Mc Graw Hill Education

"All ▪ in ▪ One is All You Need."

ALL ▪ IN ▪ ONE

CISSP®认证考试指南

（第2版）

CISSP Certification All-in-One Exam Guide Second Edition

最新的内容
最全的考点

覆盖CISSP考试的10个专业领域

■

既是理想的考试学习工具，也可作为IT安全从业人员的技术参考

■

提供1100多道练习题，并给出答案和详尽的解释

光盘内容：

- 850多道模拟考题和答案
- Shon Harris讲授的密码学部分的视频培训课件

（美）Shon Harris 著　　张 辉 段海新 贾文军 译

清华大学出版社

CISSP 认证考试指南
（第 2 版）

CISSP® Certification All-in-One Exam Guide
Second Edition

[美] Shon Harris 著
张辉 段海新 贾文军 译

清 华 大 学 出 版 社
北 京

Shon Harris

CISSP® Certification All-in-One Exam Guide, Second Edition

EISBN：0-07-222966-7

北京市版权局著作权合同登记号　图字：01-2002-5671 号

本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

CISSP 认证考试指南（第 2 版）/（美）肖恩·哈里斯（Harris, S.）著；
张辉，段海新，贾文军译. —北京：清华大学出版社，2004.3
书名原文：CISSP® Certification All-in-One Exam Guide, Second Edition
ISBN 7-302-08325-8

Ⅰ. C… Ⅱ. ① 肖… ② 张… ③ 段… ④ 贾… Ⅲ. 信息系统-安全技术-资格考核-自学参考资料 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2004）第 022141 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社总机：（010）62770175　　**客户服务**：（010）62776969
组稿编辑：成昊
文稿编辑：朱起飞
封面设计：杨月静
版式设计：科海
印 刷 者：北京市耀华印刷有限公司
发 行 者：新华书店总店北京发行所
开　　本：787×1092　1/16　　**印张**：43.25　　**字数**：1052 千字
版　　次：2004 年 4 月第 1 版　　2004 年 4 月第 1 次印刷
书　　号：ISBN 7-302-08325-8/TP・5999
印　　数：1～4000
定　　价：88.00 元（1CD）

内 容 提 要

本书完全覆盖 CISSP 考试的 10 个专业领域，囊括通过 CISSP 认证考试所需的全部信息，以及最新的修订内容。借助本书，读者可以全面把握 CISSP 认证的考试重点。

全书共分 12 章，每一章都从明确的学习目标开始，接着详细介绍该领域的考试重点，最后通过考试提示、练习题以及细致的解答进行总结。配书光盘包括 850 多道模拟考题和答案，以及 Shon Harris 讲授的密码学部分的视频培训课件。

本书权威而又不失详尽，是 CISSP 认证应试者的必备教材，对广大的 IT 安全从业人员而言，亦是理想的学习工具和参考资料。

对本书第一版的赞誉

“没有这本书的帮助，我可能永远也拿不到 CISSP 证书。”

——Owen Creger，CISSP

“我向那些正在准备 CISSP 考试的人极力推荐这本考试指南，这本指南极大地帮助我全面理解了信息安全的概念、理论和实践。如今，虽然我通过了考试，我仍然不愿扔掉这本书，还把它当作一本参考指南。”

——Charles T. Danley，CCNA，CISSP，企业支持服务机构高级信息系统安全专家

“Shon 指出了一条学习捷径——你将以非常有效的方式获取所需的知识。我们公司90%的员工拥有 CISSP 证书，他们100%都读过这本书。”

——Richard Hanson，RSA 安全公司副总裁

“你的书清楚、精练、深入浅出，书中安排的方式使人集中于 CISSP 考试必备的关键知识点。无论是信息安全领域中的新手，还是资深的专家，在读完这本书之后，都会获取丰富的信息和知识。如果准备 CISSP 考试的人不读这本书，那么他们的信息安全藏书库中将缺少重要的一部分。”

——Daiel Sergile，CISSP，系统安全分析师，Cox Comminication Altanta 公司

“Shon Harris 的这本书是我准备 CISSP 考试的基础和关键。它覆盖了 CISSP 所有的 CBK，难度恰如其分，有深度而又不失幽默，这使得本书信息丰富、生动有趣，最重要的是读者容易记住其中的内容。练习题是准备考试的重要内容，需要仔细地分析才能得到正确答案。我向许多同事都推荐过这本书，自己也定期翻阅。”

——David Heydecker，CISSP，BMC 软件公司

“在找到这本书之前，准备 CISSP 考试令人望而生畏。这本书让我有机会在一本书里学到了 10 个所有安全领域（CBK）的知识，每章之后的提示和练习题使我可以测试自己掌握的程度。这本书的光盘包含的模拟考题可以测试我对全书信息的掌握。我购买并阅读了大量 CISSP 的书和其他一般性的安全书籍，对准备 CISSP 考试的安全专业人士来说，Shon 写的这本书内容广泛、深入浅出，我极力推荐这本书。”

——Betty Prince，CISSP，资深信息安全分析师，社区安全合作组

译者序

近年来，随着互联网的发展，黑客入侵、拒绝服务攻击、蠕虫病毒泛滥等安全事件越来越严重，同时计算机网络和信息安全也引起了社会各界越来越多的关注。但是长期以来，人们对信息安全的理解还是十分模糊的，特别是在企业中，经常无法明确安全管理的目标和任务。20 世纪 80 年代中期，人们开始认识到，亟需一种资格认证体系以规范信息安全行业，并证明从业人员的能力和资格，提高计算机安全行业及其从业人员的可信度。

信息系统安全专家认证（CISSP）是国际上信息安全领域中最权威的高级安全专业人员认证之一，1988 年由美国信息系统安全协会、加拿大信息处理协会、美国计算机安全研究所、爱达荷州立大学以及其他一些美国和加拿大的政府机构联合发起，后来成立了国际信息系统安全认证联盟$(ISC)^2$，负责为信息系统安全从业人员建立一套安全资格认证体系。这项认证面向信息安全领域的高级专业人员，全面考查待考人员的技术、管理、法律等各个方面的知识和能力。尽管$(ISC)^2$ 成立于北美，但它很快得到了国际上广泛的认可，为企业挑选高级安全管理人员和技术人员提供了有效的依据。

本书对准备参加 CISSP 认证考试的安全专业人员来说是一本不可多得的重要参考书之一。在本书中，身为 CISSP 的 Shon Harris 首先介绍了 CISSP 考试的特点、考试的形式、甚至考试的技巧；然后全面介绍了 CISSP 考试必备的所有 10 个公共知识体系（CBK），从安全管理、密码学、安全模型、安全通信、物理安全、灾难恢复、道德和法律等，几乎无所不包，写作风格深入浅出，非常适合 CISSP 考试“一英里宽，一英寸深”的特点。即使您不准备参加 CISSP 考试，本书也可以作为一本信息安全的教科书，供您全面了解信息安全的各个领域中最重要的知识点。

由于译者水平有限，时间有限，有不足之处希望读者和专家批评指正。您的批评和建议是对本书价值的肯定和对我们工作的帮助。

译者简介

张辉，清华大学信息网络工程研究中心讲师，多年从事网络和安全领域的研究、开发和管理工作，在入侵监测、操作系统等方面有多年实践经验，在国内外重要学术会议和刊物上发表论文多篇。

段海新，CISSP，清华大学信息网络工程研究中心副教授，博士，主要从事网络和信息安全的教学、科研和管理工作，中国教育和科研计算机网紧急响应组（CCERT）负责人。

贾文军，CISSP，从事信息安全的研究和实践工作，主要研究方向是风险评估、安全审计、信息安全管理体系（ISMS）、业务连续性管理。

作者简介

身为 MCSE 和 CISSP 的 Shon Harris 是一位安全顾问，她向各种不同的商业公司提供安全评估和分析、脆弱性测试和解决方案。她是美国空军信息战部门的工程师，该部门在入侵演习中执行渗透入侵活动，并对军事基地进行评估。

Shon 的文章经常发表在 *Information Security Magazine* 和 *Windows 2000* 这两本杂志上，她是 Mike Schiffman 所著的 *Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios*（该书最新版的中译本《黑客大挑战 2》已由清华大学出版社于 2003 年出版）一书的合著者之一，还著有 *Mike Meyers' CISSP Certification Passport*（McGraw-Hill/Osborne, 2002）一书。Shon 还在当地各个大学里教授网络安全和 CISSP 方面的课程。读者可以通过电子邮件 shonharris@hotmail.com 同她联系。

致谢

我要感谢 Sam Tomaino，在很多很多年以前，他给我讲解了计算机是怎样工作的。我要感谢 Dan Ferguson，因为他从来都没有因为我向他连珠炮式的发问而有什么抱怨，而且还培养了我永无止境的好奇心和求知欲。我要感谢 Joe Kowtko，因为他不断给予我对计算技术世界的普遍理解。这些人中的每一位都以很多方式帮助了我编写本书。

我要特别感谢我的丈夫 David Harris，感谢他一直以来的支持和爱。没有他对我的坚定信心，我根本无法取得我目前的成就。

序

在当今的世界里，信息安全这个词显得有点儿自相矛盾。随着应用和系统迅速地冲击着市场，人们几乎没有时间去评估它们的安全性到底如何。从类似 CodeRed 和 Slammer 这样的经验中，我们正迅速认识到我们需要更深入地了解安全问题，但是该从何处入手呢？这个问题提得好，答案虽然很多，但最终都不外乎会教育我们的 IT 界要有安全意识。

McClure、Scambray 和 Kurtz 在 1999 年以 *Hacking Exposed*（McGraw-Hill, Osborne）（该书中译本《黑客大曝光》由清华大学出版社出版，目前已是第 3 版）一书向 IT 界介绍了黑客（hacker）的思路。他们明确了一股正在给世界造成严重影响的潮流，并且提供了第一部正式出版的防御宝典。计算机紧急响应组（Computer Emergency Response Team，CERT）成立于 1988 年，在他们成立的第一年里报告了 6 起涉及信息安全的紧急事件，而在 2001 年的前三个季度，这个数字增加到 85 334 起。这一令人难以置信的统计数字促使我们必须要采取行动了。麻痹大意不足取，勤学习才是关键。IT 业的成长速度大大超出了我们能够教育人们去维护它的速度。留给普通 IT 专家和安全人员去“发现”新的安全措施和规程的时间更少了，而留给黑客学会怎样逃避他们的时间却更多了。我们必须向 IT 专家提供工具，使之既能维护安全的信息系统，又不会让他们的公司因为紧急事件恢复的花费和专业咨询费而背上沉重的经济包袱。我们能做到这一点的惟一方式就是通过撰写文档和开展教育工作。

专门介绍网络安全方面好的实践经验的书为数并不多。而在这些书中间，却又没有一本书能就应该如何配置系统，以便有效和可控地在服务与风险之间求得平衡这一问题给出全面的介绍。在 CERT 成立之后的 11 年里，一直没有人就如何设计、实现和维护安全的信息系统提供完整的学说。衡量安全专家的行业标准的缺乏，促成了国际信息系统安全认证联盟（International Information Systems Security Certifications Consortium，$(ISC)^2$）的成立。$(ISC)^2$ 是 CISSP 认证的策源地。CISSP 是第一种引入到 IT 界和安全领域的与厂商无关的安全认证。

由很多方面来提出对信息安全标准的需求，这更偏向团队合作而不是个人的单打独斗。我们一起努力要比各自为政能获得更多的成果。我们需要在信息和想要利用这些信息的人之间竖起一道围墙，标准化和合作是成功的关键。没有了它，我们就会无组织、无纪律地乱做一团，虽然竭尽全力地伸手去抓飘忽不定的数据，但是却抓错了。

您将要读到的这本书会使您“亲密接触”信息和网络安全领域。作者以她自身在网络和应用安全方面的丰富经验为基础编写了这本书，这些经验来源于她在国际银行业的工作以及在军方信息战中的成果。她对这个行业充满了激情。她会让读者感受到她的智慧和知识。如果您的目标是避免成为 CERT 安全事故统计数字中的一员，那么您已经找对地方了。

Joseph Kowtko

信息安全专家，Financial Solutions Group Logistics Getronics 的网络基础设施经理

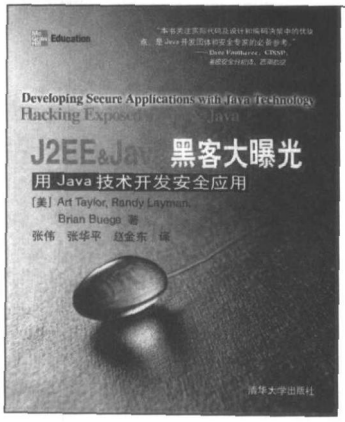
概 述

2001 年 9 月 11 日的惨剧发生之后，计算机、信息和物理安全的重要性在以指数速率增长。在过去的几年里，随着 Web 站点被黑、拒绝服务攻击增多、信用卡信息被盗、公开可得的精巧的黑客工具增加，以及如今病毒和蠕虫所造成的损失更大，计算机和信息安全的必要性已经慢慢得到人们的认识。

众多的公司不得不花掉数以百万计的美元来消除这些问题的影响，还要再花掉数以百万计的美元购买设备、软件，聘请顾问，开展培训来保护他们的周边和内部网络。但是在 2001 年 9 月 11 日之后，这类安全保障的必要性和紧迫性有了新的诠释。面对可能通过网络连线和无线电波发生的各种不同类型的攻击，政府、国家和社会的脆弱性慢慢地暴露出来。社会各界非常依赖各类计算资源和功能，而它们大多是由公有和私营的商业部门来提供的。这意味着，即使政府有责任保护其公民，但是公民及公民所有的公司必须更为安全，这样才能保护整个国家。

这种类型的保护实际上只能通过正确的教育和理解开始，而且必须专门落实这一点以持续下去。编写本书是为许多不同的领域提供一个基础，这些领域组成了有效的安全保障。在“911”之后，我们虽然处在不同的时间和地点，情况或好或坏，但都需要了解我们所易于遭受的所有威胁和危险，还需要了解减少这些脆弱性所需采取的步骤。

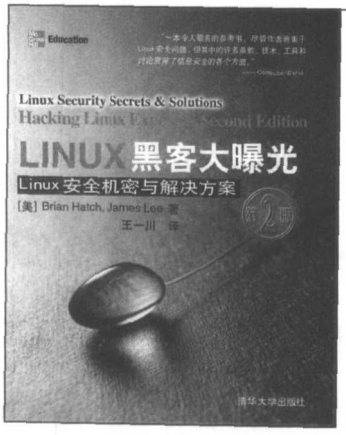
信息安全专著



原书名：Hacking Exposed J2EE&Java
作者：Art Taylor 等
书号：7-302-07649-9
页数：372
定价：43.00元

孙子云：善攻者，敌不知其所守；善守者，敌不知其所攻。本书作者通过来自现实世界的攻击案例，揭露黑客攻击 Java 应用程序的方法和手段，并及时提出应对方案，使您未雨绸缪，先人一步。

本书是开发 Java 安全应用的宝典，关注与应用开发者息息相关的问题，是 J2EE 和 Java Web 应用安全人士的良师益友。

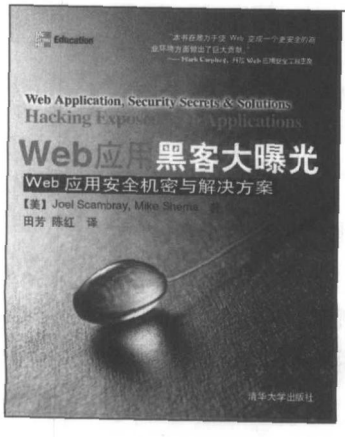


原书名：Hacking Linux Exposed, Second Edition
作者：Brian Hatch, James Lee
书号：7-302-07655-3
页数：557
定价：59.00元

为你揭开 Linux 黑客的神秘面纱。

专注于掌握入侵者收集信息、确定目标、搜寻漏洞和获得控制的方法，并给出相应的解决方案。

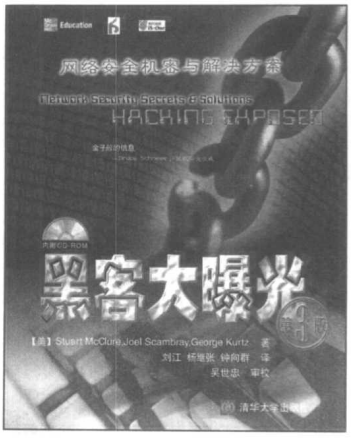
囊括了众所周知或迄今仍鲜为人知的入侵案例。



原书名：Hacking Exposed Web Applications
作者：(美) Joel Scambray, Mike Shema
书号：7-302-07486-0
页数：378
定价：39.00元

本书的作者站在技术演变的风口浪尖向我们展示了针对Web脆弱点的当前策略及最新见解。书中揭示了入侵者收集信息、锁定目标、标识脆弱点、获取控制及掩盖踪迹的全过程。您将目睹真实世界中的黑客事件并学习相应的对策。微软安全专家 Erik Oison 称此书“为 Web 架构师和操作员的必读之作。”

信息安全专著

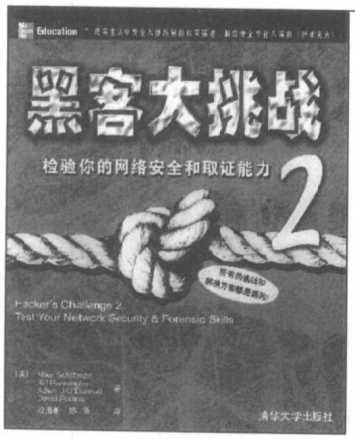


原书名：Hacking Exposed，Third Edition
作者：（美）Joel Scambray & Stuart McClure & George Kurtz
书号：7-302-05026-0
页数：750
定价：79.00元（1CD）

亚马逊网站信息安全类头号畅销书，计算机安全领域的大百科全书。

介绍最新的无线网络攻击及分布式拒绝服务攻击（DDoS），新增CD-ROM，包含口令数据库、顶级安全工具等。

负责安全保障工作的网络管理员和系统管理员的必读之书，企业及组织的政策制定者也会从中受益。

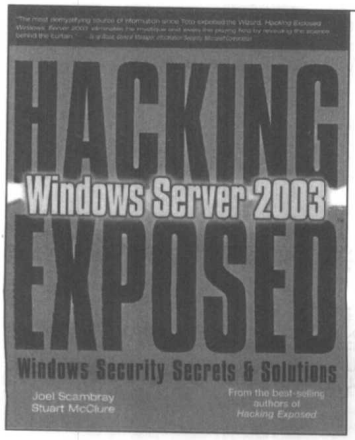


原书名：Hacker's Challenge 2
作者：（美）Mike Schiffman，Bill Pennington
书号：7-302-07207-8
页数：323
定价：39.00元

现实生活中安全入侵场景的真实描述，网络安全专业人员的《伊索寓言》。

并不是第1版的修订，而是一本全新的书，其中，挑战和解决方案都是新的。

包括两部分，第1部分是所有案例研究，即“挑战”；第2部分是第1部分所有挑战的解决方案。



原书名：Hacking Exposed Windows Server 2003
作者：Joel Scambray，Stuart McClure
页数：420
估价：40.00元

与畅销书《黑客大曝光》出自同一作者之手。

Windows Server 2003系统入侵的终结者，全面保护您的Windows Server 2003系统免受最新病毒侵扰和灾难性攻击。书中给出的案例和代码示例均来自现实世界，为您正在面临或即将面临的侵害提供应对良策。

Shon Harris' CISSP® Certification Package

Practical, Comprehensive and Extensive

In this video edition of her acclaimed CISSP seminar, *Shon Harris* presents her effective and proven methods for passing the CISSP exam. All objectives of the exam are addressed, along with real world examples, understandable explanations, full reviews, test-taking tips and question and answer sessions.

- Study with Shon on your PC at home, at work or while traveling for a fraction of the cost of attending her course in-person. Replay any section, anytime.
- Not just a training video, this package contains the new edition of Shon's best-selling *CISSP All-In-One Study Guide* with 1,000 new questions and answers; a CD-ROM with 1,500 more study questions; and 30 hours of classroom time presented on DVD-ROMs.

Fully covers all ten domains in the (ISC)² *Common Body of Knowledge*

1. *Security Management Practices*
2. *Access Control Systems & Methodology*
3. *Security Architecture & Models*
4. *Business Continuity & Disaster Recovery Planning*
5. *Cryptography*
6. *Physical Security*
7. *Telecommunications & Network Security*
8. *Law, Investigation & Ethics*
9. *Applications & Systems Development*
10. *Operations Security*

"Thoroughly covered all topics with expertise. This was a great experience." —*J. P., Joint Staff, Pentagon*

"Great presentation skills... addressed all issues, questions and concerns" —*W. S., U.S. Army*

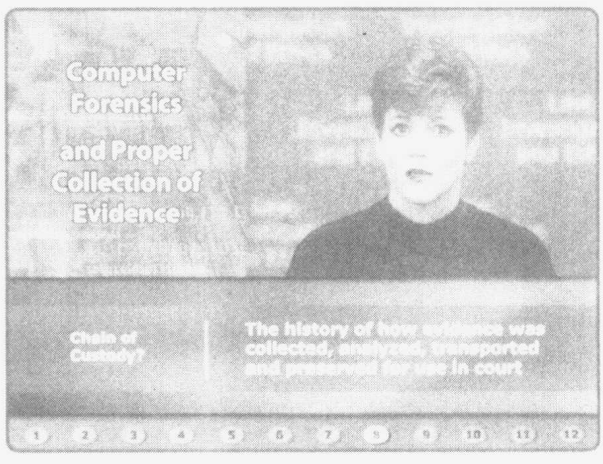
"A wealth/breadth of... real world examples." —*R. S.*

"Shon is a natural and dedicated teacher." —*J. B.*

"Exceptional, beneficial; super training!" —*W. S. WorldCom*

Shon Harris, CISSP, MCSE, is an independant security consultant and an engineer in the Air Force's *Information Warfare* unit. She has authored two best-selling CISSP books, and was co-author of the book, *Hacker's Challenge.* Shon has taught computer and information security to a wide range of clients, including *RSA, Dept. of Defense, Dept. of Energy, NSA, Bank of America, Microsoft and BMC.*

Place your order at www.intenseschool.com or call 800-330-1446.



Example from *Law, Investigation & Ethics.*

目　录