CISSP Certified Information Systems Security Professional Study Guide

CISSP:

认证信息系统安全专家全息教程

Ed Tittel
〔美〕 Mike Chapple 著
James Michael Stewart

赵 菁 魏 巍 等译

本书在certcities.com网站上获得了“最受读者喜爱奖”的荣誉

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

SYBEX

美迪亚

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

CISSP: Certified Information
Systems Security Professional Study Guide

CISSP: 认证信息系统安全专家全息教程

Ed Tittel
〔美〕 Mike Chapple 著
James Michael Stewart
赵 菁 魏 巍 等译

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

内 容 提 要

本书用于准备CISSP考试，是由安全领域的专家编写的，作者对考试非常熟悉。书中提供评估考试，帮助读者指明学习方向。这是一本涵盖所有考试要点的权威著作，包括：访问控制和责任衡量、应用软件和系统开发、商业连续性计划、密码术、操作安全、物理安全、安全体系结构和模型、安全管理、通信和网络安全。本书不仅能帮助读者通过CISSP考试，而且可以在网络安全领域取得成功。

版权贸易合同登记号：01-2003-1088

图书在版编目（CIP）数据

CISSP：认证信息系统安全专家全息教程/（美）蒂泰尔（Tittel，E.）等著；赵菁等译.—北京：电子工业出版社，2003.10

书名原文：CISSP：Certified Information Systems Security Professional Study Guide

ISBN 7-5053-9126-7

Ⅰ.C… Ⅱ.①蒂… ②赵… Ⅲ.信息系统—安全技术—资格考核—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字（2003）第079232号

责任编辑：陈 宇

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：29.25 字数：740 千字

版 次：2003年10月第1版 2003年10月第1次印刷

定 价：48.00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。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

致 读 者

感谢你选择Sybex公司的图书作为CISSP认证考试的准备资料。CertCities.com网站最近将CISSP认证考试列为“2003年十大最热门的认证考试”之一，当然，这是毫无疑问的。由国际信息系统安全认证协会，即（ISC）²开发的，用来测试对信息安全国际标准掌握程度的CISSP认证考试，作为IT安全领域最权威的认证考试之一是值得参加的。

我们为Sybex公司能够给参加认证考试的人员提供实用的知识和技巧，在竞争激烈的IT领域获得成功而感到骄傲。在现实世界，教会用户如何使用技术，而不是简单地告诉他们如何回答考试问题，一直是Sybex公司的任务。正如（ISC）²所提倡的，要建立可衡量的标准，对那些工作在计算机和网络安全领域最前沿的专业人士进行认证。Sybex公司同样提倡，为那些专业人士提供符合这些标准的获得知识和技巧所需的方法。

Sybex公司的作者、编辑和技术评论家努力工作，保证这本学习指南的内容全面、深入和具有教学价值。我们相信，本书和包含在选配光碟中的测试软件学习工具，将满足并超过认证市场要求的认证标准，帮助参加CISSP认证考试的学员取得成功。

祝在CISSP的认证考试中一帆风顺！

Neil Edde
Sybex公司认证副总编

致　谢

感谢Sybex公司的Neil Edde和Jordan Gold，帮助我们选定这个项目。感谢Rodnay Zaks帮助我们想出了许多好主意。感谢我的父亲和母亲，为我提供了成为作家和教师的基本素质，即爱追根究底的精神和良好的口才与辩论技巧。感谢Dina Kutueva嫁给了我，组建了一个美好的家庭，使我的人生变得完美。最后，感谢LANWrights公司的团队成员：Dawn、Mary、Kim、Bill、Chelsea和Michael，他们给予我十年伟大的友情与合作，你们是最伟大的，没有你们，我将不会如此顺利地完成本书！

—Ed Tittel

我非常感谢Ed Tittel、Dawn Rader和LANWrights公司的团队成员对这个项目的帮助。我还要感谢那些在政府和行业中工作的、耐心回答我的问题并激励我这么多年从事安全领域工作的技术专家。最重要的是，我要感谢我的妻子Renee，在我写作此书时给予我无限耐心，没有她的支持，这一切都不会成为可能！

—Mike Chapple

感谢Ed Tittel和LANWrights公司，给了我这次机会完成本书的创作。与这些同事一起工作是我的荣幸。感谢我的编辑Dawn Rader容忍我糟糕的语法和提出的计划变动。感谢我的父母Dave和Sue、我的姐姐Sharon和外甥Wesley对我的爱和支持。我还要感谢Mark、HERbert和Quin，以及Elvis，感谢你们的帮助。

—James Michael Stewart

简　介

本书为读者提供了有关信息系统安全专家认证（CISSP）考试的完整基础知识。购买本书后，读者会自发地学习并期望不断提高完成认证考试的技能。简介为读者提供了本书和CISSP考试的基本概述。

本书是专为参加CISSP认证考试的读者和学生设计的。如果你的目标是要成为一个经过认证的安全专家，那么CISSP认证和这本学习指南就是为你写的。本书的目的就是要帮助你做好充分的准备通过CISSP认证考试。

在开始本书的学习之前，你需要先完成一些工作。你应该已经具有对IT和安全行业的一般理解。你应该具有CISSP考试所涵盖的十个领域中的一个领域4年的经验（或3年经验加上大学学位）。根据（ISC）²，如果你有资格参加CISSP考试，那么你可以通过使用本书充分地准备CISSP考试。有关（ISC）²的更多信息，参见简介部分（ISC）²的介绍。

如何使用本书

对于任何教程或准备考试的书籍，你花费在阅读资料和做练习上的时间越多，你记住的东西就越多。我们并不强调必须理解本书所讲述的全部概念。

为了从本书学到更多的东西，下面推荐一个学习过程：

1. 认真并完整地阅读每一章。
2. 复习每章最后概括出的需要重点理解的知识。
3. 完成每章最后的复习题。如果你有任何问题，请重新阅读书中包括这个问题的相关部分。
4. 阅读完本书后，完成本书选配光碟上的考试练习题。
5. 打印出闪存卡上的内容，进一步强化学习过程。

本书的组织结构

本书涵盖了10个CISSP通用知识体系（CBK）领域，为读者能够清楚地理解书中的内容，对每一个领域都进行了深入详细的讨论。本书的主要内容共19章，前九个领域分别包含在两章中，最后一个领域（物理安全）涵盖在第19章中。领域/章的安排如下：

第1章和第2章　访问控制系统和方法
第3章和第4章　通信和网络安全
第5章和第6章　安全管理原则
第7章和第8章　应用软件和系统开发安全
第9章和第10章　密码技术
第11章和第12章　安全体系结构和模型
第13章和第14章　操作安全
第15章和第16章　商业连续性计划（BCP）和灾难恢复计划（DRP）

第17章和第18章 法律、调查和道德规范

第19章 物理安全

每章中包括的基础知识用来帮助读者强化学习重点和测试掌握知识的程度，其中包括考试要点、关键术语和复习题。考试要点指出考试中要求的关键目标。关键术语表包括这一章中的重要术语。为了查找方便，在本书最后的词汇表中对每个关键术语都进行了定义。复习题用来测试读者对这一章知识的掌握程度。

本书有一个选配光碟，提供了许多其他的学习工具，其中包括较长的考试练习题（超过700个问题）和一套完整的学习闪存卡。

（ISC）²

CISSP考试由国际信息系统安全认证协会（International Information Systems Security Certification Consortium）管理。（ISC）²是一个全球性的非盈利性组织。它有四个主要的任务目标：

- 维护信息系统安全领域的通用知识体系；
- 为信息系统安全专业人士和从业者提供认证；
- 从事认证考试的培训和对认证考试进行管理；
- 通过连续的教育培训，对有资格的认证候选人的授权工作进行管理。

（ISC）²由董事会运作，董事会成员从经过认证的从业者中按级别进行选举。有关（ISC）²的更多信息，可以从网站www.isc2.org中获得。

CISSP和SSCP

（ISC）²支持并提供两种主要的认证考试：CISSP和SSCP。这些认证考试用来对所有行业的IT安全专业人士进行知识和技能的强化。CISSP是为从事组织机构安全体系构建的安全专业人士设计的认证考试。系统安全从业者（SSCP）是为在组织机构中负责实施安全基础体系的安全专业人士设计的认证考试。CISSP认证考试涵盖了先前列出的10个CBK领域的知识。SSCP认证考试涵盖了7个CBK领域的知识：

- 访问控制
- 管理
- 审计和监控
- 密码技术
- 数据通信
- 恶意代码/Malware
- 风险、响应和灾难恢复

CISSP和SSCP认证考试内容所涉及的领域有重复的地方，但它们有各自不同的侧重点。CISSP关注理论和设计，而SSCP更多关注安全实施的内容。本书的重点只集中在CISSP考试所涉及的领域。

道德规范

（ISC）²已经定义了成为CISSP所必须满足的几项资格。首先，你必须是一位至少有4

年安全从业经验或3年经验加学士学位的专业人士。专业经验的定义是：在10个CBK领域中的一个或多个领域从事有工资收入的安全工作。

其次，你必须同意遵守道德规范。CISSP的道德规范是一套准则，为了维护信息系统安全领域的职业道德，（ISC）²希望所有的CISSP候选人都要遵守。你可以在（ISC）²网站www.isc2.org的信息部分找到这些规范准则。

要想报名参加考试，请访问（ISC）²的网站，并按照所列出的参加CISSP考试的指导完成注册。请提供你的联系方式、付款信息和有关安全行业的专业经验。你还要选择可以参加考试的时间和地点。一旦（ISC）²同意你参加考试，你将会收到一封进行确认的电子邮件，在邮件中你会找到有关测试中心和如何参加考试的详细信息。

CISSP考试概述

CISSP考试由250个问题组成，用6个小时完成。考试时使用一本小册子和答案纸，也就是说，你要使用铅笔来填写答案框。

CISSP考试从很深的角度关注安全，它更注重安全理论和概念，而不是实施过程和方法。考试所涉及的范围非常宽，但不是很深。为了成功通过考试，你需要熟悉每个领域，但没有必要成为每个领域的专家。

你需要通过（ISC）²的网站www.isc2.org来进行考试注册。

（ISC）²负责管理考试。在大多数情况下，考试在酒店的大会议室中举行。CISSP现在的所有者作为考试的监考人或系统管理员。请保证在早上8 :00左右到达考试中心，并且记住，早上8 :30之后进入考场是不允许的。

CISSP考试问题的类型

CISSP考试的每一道题有四个选项，但只有一个正确答案。下面是一个例子：

1. What is the most important goal and top priority of a security solution?
   A. Prevention of disclosure
   B. Maintaining integrity
   C. Human safety
   D. Sustaining availability

你必须选择一个正确的或是最合适的答案，并把它标记在你的答案纸上。在一些情况中，正确答案是非常明显的。但在有些情况中，可能会有几个答案看上去都是正确的，在这个时候，你必须选择对于这道问题最合适的答案。留意那些一般性的、明确的、全面的、扩展集和子集的答案选项。如果在某些情况下，似乎没有一个答案正确，那么你就要选择错误的可能性最小的答案。

参加考试的建议

参加CISSP考试时有两个关键要素。首先，需要了解10个CBK领域所涉及的内容。其次，一定要有很好的参加测试的技巧。要想在6个小时内完成250个问题的考试，回答每个问题所需的时间不能超过90秒。因此，速度快很重要，虽然不能仓促但也不要浪费时间。

要记住，猜测答案也比不回答问题强。如果你跳过一个问题，将没有得分。但是，如

果猜测答案，至少有25%的正确机会。答案错误是不扣分的。因此，在6个小时考试快结束的时候，确认答案纸上的每一道题都有答案。

你可以在测试的小册子上写字，但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和掌握考试进度。我们建议，在你把答案标记在答案纸上之前，再看一下你选择的每一个答案。

为了激发你参加考试的最大潜能，以下是一些一般性的指导原则：

1. 首先回答容易的问题。
2. 跳过较难的问题，稍后再返回来思考。为了记住被跳过的问题，在测试小册子的封面上记下它们的题号。
3. 在选择正确的答案之前，先排除错误的答案。
4. 注意双重否定的问题。
5. 确认了解问题问的是什么。

合理安排时间。你应该在一小时之内回答大约50个问题。这样，可以留下一个小时左右的时间用来重新考虑跳过的问题。

一定注意要把答案填写在答案纸上的正确的题号下。最容易犯的错误就是考试小册子上的题号与答案纸上的题号顺序发生了错位。

学习和考试准备要领

在CISSP考试学习的过程中，我们建议安排一个月的时间进行学习或每晚强化学习。这里有一些提议，可以帮助你充分利用学习时间。你可以根据自己的学习习惯来安排它们：

- 花一到两个晚上阅读每一章的内容并进行复习。
- 参加本书和选配光碟上所提供的所有练习考试。
- 从网站www.isc2.org上查阅（ISC）²的教程。
- 使用闪存卡强化你对概念的理解。

评估考试

1. In what phase of the Capability Maturity Model for Software are quantitative measures utilized to gain a detailed understanding of the software development process?
   A. Repeatable
   B. Defined
   C. Managed
   D. Optimizing

2. You are the security administrator of a large law firm. You have been asked to select a security model that supports your organization's desire to ensure data confidentiality and integrity. You must select one or more models that will protect data from internal and external attacks. What security model(s) will you choose? (Choose all that apply.)

A. Bell-LaPadula
B. Biba
C. Clark-Wilson
D. TCSEC

3. Why are military and intelligence attacks among the most serious computer crimes?
A. The use of information obtained can have far-reaching detrimental strategic effect on national interests in an enemy's hands.
B. Military information is stored on secure machines, so a successful attack can be embarrassing.
C. The long-term political use of classified information can impact a country's leadership.
D. The military and intelligence agencies have ensured that laws protecting their information are the most severe.

4. What is the length of a message digest produced by the MD5 algorithm?
A. 64 bits
B. 128 bits
C. 256 bits
D. 384 bits

5. Which of the following is most likely to detect DoS attacks?
A. Host-based IDS
B. Network-based IDS
C. Vulnerability scanner
D. Penetration testing

6. How is annualized loss expectancy (ALE) calculated?
A. Single loss expectancy × asset value
B. Asset value × exposure factor
C. Annualized rate of occurrence × vulnerability
D. Single loss expectancy (SLE) × annualized rate of occurrence (ARO)

7. At what height and form will a fence deter determined intruders?
A. 3- to 4-feet high chain link
B. 6- to 7-feet high wood
C. 8-feet high with 3 strands of barbed wire
D. 4- to 5-feet high concrete

8. A VPN can be established over which of the following?
A. Wireless LAN connection
B. Remote access dial-up connection

C. WAN link

D. All of the above

9. What is the Biba access control model primarily based upon?

A. Identity

B. Analog

C. Military

D. Lattice

10. Which one of the following database backup techniques requires the greatest expenditure of funds?

A. Transaction logging

B. Remote journaling

C. Electronic vaulting

D. Remote mirroring

11. What is the value of the logical operation shown here?

X: 0 1 1 0 1 0

Y: 0 0 1 1 0 1

X ∨ Y: ?

A. 0 1 1 1 1 1

B. 0 1 1 0 1 0

C. 0 0 1 0 0 0

D. 0 0 1 1 0 1

12. Which one of the following security modes does not require that a user have a valid security clearance for all information processed by the system?

A. Dedicated mode

B. System-high mode

C. Compartmented mode

D. Multilevel mode

13. You are the security administrator for an international shipping company. You have been asked to evaluate the security of a new shipment tracking system for your London, U.K., office. It is important to evaluate the security features and assurance of the system separately in order to compare it to other systems that management is considering. What evaluation criteria should you use?

A. TCSEC

B. ITSEC

C. The Blue Book

D. IPSec

14. What is the last phase of the TCP/IP three-way handshake sequence?
    A. SYN packet
    B. ACK packet
    C. NAK packet
    D. SYN/ACK packet

15. Which of the following is a requirement of change management?
    A. Changes must comply with Internet standards.
    B. All changes must be capable of being rolled back.
    C. Upgrade strategies must be revealed over the Internet.
    D. The audit reports of change management should be accessible to all users.

16. Which of the following is a procedure designed to test and perhaps bypass a system's security controls?
    A. Logging usage data
    B. War dialing
    C. Penetration testing
    D. Deploying secured desktop workstations

17. At which layer of the OSI model does a router operate?
    A. Network layer
    B. Layer 1
    C. Transport layer
    D. Layer 5

18. Which of the following is considered a denial of service attack?
    A. Pretending to be a technical manager over the phone and asking a receptionist to change their password
    B. While surfing the Web, sending to a web server a malformed URL that causes the system to use 100 percent of the CPU to process an endless loop
    C. Intercepting network traffic by copying the packets as they pass through a specific subnet
    D. Sending message packets to a recipient who did not request them simply to be annoying

19. Audit trails, logs, CCTV, Intrusion Detection Systems, antivirus software, penetration testing, password crackers, performance monitoring, and cyclical redundancy checks (CRCs) are examples of what?
    A. Directive controls
    B. Preventive controls
    C. Detective controls
    D. Corrective controls

20. Which one of the following vulnerabilities would best be countered by adequate parameter checking?
    A. Time-of-check-to-time-of-use
    B. Buffer overflow
    C. SYN flood
    D. Distributed denial of service

21. What technology allows a computer to harness the power of more than one CPU?
    A. Multitasking
    B. Multiprocessing
    C. Multiprogramming
    D. Multithreading

22. What type of backup stores all files modified since the time of the most recent full backup?
    A. Full backup
    B. Incremental backup
    C. Partial backup
    D. Differential backup

23. What law allows ISPs to voluntarily provide government investigators with a large range of user information without a warrant?
    A. Electronic Communications Privacy Act
    B. Gramm-Leach-Bliley Act
    C. USA Patriot Act
    D. Privacy Act of 1974

24. What type of detected incident allows the most time for an investigation?
    A. Compromise
    B. Denial of service
    C. Malicious code
    D. Scanning

25. Auditing is a required factor to sustain and enforce what?
    A. Accountability
    B. Confidentiality
    C. Accessibility
    D. Redundancy

26. Which type of firewall automatically adjusts its filtering rules based on the content of the traffic of existing sessions?
    A. Static packet-filtering
    B. Application-level gateway

C. Stateful inspection

D. Dynamic packet-filtering

27. Which one of the following is a layer of the ring protection scheme that is not normally implemented in practice?

A. Layer 0

B. Layer 1

C. Layer 3

D. Layer 4

28. What type of cipher rearranges the letters of the plaintext message to form the ciphertext?

A. Substitution cipher

B. Block cipher

C. Transposition cipher

D. One-time pad

29. What is the formula used to compute the ALE?

A. ALE = AV × EF

B. ALE = ARO × EF

C. ALE = AV × ARO

D. ALE = EF × ARO

30. Which of the following is the principle that objects retain their veracity and are only intentionally modified by authorized subjects?

A. Privacy

B. Authentication

C. Integrity

D. Data hiding

31. E-mail is the most common delivery vehicle for which of the following?

A. Viruses

B. Worms

C. Malicious code

D. All of the above

32. What type of physical security controls are access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression?

A. Technical

B. Administrative

C. Physical
D. Preventative

33. In the United States, how are the administrative determinations of federal agencies promulgated?
A. Code of Federal Regulations
B. United States Code
C. Supreme Court decisions
D. Administrative declarations

34. What is the first step of the Business Impact Assessment process?
A. Identification of priorities
B. Likelihood assessment
C. Risk identification
D. Resource prioritization

35. If Renee receives a digitally signed message from Mike, what key does she use to verify that the message truly came from Mike?
A. Renee's public key
B. Renee's private key
C. Mike's public key
D. Mike's private key

36. The "something you are" authentication factor is also known what?
A. Type 1
B. Type 2
C. Type 3
D. Type 4

37. What is the primary goal of risk management?
A. To produce a 100-percent risk-free environment
B. To guide budgetary decisions
C. To reduce risk to an acceptable level
D. To provide an asset valuation for insurance

评估考试答案

1. C。SW-CMM的管理过程设计涉及定量开发标准的使用。SEI为这一级定义了主要处理区域，作为定量处理管理和软件质量管理。更多的内容，请参见第7章。

2. A、C。由于公司需要确保保密性，因此你应该选择Bell-LaPadula模型。为了确保数据的完整性，还应当使用模型，它将对职责的分离进行说明。这个特性可以用来更好地保护系统免受内部和外部的攻击。更多的内容，请参见第12章。

3. A。军事和智能攻击的目的是获取分类信息。使用这种信息的不利结果可能导致敌人掌握几乎无限制的访问权利。这种类型的攻击通常是由非常有经验的攻击者发起的。常常很难确定对方成功获取了什么文件。因此当这种类型的破坏发生时，有时你并不能知道全部的破坏程度。更多的内容，请参见第18章。

4. B。MD5算法为任意的输入内容生成一个128位报文摘要。更多的内容，请参见第10章。

5. B。网络型的IDS通常可以检测到一个攻击的开始，或正在进行的攻击企图（包括DoS）。然而，它们不能够提供是否攻击已经成功的信息，或者是哪个特定的系统、用户账户、文件或应用受到影响。主机型的IDS检测和跟踪DoS攻击有一些困难。弱点扫描仪不检测DoS攻击，它对可能的弱点进行监测。渗透测试可能执行DoS或DoS弱点的测试，但它不是检测工具。更多的内容，请参见第2章。

6. D。年损益预算（annualized loss expectancy，ALE）是已经明确识别的对于特定资产的威胁每年所造成的开销。ALE使用公式：单一损益预算（single loss expectancy，SLE）×年事件发生率（annualized rate of occurrence，ARO）。更多的内容，请参见第6章。

7. C。由三股线绞成的带刺的8英尺高的围墙挡住了坚定的入侵者。更多的内容，请参见第19章。

8. D。VPN链接可以在任何其他的网络通信连接上建立。这可能是一条典型的局域网线缆连接、一条无线局域网连接、一条远程拨号访问连接、一条广域网链接，甚至是一条用户访问公司局域网的因特网连接。更多的内容，请参见第4章。

9. D。Biba还是建立在带有强制访问控制的分类格子基础上的状态机模型。更多的内容，请参见第1章。

10. D。远程镜像保持了远程节点上的有效的数据库服务器，并且成本最高。更多的内容，请参见第16章。

11. A。符号∨代表了或（OR）操作，当一个或者两个输入位都是真时，结果为真。更多的内容，请见第9章。

12. D。在多级安全模式中，一些用户对于系统处理的所有信息不具有有效的安全性许可。更多的内容，请参见第11章。

13. B。ITSEC在欧洲为评估系统而开发。虽然TCSEC（也称做橘皮书）将满足评估标准，但是只有ITSEC对功能性和质量保证进行了分别的评估。更多的内容，请参见第12章。

14. B。SYN包是从初始主机向目标主机发送的第一个包。然后目标主机利用SYN/ACK包进行回应。初始主机发出ACK包，然后连接建立。更多的内容，请参见第8章。

15. B。变动管理的一个要求是所有的变动都必须能够回退到原来的状态。更多的内容，请参见第5章。

16. C。渗透测试是指为了测试所有系统安全性而通过安全性控制的企图。更多的内容，请参见第14章。

17. A。网络硬件设备（包括路由器）工作在第3层，即网络层。更多的内容，请参见第3章。

18. B。不是所有的DoS事件都会导致恶意攻击。操作系统代码、服务和应用程序中的错误都已成为DoS的条件。有关这种情况的例子包括进程无法释放对CPU的控制，或者某个服务占用的资源超出了服务请求的范围。社会工程学和探测技术并不是特别针对DoS攻击的。更多的内容，请参见第2章。

19. C。探测控制的例子包括审核跟踪、日志记录、闭路电视、入侵监测系统、反病毒软件、渗透测试、密码解密、性能监控和CRC。更多的内容，请参见第13章。

20. B。参数检查用来防止缓冲区溢出攻击的可能性。更多的内容，请参见第8章。

21. B。多处理器计算机使用多个处理器，采用对称多处理（symmetric multiprocessing，SMP）或大规模并行处理器（massively parallel processing，MPP）的配置。更多的内容，请参见第11章。

22. D。差异备份对最近的完全备份以来修改过的所有文件进行存储。更多的内容，请参见第16章。

23. C。美国的爱国者法案对法律执行赋予了新的宽泛的权力，包括招揽自愿的ISP合作。更多的内容，请参见第17章。

24. D。对易发生的事件进行扫描通常是对攻击的搜索。对于系统的真正的攻击来自于后续的攻击，因此如果提早监测到攻击，那么还可能有时间做出应对。更多的内容，请参见第18章。

25. A。审核是持续进行的加强责任衡量所需要的一个因素。更多的内容，请参见第14章。

26. D。动态的包过滤防火墙使得基于信息传输内容的过滤规则可以进行实时的改动。更多的内容，请参见第3章。

27. B。第1层和第2层包含设备的驱动程序，但是实际上通常没有执行。第0层包含用户的应用程序。第4层不存在。更多的内容，请参见第7章。

28. C。更改顺序的密码使用加密算法重新安排明码报文的文字，形成密码报文。更多的内容，请参见第9章。

29. C。年损益预算（ALE）按照评估值（AV）乘以年事件发生率（ARO）所得乘积进行计算。更多的内容，请参见第15章。