ProsoftTraining 独家授权

CIW Security Professional Study Guide

Certified Internet Webmaster
认证因特网Web主管


# CIW:
# 安全专家全息教程

〔美〕 James Stanger 等著

魏 巍 等译

考试号：1D0—470

全球最优秀的出版社之一
各种SYBEX学习指南书籍
印数已经超过500万册




電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

*CIW: Security Professional Study Guide*

考试号
1D0-470

# CIW：安全专家全息教程

〔美〕 James Stanger 等著

魏巍 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

## 内 容 提 要

本书是Sybex公司出版的CIW认证考试学习指南丛书之一。书中在重视实践应用的基础上，不仅涵盖了参加考试所需的知识，而且还全面介绍了如何完成一个系统安全的设计工作。本书介绍了安全概念、安全策略和用于Windows与UNIX系统的安全机制，以及各种安全实现方法，包括加密技术、防火墙种类、入侵检测和审核过程与日志分析等。

书中内容新颖、全面，图文并茂，适合于需要建立系统安全的设计者和开发者，而且也是系统管理员必备的参考指南。


Copyright©2003 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

本书英文版由美国SYBEX公司出版，SYBEX公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可，不得以任何形式和手段复制或抄袭本书内容。

版权贸易合同登记号：01-2002-2666

**图书在版编目（CIP）数据**

CIW：安全专家全息教程/（美）斯坦戈（Stanger, J.）等著；魏巍等译.—北京：电子工业出版社，2003.1

书名原文：CIW Security Professional Study Guide

ISBN 7-5053-8029-X

Ⅰ. X… Ⅱ. ①斯… ②魏… Ⅲ. 因特网－工程技术人员－资格考核－教材 Ⅳ. TP393.4

中国版本图书馆CIP数据核字（2002）第074641号

责任编辑：郝黎明 徐云鹏

印　　刷：北京天竺颖华印刷厂

出版发行：电子工业出版社 http://www.phei.com.cn

北京市海淀区万寿路173信箱 邮编：100036

北京市海淀区翠微东里甲2号 邮编：100036

经　　销：各地新华书店

开　　本：787×1092 1/16 印张：30 字数：760千字

版　　次：2003年1月第1版 2003年1月第1次印刷

定　　价：58.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换，若书店售缺，请与本社发行部联系。联系电话：（010）68279077

# 读者购碟说明

为了方便读者阅读本书，我公司为读者准备了该书的选配光碟（1张），售价25.00元（免费邮寄）。

该光碟系阅读本书的辅助资料，受国际版权保护，不得复制、拷贝。

凡购买光碟的读者，请将现金寄往我公司，我公司在收款后尽快将光碟寄出。为避免差错，请将收件人姓名、地址和邮编填写清楚。请勿在信中夹带现金。

**请务必在汇款单附言栏中填写清楚所购光碟的配套书名，以免延误邮寄时间。**


通讯地址：北京市海淀区翠微东里甲2号
北京美迪亚电子信息有限公司
邮政编码：100036
联 系 人：发行部
联系电话：68252397


# 欢迎与我们联系

为了方便与我们联系，我们已开通了网站（www.medias.com.cn）。您可以在本网站上了解我们的新书介绍，并可通过读者留言簿直接与我们沟通，欢迎您向我们提出您的想法和建议。也可以通过电话与我们联系，电话号码（010）68252397。

# 出 版 前 言

CIW认证考试自2002年5月进入中国以来，发展势头极猛，考生数量剧增，询问是否有中文版图书出版的咨询电话不断打进美迪亚公司。作为一家业界知名的公司，美迪亚早在1998年就开始引进出版Microsoft、Cisco、Oracle、Lotus、Java、PMP、IT Project+、Network+等国际著名认证考试用书，至今已出版了六十余种。2002年8月，美迪亚又率先从美国Sybex公司引进了一套五种CIW认证考试全系列教材，翻译出版了目前市场上惟一一套既权威又完整的中文版教程。

美国Sybex公司是一家以出版国际权威认证考试和编程语言用书为主的专业出版社，也是全美最大的独立计算机出版社，至今已有25年的出版历史。世界最权威的认证考试参考教程在Sybex都有出版。为了更好地编写并出版CIW认证考试丛书，Sybex与组织CIW考试的ProsoftTraining建立了战略伙伴关系，按照助理、管理大师、设计大师三条主线共同推出五本书。每本书都基于ProsoftTraining的要求编写，完全符合ProsoftTraining考试大纲，因此得到了ProsoftTraining的独家授权（Exclusively Endorsed by ProsoftTraining）。

目前CIW认证有五门，五门考试及相关中文版图书情况如下：

| 考试号 | 考试名称 | 书名 | 出版时间 |
|---|---|---|---|
| 1D0-410 | Foundations | CIW：基础全息教程 | 2002.8 |
| 1D0-470 | Security Professional | CIW：安全专家全息教程 | 2002.9 |
| 1D0-420<br>1D0-425 | Site Designer<br>E-Commerce Designer | CIW：站点与电子商务设计全息教程 | 2002.12 |
| 1D0-450 | Server Administrator | CIW：服务器管理员全息教程 | 2002.12 |
| 1D0-460 | Internetworking Professional | CIW：网际互联专家全息教程 | 2002.12 |

本套中文版CIW丛书每本都既包含学习考试要点，又配有几百道英文考题和中文答案。如果读者想看英文原书，可在该书选配光碟中找到PDF格式文件的英文原书内容，可通过计算机阅读，检索起来非常方便。在选配光碟中，Sybex还为每本书开发了能够模拟真实环境测试的工具和相应软件，有几百道题的题库，模拟环境中有一个倒计时钟表，回答结束后给机会检查，然后自动给出分数，此外还提供了两套书中没有的考试真题。

与目前的英文教材相比，此套中文教材将有助于正确理解概念、理论和实例，尤其是对于像您这样工作繁忙、责任重大的数十万因特网Web主管，在有限的时间内，无论是接受正式培训还是自学，学习本套丛书，尽得各门课程精髓。

祝大家好运！

美迪亚公司

此为试读，需要完整PDF请访问：www.ertongbook.com

# CIW：安全专家全息教程考试目标

考试号：1D0-407

| 目标 | 章 |
| --- | --- |
| **网络安全和防火墙** | |
| 阐明网络安全的重要性，确定有效安全策略中的各种要素，这些要素包括但不限于：风险要素、与安全相关的组织机构、保证安全的关键资源、威胁安全的种类和访问控制 | 1 |
| 定义互联网络中使用的加密技术和加密方法 | 2，6 |
| 使用有效网络安全的指导方针和原则建立有效详细的解决方案 | 2，4 |
| 应用安全原则和识别安全攻击 | 3，4 |
| 识别防火墙类型和定义常用的防火墙术语 | 5，6 |
| 设计防火墙系统合并多级保护，包括但不限于：防火墙系统设计、前摄检测、设置陷阱、破坏安全的响应和安全警告组织 | 5，6，7 |
| **操作系统安全** | |
| 确定保护操作系统安全的关键原则，包括但不限于：工业评估准则，UNIX和Windows服务器、安全管理和默认设置 | 8 |
| 确定机制、安全参数和保护Windows和UNIX账户安全所需的技术 | 8，9 |
| 识别、分配和使用用于Windows和UNIX服务器的文件系统的权限 | 9 |
| 对常见的与Windows和UNIX服务器相关的风险进行评估，包括但不限于：操作系统攻击、系统扫描、NIS、NFS和Trojans | 10 |
| 通过修改系统参数和锁死服务降低风险 | 10 |
| **安全审核、攻击和威胁分析** | |
| 确定安全审核原则，包括但不限于：安全审核员的职责、网络风险因素分析和审核步骤 | 11 |
| 定义安全审核和发现程序、计划一个审核、安装和配置基于网络和基于主机的发现软件 | 11 |
| 确定渗透和控制的策略和方法，包括但不限于：潜在的攻击、路由器安全、威胁抑制和入侵检测 | 3，7，12，13 |
| 在一个企业环境中建立一个入侵检测系统 | 13 |
| 实施日志分析，建立一个用户行为基准，并对不同的服务和系统执行审核 | 14 |
| 增强安全策略适应性并建立评估报告的辨别方法 | 15 |
| 安装操作系统附加软件，包括但不限于：个人防火墙、本机审核SSH | 15 |

## 致读者:

ProsoftTraining的认证因特网Web主管（CIW）程序已经确定自己为IT行业的最重要的Internet认证之一。Sybex与ProsoftTraining合作创作了全息教程系列丛书——正如你手中拿到的这本——为针对Associate、Master Administrator和Master Designer系列考试。每本Sybex的书都以正式的课件为基础，并且由ProsoftTraining专门授权。

正像ProsoftTraining专注于针对认证使用Internet技术的IT专家建立可测量的标准，Sybex也专注于提供给这些专家所需的技术和知识，来达到那些标准。Sybex的长期愿望是能够帮助跨过目前IT行业所面临的知识与技术上的裂缝。

为了保证本书能够全面、深入和易于学习，作者和编辑在工作中付出了很多努力。我们相信本书将会满足并超过认证市场严格的标准，帮助CIW认证的候选人在努力后获得成功。

在完成CIW认证的追求中，祝好运！

Neil Edde
Sybex认证副总编

# 致　谢

首先，我要感谢Liz Welch使创作这本书的过程如此愉快。很难找到像你这样有才能和对细节如此关注的编辑。我知道我本应该让语言更简练些。我还希望感谢Molly Glover，他的灵活性和幽默感，使得商讨此书的过程变得令人愉快。对于Liam Noonan，感谢你作为技术编辑的聪明才智。我很少有机会能与如此完美的专家一起工作。我要特别感谢Heather O'Connor，你不仅是一位真正的Bugs Bunny爱好者，而且，给我印象最深的是你在商量出版一部如此杰出的书籍方面的才能。我很少见到如此复杂的项目进展得如此顺利，荣誉属于你们！

我还想占用一点时间感谢Tim Crothers，他是第一个激起我对网络安全兴趣的人。我要感谢你的耐心和你花费时间与我一起分享知识。最后，我要感谢我的家庭。我的妻子Sandi，以及James、Jacob、Joel和现在的Joseph（我知道许多以“J”开头的名字），在我写这本书的时候，你们对我显示出了极大的耐心。

——James Stanger

我要感谢我的家庭，在我利用额外的时间写原稿的时候，Lori、Emily、Ben和Jacob对我给与支持。我要特别感谢James Stanger，他的努力远远超过了原稿所要求的。我还要感谢Jud Slusser和他的全体工作人员，在原稿创作上的一个优秀的支持小组。

——Tim Crothers

Patrick Lane想要感谢他的妻子Susan，感谢她的支持。在耗费时间的创作CIW基础学习、CIW网际互联专家和CIW安全专家这些书期间，妻子让他看到生活的亮光。他还要感谢Jud Slusser的智慧和对认证长远的目标，感谢James Stanger技术方面的专业知识。他还想感谢Heather O'Connor为Sybex公司创作CIW丛书提供的机会。

——Patrick T. Lane

# 译 者 序

从20世纪60年代末现代意义上的计算机网络——ARPANET实验网问世到今天，人们无时无刻不在谈论系统安全这个话题。但是，从没有一个阶段像今天这样，系统安全被大范围地引入到民用领域，并随时随地面临着大规模的安全破坏与威胁。面对层出不穷的五花八门的攻击手段，各种各样的安全保护措施也应运而生。如何有效保护自己的系统，甚至打击系统入侵者？如何及时检测来自内部和外部的攻击，并对隐患做出预警？如何培训自己的员工，并说服管理层协助安全保护？这些都应验了一句古话“道高一尺，魔高一丈”。

本书全面、详细地介绍了系统安全的策略和多种保护措施，以及黑客攻击系统的常用手段，有助于安全决策者和系统管理员能够根据公司的业务特点，协同公司管理人员确定具体业务运作和系统安全保护的方向和原则。本书涉及的个人和网络系统的保护工具，为系统管理员和安全保护人员提供了形象而生动的实例。同时，也细化了安全保护与攻击的概念。

本书是一本全息教程，主要是为了参加CIW安全专家认证考试的朋友而写的。对于从事企业网络系统管理的人员及希望了解系统安全的朋友，本书既提供了快捷有效的查阅途径，也提供了安全架构建设的依据。

参加本书翻译工作的人员有：魏巍、赵菁、赵明大、秦迤君、赵宇。

在翻译书中大量专业术语的时候，我们参阅了相关的技术文献，但由于时间仓促，书中有不足之处，望广大读者批评指正。

# 简　介

Prosoft CIW（Certified Internet Webmaster）认证证明你具备建立、运行和修改一个网站的必需的技能。这些正是那些在当今经济体制下，雇主正在寻找的技能，并且，是你需要在当前的工作市场上保持领先的竞争优势所需要的技能。CIW认证将向你现在的或今后的雇主证明你在发挥知识技能时认真严肃的态度。获得CIW认证还将为你提供一些重要的技能，包括基本联网知识、网页制作、网络互联、安全维护和网站设计，并且，使你接触多家的厂商的Web设计和实施的产品。

本书是为了帮助你准备CIW安全专家考试1D0-470（Certified Internet Webmaster Security Professional Exam 1D0-470）。安全专家考试是全部“CIW服务器管理大师（Master CIW Server Administrator）”系列的最后一门考试，它涵盖了基本的、高级的网络安全概念，包括如何使用强加密、保护操作系统、使用防火墙和审核网络。它还讨论了如何配置入侵检测系统和改善一个网络的安全外壳。一旦通过了CIW安全专家考试，你就获得了CIW管理大师（CIW Master Administrator）资格。拥有了证书后，你可以充满自信地考虑一个网络安全分析和顾问的职责。

## 认证因特网Web主管方案

CIW的Internet技能认证程序是针对那些设计、开发、管理、安全和支持Internet或Intranet相关服务的专业人员。CIW认证程序提供了行业范围的、对个人Internet和Web知识和技能的认可，并且，认证常常是雇佣和分配决定的一个因素。它还为一个人作为Internet专家的资格提供了切实的证据。拥有这个认证，可以向潜在的雇主和客户证明，他们经过了严格的培训和考试要求，应该将他们与非认证的竞争者分开。所有的CIW认证都由International Webmasters Association（IWA）和Association of Internet Professionals（AIP）签署。

### CIW助理

通向CIW认证的第一步是CIW基础（Foundations）考试。通过CIW助理认证和基础考试的考生具备基本的动手技能和一个Internet专家需要理解和应用的知识。基础技能包括基本的Internet技术、网络架构和使用HTML进行Web编辑的知识。

CIW基础程序为所有使用Internet的专业人员设计。对于CIW助理或完成程序并通过基础考试的人，他的工作期望包括：

- 理解Internet、联网和网页的制作基础
- 基础技能的应用需要专业化

**说明：** 要成为一名CIW助理，需要几个前提。例如，为了开始基础考试的准备，不需要具备Internet经验，但是应该懂得Microsoft Windows。

表1显示了CIW基础考试和相应的涵盖了CIW助理认证的Sybex全息教程。

**表1 CIW助理考试和相应的Sybex全息教程**

| 考试名 | 考试号 | Sybex全息教程 |
| --- | --- | --- |
| Foundations | 1D0-410 | CIW：基础全息教程（ISBN 7-5053-7917-8，电子工业出版社） |

**说明：** CIW从CIW助理考生那里接受分数报告，考生已经通过了入门级别的CompTIA i-Net+考试（IKO-001），并且将被授予Foundations认证证书。更多有关i-Net+和其他CompTIA考试的信息，请参阅www.comptia.org。

在通过考试后，考生们成为CIW助理，并且能够在四个Master CIW认证系列中选择一个感兴趣的方式通过要求的考试：

- Master CIW Designer
- Master CIW Administrator
- CIW Web Site Manager
- Master CIW Enterprise Developer
- CIW Security Analyst

## CIW设计大师（Master CIW Designer）

设计大师系列由两个考试组成，每个考试代表了一个Internet工作角色的具体方面：

**站点设计师考试** CIW站点设计师使用人为因素的原则设计、实施和维护基于超文本的网站。站点设计师使用制作和脚本语言，以及数字媒体工具，提供内容创建和网站管理。

**电子商务设计师考试** CIW电子商务设计师，在电子商务建立、有关产品选择和付款的人为因素原则和站点安全和管理的基础上被进行考察。

表2显示了CIW站点设计师和电子商务设计师的考试，以及相应的通向CIW设计大师认证证书的每一步的Sybex全息教程。

**表2 设计大师考试和相应的Sybex全息教程**

| 考试名 | 考试号 | Sybex全息教程 |
| --- | --- | --- |
| 站点设计师 | 1D0-420 | CIW：站点与电子商务全息教程（电子工业出版社） |
| 电子商务设计师 | 1D0-425 | CIW：站点与电子商务全息教程（电子工业出版社） |

## CIW管理大师（Master CIW Administrator）

CIW管理员精通三个领域的管理：

- 服务器
- 网际互联
- 安全管理

此为试读，需要完整PDF请访问：www.ertongbook.com

在通过每一个考试后，你就成为了一名在那个具体领域的CIW专家。

**服务器管理员考试（Server Administrator Exam）** CIW服务器管理员为中到大型商务进行管理，并调整公司的电子商务架构，包括Web、FTP、新闻和邮件服务器。服务器管理员配置、管理并使用电子商务解决方案服务器。

**网际互联专家考试（Internetworking Professional Exam）** 网际互联专家定义网络结构、确定结构组件、监控并分析网络性能。CIW网际互联专家负责设计和管理企业TCP/IP网络。

**安全专家考试（Security Professional Exam）** CIW安全专家使用防火墙系统和攻击识别技术，实施安全策略、识别安全威胁并开发对策。作为一位CIW安全专家，你负责管理电子商务事务处理和报偿的安全解决方案。

表3列出了管理大师系列的考试。

**表3　管理大师考试和相应的Sybex全息教程**

| 考试名 | 考试号 | Sybex全息教程 |
|---|---|---|
| 服务器管理员 | 1D0-450 | CIW：服务器管理员全息教程（电子工业出版社） |
| 网际互联专家 | 1D0-460 | CIW：网际互联专家全息教程（电子工业出版社） |
| 安全专家 | 1D0-470 | CIW：安全专家全息教程（电子工业出版社） |

### 其他CIW认证证书

Prosoft在网站管理、企业发展、安全分析方面还提供另外三个认证证书系列。

**CIW网站管理大师** 网站管理员认证，由两个Internet工作角色系列考试（站点设计师1D0-420和服务器管理员1D0-450）和另外两个语言考试（CIW Web语言系列中的JavaScript 1D0-435和Perl Fundamentals 1D0-437）组成。

**CIW企业专家开发员** 企业开发员认证，由三个Internet工作角色系列（应用程序开发员1D0-430、数据库专家1D0-441和企业专家1D0-442）和另外三个语言/理论系列（Web语言、Java编程和面向目标的分析）组成。

**CIW安全分析师** 安全分析师认证，认可那些已经获得了一个网络证书，并被证明他们具有需要的安全技能的人，并利用他们的技术能力，阻止内部和外部的与计算机相关的威胁。

有关Prosoft的全部认证和考试的更多信息，请参阅www.ciwcertified.com。

## 本书的特点

是什么使得Sybex全息教程这本书成为众多技术领域里五十多万考生的选择呢？我们不仅重视为了你通过考试时所需要的知识信息，而且重视你在真实世界中应用所学到的知识时所要知道的信息。每一本书都包含下列一些内容：

**目标信息** 每一章在开始，列出了CIW目标组在其中涵盖的内容。

**评估测试** 在这一章介绍后面是一个评估测试，可以通过它帮助确定对配置防火墙、

保护操作系统和网络审核了解的程度。每一个问题都与本书中讨论的一个主题相关。利用评估测试的结果，可以找出你需要集中学习的领域。当然，我们建议你阅读本书的全部内容。

**考试要点** 为了回顾所学到的内容，你会在每一章的结尾处发现一个考试要点列表。这个考试要点简要地突出了在你准备考试的时候需要特别关注的话题。

**关键术语和词汇表** 每一章都会被引入一些重要的术语和概念，这些都是参加考试时需要知道的。这些术语在每一章中以列表的形式出现，而且关键术语列表正好出现于考试要点之后。在本书的最后，一个详细的词汇表给出了这些术语的定义，以及其他你应知道的常规术语。

**复习题，包括详细的解释** 每一章的最后都是一套用来测试你在这一章中学到的内容的复习题。题目是按你心目中的考试来编写的，也就是说，它们与你将在考试中看到的、感觉到的是一样的。

**动手练习** 阅读全书，你将会发现一些练习，通过这些练习，可以获得重要的动手经验，这对考试准备过程是非常关键的。这些练习紧扣每一章中的主题，并且它们使你完成了执行一个具体功能所必需的步骤。

**交互式CD** 每本Sybex全息教程都选配一张光碟，包括附加的题目、用于笔记本电脑或PC的闪存卡和本书完整的英文电子版本。其细节在接下来这部分中介绍。

## 选配光碟内容

Sybex的《CIW：安全专家全息教程》选配光碟中包括相当多的培训资源，并提供很多模拟测试、积分考试和闪存卡，它们可帮助你对考试内容进行学习。选配光碟中还包括了完整的全息教程的电子版内容。选配光碟内容如下：

**Ebook** 很多人喜欢方便地在一张光碟上携带他们的全部全息教程。他们还希望能够通过计算机搜索文本，从而快捷、容易地发现具体的信息。因此，本全息教程的全部内容以PDF格式在选配光碟中提供。我们在选配光碟上还提供Adobe Acrobat Reader，它提供了PDF内容的界面以及查询功能。

**CIW Edge Tests** Edge Tests是一组多选题，它会帮助你准备考试。一共有三套题目：

- 两个积分考试，用来模拟真实的考试。
- 以电子测试器形式出现的全息教程中的所有复习题。可以逐章地或按目标范围地回顾这些题目，或者可以制定一个随机的测试。
- 评估测试。

**适用于PC和掌上设备的闪存卡** 闪存卡形式的题目提供了一个有效的方法，快速并且高效率地测试你对考试所涵盖的基本概念的理解。Sybex CIW闪存卡，在专为全息教程系列开发的专用引擎中包括150道题。我们还与Land-J Technologies携手，开发了一个闪存卡考题的版本，可以在你的掌上OS PDA（包括Palm和Visor PDA）中携带这些考题。

## 如何使用本书

本书提供了一个坚实的基础，可以使你认真地准备考试。为了从本书中获得最大的收益，希望你使用下面的学习方法：

1. 参加评估测试，确定你的薄弱环节。
2. 仔细学习每一章，尽全力理解书中提供的信息。
3. 学习考试要点和关键术语，确信熟悉这些需要集中精力学习的领域。
4. 复习题答案在每一章的结尾处。如果更喜欢以计时或计分的形式回答问题，那么可以从选配光碟中安装Edge Tests，并且回答其中每章的问题。
5. 在你没有理解的题目上做出标记，并重新学习书中对应的部分。
6. 从头复习考试要点和关键术语。
7. 完成选配光碟中包括的其他培训资源。这些包括电子闪存卡、每章复习题的电子版本（试着按考试对象分类去做）和两个积分考试。

为了学习本书中的所有内容，你需要定时、按要求进行学习。试着在每一天安排出相同的时间学习，并选择一个舒适、安静的地方去学习。如果你努力学习，那么你将会很惊讶你学得这么快。祝你好运！

## 考试注册

CIW认证证书由Prometric公司通过Prometric考试中心和Virtual University Enterprises（VUE）考试中心管理。你可以致电Prometric（800）380-EXAM或VUE（952）995-8800，确定任何一门CIW考试的时间。

**说明：** 你还可以在线注册考试，网址是www.prometric.com或www.vue.com。

每门考试费用为125美元，必须预先交付。考试必须在付款后的一年里进行。考生可以提前六周时间确定考试，或最晚至考试前的一个工作日。取消或重新安排考试的时间，至少提前考试日期的两个工作日与中心联系。在一些地区，同一天的注册是有效的，这取决于可用的考试席位。在同一天注册有效的地区，必须在考试时间前至少两个小时进行注册。

当确定考试时间的时候，考试中心会向你提供有关预约和取消手续的说明书、ID申请和考试中心位置信息。另外，你会从Prometric或VUE收到一份注册和付款确认信。

## 参加CIW安全专家考试的提示

这里有一些关于成功通过认证考试的常规提示：

- 早一点儿到达考试中心，这样你可以放松一下，并且回顾一下所学的内容。在这最后的回顾期间，你可以查看考试相关信息的表格和列表。
- 仔细阅读题目，不要过早地下结论，确信你确切地知道题目的含义。
- 对于那些没有把握的问题，利用排除法先去掉明显错误的答案。在需要做出有根据的猜测时，这样做增强了你选择正确答案的可能性。
- 标记没有把握的题目，稍后再回到这里。后面题目中经常出现的信息会提醒或提示你前面题目的正确答案。

## 联系方法和资源

这里是一些需要记住的使用方便的网站，可供将来参考：

| | |
|---|---|
| Prosoft培训和CIW考试信息 | www.CIWcertified.com |
| Prometric | www.prometric.com |
| VUE测试服务 | www.vue.com |
| Sybex计算机书籍 | www.sybex.com |
| Sybex中文版计算机书籍网上优惠购书 | www.medias.com.cn |

## 评估测试

1. Which of the following terms describes the time it takes for a server to fulfill a request from a client?
   A. Lag time
   B. Latency
   C. Media verification
   D. Delay

2. Which of the following operating system elements can a host-based IDS application augment?
   A. System authentication
   B. Data confidentiality
   C. System logging
   D. Data integrity

3. During an audit, which of the following can be used to responsibly provide proof of a system compromise?
   A. Web graffiti
   B. Locked-out user accounts
   C. Screen shots of penetrated resources
   D. Creation of user accounts

4. Which type of encryption scrambles text so that it is theoretically not recoverable?
   A. Public-key encryption
   B. Private-key encryption
   C. Symmetric encryption
   D. Hash encryption

5. Which of the following security elements creates perimeter security?
   A. A network vulnerability scanner
   B. An intrusion-detection system

C. A packet-filtering firewall

D. A server-based antivirus application

6. Which of the following can automatically detect an intrusion on a UNIX system?

A. Tripwire

B. Top

C. A login script

D. Crond

7. What Windows 2000 element holds the security settings for a particular object, such as a network share?

A. A security identifier (SID)

B. An access control list (ACL)

C. An access token (AT)

D. A security descriptor (SD)

8. A packet-filtering firewall has been able to detect a port scan, and has stored this information into a database. It has then reconfigured itself to block all connections from the scanning host. What term describes the ability for a packet-filtering firewall to detect port scans?

A. Packet filtering

B. Reverse circuit-level proxying

C. Chaining

D. Stateful multilayer inspection

9. Serena is using the Pretty Good Privacy (PGP) application. She has just received a public key from a friend and wishes to use it. What must she first do in order to use her friend's public key?

A. Place it into her e-mail client.

B. Sign it with her public key.

C. Use the ODBC applet to register it.

D. Import the key into her key ring.

10. Which of the following is not a feature provided by personal-firewall software?

A. Logging of packets sent to the host

B. Notification of an attack on the host

C. Notification of low password levels

D. Blocking of packets sent to the local host

11. What is the benefit of placing the operating system on one partition and the data files on another?

A. It protects against system bugs and buffer overflows.
B. It ensures that the operating system files cannot be overwritten.
C. It ensures that hackers cannot penetrate the system.
D. It helps contain a security breach.

12. Sandi has been asked to allow all SMTP, POP3, and IMAP traffic to pass from the internal network out to the Internet. She is configuring a proxy server to allow this traffic. The proxy server blocks all traffic unless it is explicitly permitted. Which ports will she have to open?
A. TCP ports 21, 110, and 143
B. TCP ports 25, 110, and 143
C. UDP ports 21, 110, and 143
D. UDP ports 25, 110, and 143

13. Jason changes his system's umask value from 002 to 200 on his Linux system. What permissions will newly created files have?
A. 664
B. 400
C. 466
D. 477

14. Eric wishes to encrypt transmissions between all of the hosts on his LAN. What can he use to do this?
A. IPsec
B. A firewall
C. Symmetric-key encryption
D. Public-key encryption

15. Ian is using his web browser to access the following URL: www.goodstuff.com/purchase/niceprogram.exe. However, the purchase directory is protected by an access control list (ACL). What step must take place before Ian is allowed to access the niceprogram.exe file?
A. He must provide an access token.
B. He must authenticate.
C. He must provide a password.
D. He must activate the execution control list.

16. Which of the following files can you edit without restarting the xinetd daemon?
A. /etc/hosts.deny
B. /etc/xinetd.conf
C. /etc/xinetd.d/telnet

此为试读，需要完整PDF请访问：www.ertongbook.com