 年之久，目前专注于信息安全。自从 2002 年开始，他教授许多 CISSP 培训课程，此外还有其他关于互联网安全和道德黑客/渗透测试方面的课程。Michael 的 75 余本著作和教材主要涉及安全认证、Microsoft 专题以及网络管理。可以在 Web 站点 www.impactonline.com 上了解到 Michael 的更多信息。

Mike Chappie，CISSP，博士，Notre Dame 大学的 IT 服务交付部门的高级总监。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 TechTarget's SearchSecurity 站点的长期撰稿人，以及 25 余本著作的作者，包括 *CompTIA Security+ Training Kit* 和 *Information Security Illuminated*。可以通过 Twitter @mchapple 联系他。

Darril Gibson，CISSP，是YCDA有限责任公司的CEO，他创作或合著了超过 35 本书。Darril定期撰写、咨询和教授各种技术和安全主题，并持有多项认证。他定期在 http://blogs.getcertifiedgetahead.com/上发布关于认证主题的博客文章，并使用该网站帮助人们了解认证考试的变化。他喜欢倾听读者，特别是当读者使用他的一本书后通过考试时，并且你可以通过博客网站联系他。

致　谢

我要感谢 Sybex 继续支持这个项目。感谢 Mike Chapple 和 Darril Gibson 继续为这个项目做出贡献。感谢所有我的 CISSP 课程学生提供他们的观点和输入，以提高我的培训课件，最终成册。感谢本书第 7 版的开发编辑 Alexa Murphy 和技术编辑 David Seidl，他们在指导我们改进这本书方面表现出色。也感谢我的代理人 Carole Jelen，他继续帮助打理这些项目。

对于我敬慕的太太，Cathy：一起建立的生活和家庭比我想象的更美妙。对于 Slayde 和 Remi：你们的成长如此快速，在如此和优质的环境中你们继续快乐着生活，每天给我留下深刻的印象。你们都成长为神奇的人。对于我的妈妈，Johnnie：在你的身边是多么美好。Mark：无论过去多少时间，或者我们见面很少，我一直到永远都将是你的朋友。最后，一如既往，对 Elvis：你的方式领先当前的培根迷恋，用你的花生酱香蕉-培根；我认为这是你旅行时间的证明！

特别感谢 Notre Dame 大学的信息安全团队，他们为安全问题提供了数个小时的有趣对话和辩论，并激发和形成了本书的大部分内容。

我要感谢 Wiley 团队在整本书编写过程中提供的宝贵帮助。我还要感谢我的文学代理人，Waterside Productions 公司的 Carole Jelen。我的合作者 James Michael Stewart 和 Darril Gibson，他们都是伟大的合作者。David Seidl，我们勤奋和知识渊博的技术编辑，提供了宝贵的见解，因而我们带来了这个版本。

—James Michael Stewart

特别感谢 Notre Dame 大学的信息安全团队，他们为安全问题提供了数个小时的有趣对话和辩论，并激发和形成了本书的大部分内容。

我要感谢 Wiley 团队在整本书编写过程中提供的宝贵帮助。我还要感谢我的文学代理人，Waterside Productions 公司的 Carole Jelen；我的合作者 James Michael Stewart 和 Darril Gibson，他们都是伟大的合作者；David Seidl，我们勤奋并且知识渊博的技术编辑，他提供了宝贵的见解，因而我们带来了这个版本。

我还要感谢许多参与制作这本书的人，但我从来没有机会与他们相遇：图形团队、制作人员以及所有参与这本书的人。

我还要感谢许多参与制作这本书的人，但我从来没有机会相遇：图形团队、制作人员以及所有参与这本书的人。

—Mike Chapple

感谢 Carol Long 和 Carole Jelen 帮助获得(ISC)^2 发布的这个更新目标。这有助于我们在这个新版本上取得突破性进展，我们感谢你的努力。与像 James Michael Stewart 和 Mike Chapple 这样有才华的人一起工作很愉快。感谢你为这个项目所做努力工作和合作。技术编辑 Dave Seidl 为我们提供了一些优秀反馈。这本书更好，是因为他的努力。再次感谢 Dave。最后，感谢 Sybex 的团队(包括项目经理、编辑和图形艺术家)帮助我们打印这本书的所有工作。

—Darril Gibson

前　言

本书为你提供了 CISSP 认证考试的完备基础知识。购买本书表示你愿意学习和进一步通过完成 CISSP 认证要求技能的需求。本书前言为你概述了本书与 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。你应当在 CISSP 考试所覆盖的 8 个域中的某个域具有 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($(ISC)^2$)管理。$(ISC)^2$ 是一个全球性的非营利性组织，该组织具有 4 个主要的目标：

- 为信息系统安全领域维护公共知识体系(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。

$(ISC)^2$ 支持并提供多种认证，包括 CISSP、SSCP、CAP、CSSLP、CCFP、HCISPP 和 CCSP。这些认证旨在验证所有行业的 IT 安全专业人员的知识和技能。可以从网站 www.isc2.org 获取有关$(ISC)^2$ 及其他认证的更多信息。

CISSP 认证适用于负责设计和维护组织内安全基础设施的安全专业人员。

专题域

CISSP 认证考试涵盖了 CBK 8 个域的知识：

- 安全和风险管理
- 资产安全
- 安全工程
- 通信与网络安全
- 身份和访问管理
- 安全评估与测试
- 安全运营

- 软件开发安全

这 8 个域提供了通用安全框架并独立于供应商的观点。此框架是支持在全世界所有类型的组织中讨论安全实践的基础。

截至 2015 年 4 月，主题域进行了重大修订。域从 10 个减少到 8 个，并重新组织了许多主题和概念。有关这 8 个新域名分组在 CISSP 考试中涵盖的主题范围的完整视图，请访问(ISC)^2 网站 www.isc2.org 并索取候选信息公告的副本。本文档包括完整的考试大纲以及有关认证的其他相关事宜。

资格预审

(ISC)^2 定义了成为一名 CISSP 所必须满足的几项资格。首先，必须具有至少 5 年的安全从业经历，或者具有至少 4 年的安全从业经历加上近期的 IT 或 IS 学位。专业经历的定义是：在 CBK 8 个域中的一个或多个域从事有工资收入的安全工作。

其次，必须认可遵守相关的道德规范。CISSP 的道德规范是(ISC)^2 希望所有 CISSP 候选人都要遵守的一套准则，目的是为了维护信息系统安全领域的职业道德。可以在(ISC)^2 的 Web 站点 www.isc2.org 的 Information 部分找到这些准则。

(ISC)^2 还提供了一个被称为 Associate of (ISC)^2 的报名程序，这个程序允许由于没有安全从业经历或从业经历不足而未获得 CISSP 资格的任何人都能够先参加 CISSP 考试，随后再获取所要求的经历。Associate of (ISC)^2 的资格能够保留 6 年，以便相关人员获得 5 年的安全从业经历。只有在提供安全从业证明(通常采用提交书面证明和简历的方式)之后，(ISC)^2 才会为其授予 CISSP 认证证明。

CISSP 考试概述

CISSP 考试的重点是从三万英尺高的安全角度，涉及更多的理论和概念而不是实施和程序。虽然非常宽泛，但不是很深。要成功完成此考试，需要熟悉每个域，但不必成为每个域的专家。

CISSP 考试由 250 个问题组成，要在 6 个小时内完成。考试可以采用 PBT(基于纸质的测试)形式或 CBT(基于计算机的测试)形式。需要通过(ISC)^2 网站 www.isc2.org 注册参加 PBT 形式的考试，或通过 www.pearsonvue.com/isc2 参加 CBT 形式的考试。CBT 形式的考试由 Pearson Vue 测试机构(www.pearsonvue.com/isc2)进行管理。

PBT 形式的考试是使用纸质小册子和答卷来管理的。这意味着将使用铅笔填写答案。如果参加 PBT 考试，请务必在上午 8 点左右到达考试中心，并记住在 8:30 前进入考点。一旦所有考生都登录并参加考试，考官将会分发测试材料和几页说明页。这可能需要 30 分钟或更长时间。一旦完成该过程，将开启 6 小时的测试窗口。

CISSP 考试的题型

CISSP 考试的每一道题都有 4 个选项，但是其中只有一个选项是正确答案。有些问题非常简单，如选择正确的定义；有些问题较为复杂，如选择适当的概念或最优方法；另外一些问题则描述某个场景或环境，考生需要选择最佳的解决方案。下面给出了一道例题：

安全解决方案的最重要目标和最高优先级是什么？

A. 防止泄露

B. 保护完整性

C. 保护人身安全

D. 维持可用性

必须选择一个正确的或是最合适的答案，并且标记在答案纸上。某些情况下，正确答案显而易见。另外一些情况下，可能会有几个答案看上去都是正确的。遇到这种情况时，必须选择最适合这道问题的答案。要留意那些一般性的、明确的、全面的、扩展集和子集选项。在某些情况下，似乎没有一个答案是正确的，那么就要选择错误可能性最小的答案。

注意：

此题的答案为 C。保护人身安全应当始终是首先考虑的问题。

除了标准的多选题以外，(ISC)^2 还增加了一些新的问题形式。这些包括拖曳和热点题。拖曳问题要求测试者移动标签或图标以标记图像上的项。热点题要求测试者用十字准线标记图像上的位置。这两个问题都很容易使用和理解，但要小心拖曳或标记的准确性。

注意：

要查看这些新问题类型的实例，请访问考试大纲：候选信息公告。在后面的“示例考试问题”部分，提供了一个网址，其中提供了这些问题格式的教程。

答题建议

参加 CISSP 考试时有两个关键要素。首先，必须了解 CBK 8 个域所涉及的内容。其次，一定要有良好的考试技巧。要想在 6 个小时内完成 250 个问题的考试，每道题的平均答题时间不能超过 90 秒。因此，快速答题十分重要，虽然考生不能过于仓促，但也不能拖拖拉拉，浪费时间。

需要记住的一个关键因素是，猜测答案总比不回答问题强。如果你跳过某个问题，那么该题将不得分。但是，如果猜测一个答案，那么你至少有机会得分。答案错误并不扣分，对你来说也不会造成任何损失。因此，在 6 个小时的考试时间即将结束之前，请确认答题纸上的每道题都标记了答案。

在 PBT 形式的考试中，可以在考试小册子上写字，但是写在上面的任何东西都不会用来计算得分。可以使用小册子做笔记与掌握考试进度。我们建议你在将答案标记到答案纸上之前，再仔细看一下所选择的每一个答案。

在 CBT 形式的考试中，你将获得一个干擦板和一个记号笔，用于记下想法和做笔记。但是写在板上的任何东西将不会用来改变你的分数。并且在离开考试场所之前，该板必须上交。为了激发你参加考试的最大潜能，下面给出了一些一般性的指导原则：

- 首先回答简单的问题。
- 跳过较难的问题，稍后再返回思考。为了记住被跳过的问题，可以在考试小册子的封面上记下它们的题号。
- 在选择正确的答案之前，先排除错误的答案。
- 注意双重否定的问题。

- 务必了解问题的含义。

合理安排考试时间。你应当在一个小时内完成大约 50 个问题，这样才能在留下的时间内重新考虑被跳过的问题并重新检查一遍。记着携带食物和饮料进入考场。你不得离开考场就餐。你的食物和饮料将存放在远离测试的区域。你可以随时补充食物和饮料，但休息时间将计入你的总时间限制。还应当携带药品或其他必要的物品，但是把所有电子用品都放在家里或你的车上。考生可以戴手表，但是绝对不能使用可编程的手表。如果参加的是 PBT，需携带铅笔、人工刨笔刀以及橡皮擦。我们还建议你带上泡沫耳塞、穿舒适的衣服和轻夹克(有些测试地点有点冷)。

如果英语不是你的母语或第一外语，那么可以注册使用 CISSP 考试允许的某种语言。否则，如果选择使用英语参加考试，可以携带翻译字典。你必须能够证明自己需要使用字典，通常提供出生证明或护照就可以解决这个问题。

注意：

偶尔，会对考试或考试对象进行小的更改。当发生这种情况时，Sybex 会将更新发布到其网站。请在参加考试之前访问 www.sybex.com/go/cissp7e，以确保掌握最新的信息。

学习和备考要领

在 CISSP 考试的准备过程中，我们建议安排一个月左右的时间进行学习或者每晚进行强化学习。下面提供了几个建议，能够帮助你充分地利用学习时间；你也可以根据自己的学习习惯进行一些调整：

- 每一章的内容要花一两个晚上阅读并进行复习。
- 完成本书与考试引擎中提供的所有考试练习。完成每章的书面练习与自测题，这有助于明确需要通过认真学习和花费时间才能掌握的关键概念与策略。
- 查阅(ISC)^2 的考试大纲：www.isc2.org 上的考生信息公告。
- 使用闪视卡(包括学习工具)以强化对概念的理解。

提示：

我们建议读者将一半的学习时间用于阅读和复习各种概念，将另一半时间用于完成考试练习。学生们反映：投入考试练习的时间越多，就更容易记住考点。此外，还需要经常访问诸如 www.cccure.org 以及其他关注 CISSP 的 Web 站点。

认证过程的完成

一旦接到成功通过 CISSP 认证的通知，还剩下最后一步就能够真正获得 CISSP 认证资格。这个最后步骤被称为背书(endorsement)。从根本上说，这需要获得 CISSP 证书的某个熟悉你工作经历的人为你签字并提交背书。背书文件会作为通知你已经通过认证考试的电子邮件的附件发送给你。你只需将书面证明文件和自己的履历发送给某位声誉良好的 CISSP 即可。证明人必须查看你的履历，确认你在 8 个 CISSP 域中具有足够的从业经历，随后他会通过传真或邮寄方式向(ISC)^2 提交有自己签名的背书文件。在接到考试通过的确认邮件之后，你必须在 90 天之内向(ISC)^2 提交背书文件。一旦(ISC)^2 收到已签名的背书文件，认证过程就会结束，并且会通过 USPS 向你邮寄一个欢迎成为 CISSP 的包裹。

如果没有通过考试，可以再次参加考试，但必须等待 30 天。如果需要第 3 次尝试，必须等待 90 天。如果需要第 4 次尝试，必须等待 180 天。仅可以在任何一年尝试三次考试。需要为每次额外考试尝试支付全额费用。

CISSP 继续认证

(ISC)^2 提供了 3 种继续认证，这些认证只针对具有 CISSP 认证资格的人员。在 3 个继续认证中，(ISC)^2 应用 CISSP 考试所涉及的概念并侧重于特定的领域，也就是体系结构、管理和工程。下面讲述了这三种认证：

信息系统安全体系结构专家(Information Systems Security Architecture Professional，ISSAP)认证：针对从事信息安全体系结构工作的人员。这个认证涉及的主要领域包括：访问控制系统和方法学；密码学；物理安全集成；需求分析和安全规范、指导原则与标准；业务连续性计划和灾难恢复计划的技术方面；以及电信和网络安全。ISSAP 既可以为设计安全系统或基础架构的人员提供认证，也可以为审计和分析这些安全体系结构的人员提供认证。

信息系统安全管理专家(Information Systems Security Management Professional，ISSMP)认证：针对管理信息安全策略、实践、准则与过程的人员。这个认证涉及的主要领域包括：企业安全管理实践；整个企业的系统开发安全性；法律、犯罪调查、法庭辩论与道德规范；监督操作安全合规性；理解业务连续性计划、灾难恢复计划以及操作计划的连续性。这是对负责安全基础设施的专业人员的一项认证，特别是在强制遵守法规的情况下。

信息系统安全工程专家(Information Systems Security Engineering Professional，ISSEP)认证：针对安全硬件和软件信息系统、组件或应用程序的设计与工程人员。这个认证涉及的主要领域包括：认证和鉴定；系统安全工程；技术管理；美国政府信息保障规则和规章制度。绝大多数 ISSEP 为美国政府或某个管理政府安全检查的政府承包商工作。

要了解这些继续认证的更多信息，请访问(ISC)^2 的 Web 站点 www.isc2.org。

本书的组织结构

本书涵盖了 CISSP 公共知识体系(CBK)的 8 个域，并且对每个域都进行了深入充分的讨论，从而使你能够清楚地理解这些内容。本书的主体由 21 章组成。下面列出了各域对应的章：

第 1～第 4 章：安全和风险管理

第 5 章：资产安全

第 6～第 10 章：安全工程

第 11 和第 12 章：通信和网络安全

第 13 和第 14 章：身份和访问管理

第 15 章：安全评估和测试

第 16～第 19 章：安全运营

第 20 和第 21 章：软件开发安全

每章包含的一些要素有助于你强化学习重点和测试掌握知识的程度，接下来我们将详细介绍这些要素。注意参阅目录和每章开头的介绍，里面涵盖域中主题的详细列表。

特殊段落

阅读本书时，你会发现许多重复出现的要素。下面描述了其中一些要素：

总结 总结简要回顾了每一章所涵盖的内容。

考试要点 考试要点中指出的要点会在考试中以某种形式出现。虽然我们不可能知道某次考试中会出现哪些考点，但是这部分强化了重要的概念，这对于你理解知识域以及 CISSP 考试的范围十分重要。

章末练习题 每章都包含一些练习题，这些练习题被用来测试你对相应章节所讲述知识的掌握程度。阅读每章之后，完成练习题。如果不能正确回答某些问题，那么就表明需要重新学习相关的知识。本书的最后会给出练习题的答案。

书面实验室 每章都包含综合了相应章节的各种概念与主题的书面实验室。这些问题的意图是帮助你将零散知识点综合在一起，从而建议或描述潜在的安全策略或解决方案。

真实场景 在阅读每一章时，将发现典型的、贴近现实的工作环境描述。如果理解了相应章节内容涉及的安全策略和方法，将能够解决现实问题或避开潜在的困难。这使读者有机会看到具体的安全策略、指南或实践应该或可以怎样应用于工作场所。

额外的学习工具还有什么

本书的读者可以访问一些额外的学习工具。我们非常努力地提供一些先进的工具来帮助参加认证的过程。学习测试时，应在计算机上装载以下所有工具：

注意：

读者可以通过访问以下网址获得工具：sybextestbanks.wiley.com。

Sybex 备考软件

由 Sybex 公司专家编制的备考软件能够帮助你准备 CISSP 考试。在这个考试引擎中，你会找到本书中的所有复习题和评估题。此外，还会专门给出 5 套额外的考题。可以进行评估测试，可以逐章进行测试，可以进行模拟考试，可以完成包括所有问题的随机考试。

电子闪读卡

Sybex 的电子闪读卡包括数百个问题，旨在进一步提升应对 CISSP 考试的能力。在审查问题、练习考试和电子闪读卡之间，你将拥有足够的考试练习！

PDF 中的术语表

Sybex 以 PDF 格式提供了强大的术语表。这个全面的术语表包括你应该理解的 CISSP 所有关键术语，并含有可搜索的格式。

额外练习考试

Sybex 包括额外的练习考试，每个考试包括调查你对 CISSP CBK 中关键要素的理解的问题。这本书有 4 套额外的考题，每套考题包括 250 个完整的问题。这些考试可以在网上找到：http://sybextestbanks.wiley.com。

如何使用本书的学习工具

本书设计了许多能够指导准备 CISSP 认证考试的细节。每章开头都会开宗明义地列出相应章节将会详细讨论的 CISSP 知识点，每章结尾都提供了许多复习题和模拟考试，能够帮助你测试对各种知识的记忆以及发现自己需要继续学习的内容。这里给出了一些使用本书与学习工具的建议(可以在 sybextestbanks.wiley.com 上找到)：

- 阅读本书前先完成评估测试。这样你会了解自己需要多花些时间学习的内容以及只需快速浏览的内容。
- 阅读完每章后，完成相应章节的复习题。如果答案出错，就重新阅读本章的相关内容并分析相应的主题，在需要了解更多信息时还可以利用其他资源。
- 将闪视卡下载至你的移动设备，每天抽空进行复习。
- 利用一切机会进行自测。除了评估测试和复习题之外，额外学习工具还提供额外的考试。在不查阅本书的情况下完成这些额外考试，根据考试结果复习还未掌握的知识，直至能够完全理解和应用相关概念为止。

最后，尽可能找到学习伙伴。与他人一起学习和参加考试，会使你的认证考试过程更为愉快，并且在遇到难以理解之处可以寻求伙伴的帮助。此外，通过帮助别人克服学习障碍,也可以巩固自己的知识。

评估测试

1. 以下哪种类型的访问控制会争取去发现不需要的、未授权的或非法行为或活动的证据？

A. 预防

B. 威慑

C. 检测

D. 纠正

2. 定义和详细说明区分良好的密码选择和非良好密码选择的方面。

A. 难以猜测或不可预测

B. 满足最小长度要求

C. 满足特定的复杂性要求

D. 以上所有

3. 以下哪一项最有可能检测到 DoS 攻击？

A. 基于主机的 IDS

B. 基于网络的 IDS

C. 漏洞扫描程序

D. 渗透测试

4. 以下哪一项被视为拒绝服务攻击？

A. 假装是技术经理，通过电话要求接待员更改他们的密码

B. 在上网时，向 Web 服务器发送一个格式错误的 URL，导致系统消耗 100%的 CPU

C. 在它们通过特定子网时，通过复制分组来拦截网络流量