EXAM CRAM

CISSP

Practice Questions

Fourth Edition

PEARSON IT
CERTIFICATION

MICHAEL GREGG

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

EXAM CRAM

CISSP

Practice Questions

Fourth Edition

Michael Gregg

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

CISSP Practice Questions Exam Cram, Fourth Edition

Copyright © 2016 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5559-9
ISBN-10: 0-7897-5559-9

Library of Congress Control Number: 2016937730

Printed in the United States of America

First Printing: June 2016

Trademarks
All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer
Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the book website or programs accompanying it.

Special Sales
For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Executive Editor
Brett Bartow

Acquisitions Editor
Betsy Brown

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Project Editor
Tonya Simpson

Copy Editor
Linda Morris

Proofreader
Suriya Narayanan

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

	Introduction	1
CHAPTER 1	Security and Risk Management	7
CHAPTER 2	Asset Security	45
CHAPTER 3	Security Engineering	77
CHAPTER 4	Communications and Network Security	121
CHAPTER 5	Identity and Access Management	167
CHAPTER 6	Security Assessment and Testing	207
CHAPTER 7	Security Operations	241
CHAPTER 8	Software Development Security	279
CHAPTER 9	The Application and Use of Cryptography	317
CHAPTER 10	Business Continuity Planning	361

Table of Contents

Introduction **1**

Chapter 1:
Security and Risk Management **7**

Practice Questions 9
Practice Questions (True or False) 29
Practice Questions (Mix and Match) 30
Quick-Check Answer Key 33
Answers and Explanations 35

Chapter 2:
Asset Security **45**

Practice Questions 46
Practice Questions (True or False) 61
Practice Questions (Mix and Match) 63
Quick-Check Answer Key 65
Answers and Explanations 67

Chapter 3:
Security Engineering **77**

Practice Questions 79
Practice Questions (True or False) 102
Practice Questions (Mix and Match) 102
Quick-Check Answer Key 105
Answers and Explanations 107

Chapter 4:
Communications and Network Security **121**

Practice Questions 122
Practice Questions (True or False) 145
Practice Questions (Mix and Match) 146
Quick-Check Answer Key 149
Answers and Explanations 151

Chapter 5:
Identity and Access Management **167**

Practice Questions 169
Practice Questions (True or False) 187
Practice Questions (Mix and Match) 190
Quick-Check Answer Key 192
Answers and Explanations 194

Chapter 6:
Security Assessment and Testing **207**

Practice Questions 209
Practice Questions (True or False) 227
Practice Questions (Mix and Match) 228
Quick-Check Answer Key 229
Answers and Explanations 230

Chapter 7:
Security Operations **241**

Practice Questions 242
Practice Questions (True or False) 260
Practice Questions (Mix and Match) 262
Quick-Check Answer Key 264
Answers and Explanations 266

Chapter 8:
Software Development Security **279**

Practice Questions 280
Practice Questions (True or False) 301
Practice Questions (Mix and Match) 303
Quick-Check Answer Key 304
Answers and Explanations 306

Chapter 9:
The Application and Use of Cryptography **317**

Practice Questions 318
Practice Questions (True or False) 339
Practice Questions (Mix and Match) 342
Quick-Check Answer Key 345
Answers and Explanations 347

Chapter 10:
Business Continuity Planning **361**

Practice Questions 363
Practice Questions (True or False) 387
Practice Questions (Mix and Match) 387
Quick-Check Answer Key 389
Answers and Explanations 391

About the Author

As the CEO of Superior Solutions, Inc., a Houston-based IT security consulting and auditing firm, Michael Gregg has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISSP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, CGEIT, and SSCP.

In addition to his experience with performing security audits and assessments, Gregg has authored or coauthored more than 20 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has served as an expert witness before the United States Congress and has been quoted on Fox News, CNN, ABC, CBS, NBC, *The New York Times*, and other media outlets. His articles have been published on IT websites such as TechTarget and he writes for the Huffington Post. He has created more than 15 security-related courses and training classes for various companies and universities.

Although audits and assessments are where he spends the bulk of his time, teaching and contributing to the written body of IT security knowledge are how Michael believes he can give something back to the community that has given him so much. He is a board member for Habitat for Humanity, works with United Way, and, when not working, enjoys traveling and restoring muscle cars.

Dedication

I would like to dedicate this book to my parents, W. P. and Betty Gregg. They both sacrificed to help me achieve my dreams.

Acknowledgments

I would like to offer a big "thank you" to my wife Christine and all my family. A special thanks to all the people of Pearson who helped edit and review this book.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CISSP Practice Questions Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789755599 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to the *CISSP Practice Questions Exam Cram*! This book contains practice questions, complete with answers and explanations, that help you learn, drill, and review for the Certified Information Systems Security Professional (CISSP) certification exam.

Who This Book Is For

If you have studied the CISSP exam's content and you believe that you are ready to put your knowledge to the test, but you're not sure you want to take the actual exam yet, this book is for you! Maybe you have answered other practice questions or unsuccessfully taken the real exam, reviewed, and wanted to do more practice questions before retaking the exam. If so, this book is for you, too!

Be aware that the *CISSP exam is difficult and challenging*; therefore, this book shouldn't be your only vehicle for CISSP study. Because of the breadth and depth of knowledge needed to successfully pass the CISSP exam, you should use plenty of different study materials and use this book as a drill, review, and practice vehicle. It is recommended that you use this book with the *CISSP Exam Cram*, Fourth Edition (published by Pearson IT Certification), by Michael Gregg.

What You Will Find in This Book

This book is all about practice questions. It is divided into the eight domains that you find on the CISSP exam. The first eight chapters represent a corresponding domain, with the remaining two chapters covering topics found in a few domains or covering material that needs significantly more coverage. Each chapter has three elements:

- **Practice Questions:** This section includes numerous questions that help you learn, drill, and review.
- **Quick-Check Answer Key:** After you finish answering the questions, you can quickly grade your exam from this section. Only the correct answers are given here. No explanations are offered yet.
- **Answers and Explanations:** This section gives the correct answers and detailed explanations about the content posed in that question. Use this information to learn why an answer is correct and reinforce the content in your mind for exam day.

Hints for Using This Book

Because this book is a paper practice product, you might want to complete its exams on separate pieces of paper so that you can reuse the exams without having previous answers in your way. Also, a rule of thumb across all practice-question products is to make sure that you score into the high 90-percent range in all topics before attempting the actual exam. The higher you score on practice-question products, the better your chances of passing the real exam. Of course, we can't guarantee that you will receive a passing score on the real exam, but we can offer you plenty of opportunities to practice and assess your knowledge levels before you take the exam.

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box to indicate that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789755599
3. Answer the challenge question as proof of purchase.
4. Click on the Access Bonus Content link in the Registered Products section of your account page to go to the page where downloadable content is available.

Please note that many of our companion content files, especially image and video files, can be very large.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

Pearson IT Certification Practice Test Engine and Questions

The companion website includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode, or take a simulated exam that mimics real exam conditions. You can also serve up questions in a Flash Card Mode, which will display just the question and no answers, challenging you to state the answer in your own words before checking the actual answers to verify your work.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam (the database of exam questions) is not on this site.

NOTE

The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code.

Install the Software

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows 10, Windows 8.1, or Windows 7
- Microsoft .NET Framework 4.0 Client
- Pentium-class 1GHz processor (or equivalent)
- 512MB RAM
- 650MB disk space plus 50MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the access code card sleeve in the back of the book.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to windows prompts as with any typical software installation process.

The installation process will give you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

After the exam engine is installed, activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate Exam** button.
3. At the next screen, enter the activation key from paper inside the cardboard sleeve in the back of the book. After you've entered the key, click the **Activate** button.
4. The activation process will download the practice exam. Click **Next**, and then click **Finish**.

When the activation process completes, the My Products tab should list your new exam. If you do not see the exam, make sure that you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, display the **Tools** tab and click the **Update Products** button. Updating your exams will ensure that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson IT Certification Practice Test exam engine software, display the **Tools** tab and click the **Update Application** button. You can then ensure that you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process and the registration process only have to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another Pearson IT Certification Guide, extract the activation code from the cardboard sleeve in the back of that book; you do not even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running) and perform Steps 2 through 4 from the previous list.

Need Further Study?

If you have a difficult time correctly answering these questions, you probably need further review. Read the sister product to this book, *CISSP Exam Cram*, Fourth Edition (published by Pearson IT Certification), for further review.

This page intentionally left blank

5

CHAPTER FIVE

Identity and Access Management

The Identity and Access Management domain tests your knowledge of the large collection of mechanisms available to control authentication, authorization, and accounting. You must not only understand these systems, but also know the advantages and risks of each type as they relate to centralized and decentralized systems. Authentication is but one part of the process; authorization is also a key area of this domain. Individuals should be authorized for only what they need to complete their required tasks. Finally, there is accounting (or accountability). When things go wrong, there must be a way to establish a chain of responsibility. The following list highlights some key areas from the identity and access management domain you need to be aware of for the CISSP exam:

- Managing identification and authentication
- Authentication methods (types 1, 2, and 3)
- Authorization: DAC, MAC, role-based access control, and rule-based access control
- Integrating identity as a service (for example, cloud identity)
- Integrating third-party identity services (for example, on-premise)
- Accounting: Logging, monitoring, auditing
- Central, decentralized, and hybrid management

- Single sign-on: Kerberos, RADIUS, Diameter, TACACS
- Access control attacks: emanations, impersonation, and password cracking

TIP

Keep in mind that the CISSP exam is offered worldwide. Just because you perform activities in a specific way at your worksite does not mean that specific methodology is the best answer for the exam. As an example, privacy laws are different in Europe than in the United States.

Quick Check

Practice Questions

1. Which of the following is not one of the three types of access controls?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** Administrative
- ❍ **B.** Personnel
- ❍ **C.** Technical
- ❍ **D.** Physical

2. Your company has just opened a call center in India to handle nighttime operations, and you are asked to review the site's security controls. Specifically, you are asked which of the following is the strongest form of authentication. What will your answer be?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** Something you know
- ❍ **B.** Something you are
- ❍ **C.** Passwords
- ❍ **D.** Tokens

3. Your organization has become worried about recent attempts to gain unauthorized access to the R&D facility. Therefore, you are asked to implement a system that will require individuals to present a password and enter a PIN at the security gate before gaining access. What is this type of system called?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** Authorization
- ❍ **B.** Two-factor authentication
- ❍ **C.** Authentication
- ❍ **D.** Three-factor authentication

4. Which of the following is not one of the three primary types of authentication?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** Something you remember
- ❍ **B.** Something you know
- ❍ **C.** Something you are
- ❍ **D.** Something you have

5. While working as a contractor for Widget, Inc., you are asked what the weakest form of authentication is. What will you say?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** Passwords
- ❍ **B.** Retina scans
- ❍ **C.** Facial recognition
- ❍ **D.** Tokens

Quick Check

6. You're preparing a presentation for the senior management of your company. They have asked you to rank the general order of accuracy of the most popular biometric systems, with 1 being the lowest and 5 being the highest. What will you tell them?

Quick Answer: **192**
Detailed Answer: **194**

- ❍ **A.** (1) fingerprint, (2) palm scan, (3) hand geometry, (4) retina scan, (5) iris scan
- ❍ **B.** (1) fingerprint, (2) palm scan, (3) iris scan, (4) retina scan, (5) hand geometry
- ❍ **C.** (1) palm scan, (2) hand geometry, (3) iris scan, (4) retina scan, (5) fingerprint
- ❍ **D.** (1) hand geometry, (2) palm scan, (3) fingerprint, (4) retina scan, (5) iris scan

7. Which of the following items is the least important to consider when designing an access control system?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** Risk
- ❍ **B.** Threat
- ❍ **C.** Vulnerability
- ❍ **D.** Annual loss expectancy

8. Today, you are meeting with a coworker who is proposing that the number of logins and passwords be reduced. Another coworker has suggested that you investigate single sign-on technologies and make a recommendation at the next scheduled meeting. Which of the following is a type of single sign-on system?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** Kerberos
- ❍ **B.** RBAC
- ❍ **C.** DAC
- ❍ **D.** SAML

9. Which style of authentication is not susceptible to a dictionary attack?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** CHAP
- ❍ **B.** LEAP
- ❍ **C.** WPA-PSK
- ❍ **D.** PAP

Quick Check

10. Your organization has decided to use a biometric system to authenticate users. If the FAR is high, what happens?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** Legitimate users are denied access to the organization's resources.
- ❍ **B.** Illegitimate users are granted access to the organization's resources.
- ❍ **C.** Legitimate users are granted access to the organization's resources.
- ❍ **D.** Illegitimate users are denied access to the organization's resources.

11. Which of the following types of copper cabling is the most secure against eavesdropping and unauthorized access?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** Single-mode fiber
- ❍ **B.** Multimode fiber
- ❍ **C.** Category 6 cabling
- ❍ **D.** 802.11ac wireless

12. Which of the following is not one of the four access control models?

Quick Answer: **192**
Detailed Answer: **195**

- ❍ **A.** Discretionary
- ❍ **B.** Mandatory
- ❍ **C.** Role-based
- ❍ **D.** Delegated

13. Auditing is considered what method of access control?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Preventive
- ❍ **B.** Technical
- ❍ **C.** Administrative
- ❍ **D.** Physical

14. What method of access control system would a bank teller most likely fall under?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Discretionary
- ❍ **B.** Mandatory
- ❍ **C.** Role-based
- ❍ **D.** Rule-based

Quick Check

15. Which of the following is the easiest and most common form of offline password hash attack used to pick off insecure passwords?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Hybrid
- ❍ **B.** Dictionary
- ❍ **C.** Brute-force
- ❍ **D.** Man-in-the-middle

16. Your company is building a research facility in Bangalore and is concerned about technologies that can be used to pick up stray radiation from monitors and other devices. Specifically, your boss wants copper shielding installed. Which technology does your boss want to know more about?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Radon
- ❍ **B.** Waveguard
- ❍ **C.** Tempest
- ❍ **D.** Van Allen

17. Which of the following is an XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and a service provider?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** SAML
- ❍ **B.** LDAP
- ❍ **C.** OAuth
- ❍ **D.** KryptoKnight

18. Christine, a newly certified CISSP, has offered to help her brother-in-law, Gary, at his small construction business. The business currently has 18 computers configured as a peer-to-peer network. All users are responsible for their own security and can set file and folder privileges as they see fit. Which access control model best describes the configuration at this organization?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Discretionary
- ❍ **B.** Mandatory
- ❍ **C.** Role-based
- ❍ **D.** Nondiscretionary

19. Which of the following best describes challenge/response authentication?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** It is an authentication protocol in which a salt value is presented to the user, who then returns an MD5 hash based on this salt value.

Quick Check

- ❍ **B.** It is an authentication protocol in which a system of tickets is used to validate the user's rights to access resources and services.
- ❍ **C.** It is an authentication protocol in which the username and password are passed to the server using CHAP.
- ❍ **D.** It is an authentication protocol in which a randomly generated string of values is presented to the user, who then returns a calculated number based on those random values.

20. Your company has installed biometric access control systems. Your director has mentioned that he thinks the systems will have a high FRR. What does this mean?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Quite a few valid users will be denied access.
- ❍ **B.** Employees will accept the system.
- ❍ **C.** Almost all unauthorized users will be denied.
- ❍ **D.** The system has a high return rate and will quickly pay for itself.

21. Which of the following is the most time-intensive type of offline password attack to attempt?

Quick Answer: **192**
Detailed Answer: **196**

- ❍ **A.** Hybrid
- ❍ **B.** Plain text
- ❍ **C.** Brute-force
- ❍ **D.** Man-in-the-middle

22. You are approached by a junior security officer who wants to know what CVE stands for. What do you tell him?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Critical Vulnerability and Exploits
- ❍ **B.** Common Vulnerabilities and Exposures
- ❍ **C.** Chosen Vulnerabilities and Exploits
- ❍ **D.** Common Vulnerabilities and Exploits

23. Which of the following protocols is recommended to be turned off because it transmits usernames and passwords in plaintext?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** SSH
- ❍ **B.** HTTPS
- ❍ **C.** Telnet
- ❍ **D.** TFTP

Quick Check

24. Which biometric authentication system is most closely associated with law enforcement?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Fingerprint recognition
- ❍ **B.** Iris recognition
- ❍ **C.** Facial recognition
- ❍ **D.** Retina pattern recognition

25. What type of access control system doesn't give users much freedom to determine who can access their files and is known for its structure and use of security labels?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Discretionary
- ❍ **B.** Mandatory
- ❍ **C.** Role-based
- ❍ **D.** Nondiscretionary

26. As the newly appointed security officer for your corporation, you suggest replacing the password-based authentication system with RSA tokens. Elsa, your chief technology officer, denies your request, citing budgetary constraints. As a temporary solution, Elsa asks that you find ways to increase password security. Which of the following will accomplish this goal?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Disabling password-protected screensavers
- ❍ **B.** Enabling account lockout controls
- ❍ **C.** Enforcing a password policy that requires noncomplex passwords
- ❍ **D.** Enabling users to use the same password on more than one system

27. Which of the following is a major issue with signature-based IDSs?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Signature-based IDSs cannot detect zero-day attacks.
- ❍ **B.** Signature-based IDSs can detect only attacks in which activity deviates from normal behavior.
- ❍ **C.** Signature-based IDSs are available only as host-based systems.
- ❍ **D.** Signature-based IDSs are cost-prohibitive.

Quick Check

28. Administrative controls form an important part of security, and although most of us don't like paperwork, that is a large part of this security control. Which of the following is a high-level document that describes a management plan for how security should be practiced throughout the organization?

Quick Answer: **192**
Detailed Answer: **197**

- ❍ **A.** Guidelines
- ❍ **B.** Policies
- ❍ **C.** Procedures
- ❍ **D.** Standards

29. A hacker submits a malicious URL request for a help page from an unpatched Apache server that supports an Oracle9i Application Server. This causes a denial of service. Which of the following would have best protected the corporation from this attack?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** HIDS
- ❍ **B.** NIPS
- ❍ **C.** HIPS
- ❍ **D.** NIDS

30. One of your coworkers has joined a CISSP study group and is discussing today's list of topics. One of the topics is this: What is an example of a passive attack?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Dumpster diving
- ❍ **B.** Sniffing
- ❍ **C.** Installing SubSeven
- ❍ **D.** Social engineering

31. What is one of the major reasons why separation of duties should be practiced?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Reduced cross-training
- ❍ **B.** Legal
- ❍ **C.** Union policies and procedures
- ❍ **D.** To force collusion

32. There are two basic types of access control policies. Which of the following describes the best approach for a CISSP?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Begin with deny all.
- ❍ **B.** Allow some based on needs analysis.
- ❍ **C.** Begin with allow all.
- ❍ **D.** Deny some based on needs analysis.

Quick Check

33. Your manager asks you to set up a fake network to identify contractors who may be poking around the network without authorization. What is this type of system called?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Trap-and-trace
- ❍ **B.** Honeypot
- ❍ **C.** Snare
- ❍ **D.** Prison

34. Various operating systems such as Windows use what to control access rights and permissions to resources and objects?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** RBAC
- ❍ **B.** MITM
- ❍ **C.** ABS
- ❍ **D.** ACL

35. While hanging around the watercooler, you hear that your company, Big Tex Bank and Trust, is introducing a new policy. The company will require periodic job rotation and will force all employees to use their vacation time. From a security standpoint, why is this important?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Job rotation is important because it reduces employee burnout.
- ❍ **B.** Job rotation is important because employees need to be cross-trained in case of man-made or natural disasters.
- ❍ **C.** Job rotation ensures that no one can easily commit fraud or other types of deception without risking exposure.
- ❍ **D.** Forcing employees to use their vacation time ensures time away from work, which results in healthy, more productive employees.

36. Your manager persists in asking you to set up a fake network to identify contractors who may be poking around the network without authorization. What legal issue pertaining to these devices should you be most concerned with?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Enticement
- ❍ **B.** Federal Statute 1029
- ❍ **C.** Entrapment
- ❍ **D.** Liability

Quick Check

37. Your brother-in-law, Mario, is studying for the CISSP exam. He text-messages you with what he believes is an important question: What is a major disadvantage of access control lists? How do you answer him?

Quick Answer: **192**
Detailed Answer: **198**

- ❍ **A.** Overhead of the auditing function
- ❍ **B.** Burden of centralized control
- ❍ **C.** Independence from resource owners
- ❍ **D.** Lack of centralized control

38. Table 5.1 provides an example of some types and categories of access control. Which of the following is the best example of a technical deterrent?

Quick Answer: **192**
Detailed Answer: **199**

TABLE 5.1 Sample Access Types and Categories

Attribute	Deterrent	Preventive	Detective	Corrective	Recovery	Compensating
Administrative	–	–	Audit Policy	–	Incident Response Plan	–
Technical	–	ACLs	–	–	–	–
Physical	–	–	–	Fire Extinguisher	–	Defense in depth

- ❍ **A.** AUP
- ❍ **B.** Warning banner
- ❍ **C.** Anti-virus
- ❍ **D.** Hot site

39. What does TACACS+ use as its communication protocol?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** TCP
- ❍ **B.** UDP
- ❍ **C.** ICMP
- ❍ **D.** TCP and UDP

40. Which of the following attributes does not apply to MAC?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** Multilevel
- ❍ **B.** Label-based
- ❍ **C.** Universally applied
- ❍ **D.** Discretionary

Quick Check

41. Which of the following is not part of physical access control?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** CCTV
- ❍ **B.** Mantraps
- ❍ **C.** Data classification and labeling
- ❍ **D.** Biometrics

42. During a weekly staff meeting, your boss reveals that some employees have been allowing other employees to use their passwords. He is determined to put a stop to this and wants you to install biometric access control systems. He has asked about some basic attributes, such as type I errors, type II errors, and the CER, as shown in Figure 5.1. What's so important about the CER? How do you respond?

Quick Answer: **192**
Detailed Answer: **199**

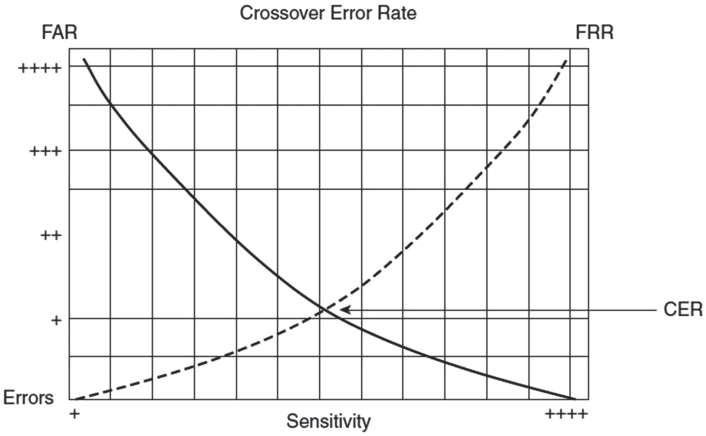

FIGURE 5.1 Crossover error rate.

- ❍ **A.** Speed typically is determined by calculating the CER.
- ❍ **B.** The CER has to do with the customer acceptance rate because some systems are more user-friendly than others.
- ❍ **C.** Accuracy typically is determined by calculating the CER.
- ❍ **D.** The CER has to do with the cost per employee because some biometric access control systems are very good, but also very expensive.

Quick Check

43. Kerberos has some features that make it a good choice for access control and authentication. One of these items is a ticket. What is a ticket used for?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** A ticket is a block of data that allows users to prove their identity to an authentication server.
- ❍ **B.** A ticket is a block of data that allows users to prove their identity to a service.
- ❍ **C.** A ticket is a block of data that allows users to prove their identity to a ticket-granting server.
- ❍ **D.** A ticket is a block of data that allows users to prove their identity to the Kerberos server.

44. What is the best definition of identification?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** The act of verifying your identity
- ❍ **B.** The act of claiming a specific identity
- ❍ **C.** The act of finding or testing the truth
- ❍ **D.** The act of inspecting or reviewing a user's actions

45. What term means that a user cannot deny a specific action because there is positive proof that he or she performed it?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** Accountability
- ❍ **B.** Auditing
- ❍ **C.** Nonrepudiation
- ❍ **D.** Validation

46. What type of cryptography does SESAME use to distribute keys?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** Public key
- ❍ **B.** Secret key
- ❍ **C.** SHA hashing algorithm
- ❍ **D.** None; it uses plaintext

47. Which of the following is a category of security controls that job rotation fits into?

Quick Answer: **192**
Detailed Answer: **199**

- ❍ **A.** Recovery
- ❍ **B.** Corrective
- ❍ **C.** Detective
- ❍ **D.** Compensation

Quick Check

48. What does RADIUS use for its transport protocol?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** UDP
- ❍ **B.** TCP
- ❍ **C.** TCP and UDP
- ❍ **D.** ICMP

49. Your chief information officer (CIO) needs your recommendation for a centralized access control system to maintain all the users and associated permissions. He also wants to be able to use this system for a wireless local area network (LAN). In addition to the wireless LAN requirement, the network administrator has stated that it is not important to the CIO to have a system that will split the authentication, authorization, and accounting processes up; however, having the option to use UDP, SCTP, or TCP is a must. The CIO also requires a SSO technology that can support non-repudiation and authenticity. The CIO has stated he is willing to purchase more than one system to meet the specified requirements. Which of the following is the best recommendation you would give?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** Purchase a Diameter for centralized access control and SESAME for SSO.
- ❍ **B.** Purchases a RADIUS for centralized access control and Kerberos because it is most commonly used and, most importantly, has been around a long time and many organizations trust it.
- ❍ **C.** Purchase a Diameter for centralized access control and Kerberos for SSO.
- ❍ **D.** Purchase Extended Terminal Access Controller System for centralized access control and use SESAME for SSO.

50. You have been promoted to security officer for a Fortune 500 company and are performing an audit of elevated privileges for the network. You observe that there are many members from the help desk that have privileges to various systems that they do not require to do their job on a daily basis. What best business practice does your company lack?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** Separation of duties
- ❍ **B.** Principle of least privilege
- ❍ **C.** Need to know
- ❍ **D.** Privilege creep

Quick Check

51. What does strong authentication require?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** Public/private keys
- ❍ **B.** Using two different methods of identification
- ❍ **C.** Using a method of identification from at least two of type I, II, or III
- ❍ **D.** Authenticating inside an encrypted tunnel

52. You have a homogeneous environment with multiple application servers. Your users are having difficulty remembering all their passwords as they complete their daily activities. What would be the best solution?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** Lower the passwords' complexity requirements
- ❍ **B.** Implement harsher penalties
- ❍ **C.** Add assisted user reset capabilities
- ❍ **D.** Use single sign-on

53. How do you lower type 1 errors on biometric devices?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** By increasing type 2 errors
- ❍ **B.** By decreasing type 2 errors
- ❍ **C.** By increasing precision
- ❍ **D.** By decreasing CER

54. When you log into your remote server from home, your server sends you a nonce that you enter into a token device that you were issued when you were hired. Your token device responds with a value you enter at the prompt. What have you entered?

Quick Answer: **192**
Detailed Answer: **200**

- ❍ **A.** A single sign-on using synchronous authentication
- ❍ **B.** A one-time password using synchronous authentication
- ❍ **C.** A single sign-on using asynchronous authentication
- ❍ **D.** A one-time password using asynchronous authentication

55. Which of the following describes a distinction between Kerberos and SESAME?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Kerberos supplies SSO; SESAME does not.
- ❍ **B.** Kerberos uses symmetric encryption; SESAME uses asymmetric encryption.
- ❍ **C.** Kerberos can be used for nonrepudiation; SESAME cannot.
- ❍ **D.** SESAME can be accessed using GSS-API; Kerberos cannot.

Quick Check

56. What type of physical control is a mantrap?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Deterrent
- ❍ **B.** Corrective
- ❍ **C.** Preventive
- ❍ **D.** Detective

57. What is the best way to store passwords?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** In a one-way encrypted file
- ❍ **B.** Using symmetric encryption
- ❍ **C.** Using asymmetric encryption
- ❍ **D.** By means of a digital signature

58. The act of professing to be a specific user is

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Validation
- ❍ **B.** Authorization
- ❍ **C.** Authentication
- ❍ **D.** Identification

59. Which of the following best describes a Zephyr chart?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** A means of establishing the accuracy of a biometric system
- ❍ **B.** A means of comparing different biometric systems
- ❍ **C.** A means of comparing type II and type III authentication systems
- ❍ **D.** A chart used to examine the accuracy of IDSs and IPSs

60. What is authentication?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Supplying a username
- ❍ **B.** Using criteria to determine what a user can do
- ❍ **C.** Verifying identification
- ❍ **D.** Reviewing audit logs

61. Being asked what your maiden name is, what city you were born in, and what your pet's name is an example of what?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Single sign-on (SSO)
- ❍ **B.** Self-service password reset
- ❍ **C.** Centralized authentication
- ❍ **D.** Assisted passwords

Quick Check

62. Which of the following best describes a federated identity?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Simply another term for SSO.
- ❍ **B.** It is restricted to use within a specific domain or area of the network.
- ❍ **C.** Type I authentication (something you know).
- ❍ **D.** It is portable and can be used across business boundaries.

63. Which of the following is the most accurate biometric system?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** A CER of 1
- ❍ **B.** A CER of 2
- ❍ **C.** A CER of 3
- ❍ **D.** None of the above because CER is not a numeric rating

64. Which type of control that includes fences, password protection, and CCTV is designed to stop an event from occurring?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Detective control
- ❍ **B.** Preventive control
- ❍ **C.** Corrective control
- ❍ **D.** Deterrent control

65. Nondiscretionary access control includes which of the following?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Role- and task-based
- ❍ **B.** Rule-based and mandatory
- ❍ **C.** Labeled and mandatory
- ❍ **D.** None of the above because there are no subcategories

66. What is a trust?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** A one-way-only bridge established between two domains
- ❍ **B.** A two-way-only bridge established between two domains
- ❍ **C.** A security bridge that is established after a valid authentication
- ❍ **D.** A security bridge that is established between two domains

Quick Check

67. What form of authorization is closely associated with labels?

Quick Answer: **192**
Detailed Answer: **201**

- ❍ **A.** Rule-based access control
- ❍ **B.** Discretionary access control
- ❍ **C.** Mandatory access control
- ❍ **D.** Role-based access control

68. How can a swipe card, smart card, or USB dongle be described?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** An active token
- ❍ **B.** A static token
- ❍ **C.** Type I authentication
- ❍ **D.** Type III authentication

69. The Equal Error Rate is equivalent to what?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** The point at which false acceptance and false rejection meet
- ❍ **B.** The crossover error rate minus 10 percent
- ❍ **C.** The point at which false acceptance is at its highest and false rejection is at its lowest
- ❍ **D.** The point at which false acceptance is at its lowest and false rejection is at its highest

70. Which of the following is the most expensive means of verifying a user's identity?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Single sign-on
- ❍ **B.** Tokens
- ❍ **C.** Biometrics
- ❍ **D.** Passwords

71. Which biometric system examines the colored portion of the eye that surrounds the pupil?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Iris
- ❍ **B.** Retina
- ❍ **C.** Fovea
- ❍ **D.** Optic disc

72. Which of the following best describes a rainbow table?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** An attack against a biometric system
- ❍ **B.** An attack against a fingerprint scanner
- ❍ **C.** A table used for digital signatures
- ❍ **D.** A table of precomputed password hashes

Quick Check

73. The ticket-granting service is a component of what?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** TACACS
- ❍ **B.** Kerberos
- ❍ **C.** RADIUS
- ❍ **D.** SESAME

74. The Privilege Attribute Certificate (PAC) is a component of what?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** TACACS
- ❍ **B.** Kerberos
- ❍ **C.** RADIUS
- ❍ **D.** SESAME

75. What nontechnical attack attempts to lure the victim into giving up financial data, credit card numbers, or other types of account information?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Pretexting
- ❍ **B.** Social engineering
- ❍ **C.** Dumpster diving
- ❍ **D.** Phishing

76. You are asked to work on a project where users need to share credentials across multiple domains without forcing them to log in more than once. What technologies might meet this business need?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Cookies
- ❍ **B.** Unique X.509 certificates
- ❍ **C.** Web access management
- ❍ **D.** Separate usernames and passwords

77. Your company was initially considering three security models to use to design access rights and controls in its new operating system (OS). These models included Biba, Bell-LaPadula, and Clark Wilson. If the company decided to base its OS on the Biba model, which of the following properties is correct?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** A user cannot write down to a lower level.
- ❍ **B.** The model makes use of transformational procedures and constrained data items.
- ❍ **C.** The user cannot write up to a higher level.
- ❍ **D.** If a user has access to one side of the wall, he does not have access to data on the other side of the wall.

Quick Check

78. Which of the following refers to the process of creation, maintenance, and deletion of user objects?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Identification
- ❍ **B.** Verification
- ❍ **C.** Authentication
- ❍ **D.** Provisioning

79. Object reuse can be an important issue when considering which of the following?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** RAM scraping attacks
- ❍ **B.** Authentication method
- ❍ **C.** Type of biometric system used
- ❍ **D.** Strength of a password

80. Which form of access control has a many-to-many relationship and makes use of mapping between a user and a subset of goals?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** MAC
- ❍ **B.** DAC
- ❍ **C.** Rule-based access control
- ❍ **D.** Core RBAC

81. Which of the following is the best example of capabilities tables?

Quick Answer: **192**
Detailed Answer: **202**

- ❍ **A.** Memory cards
- ❍ **B.** Kerberos
- ❍ **C.** Constrained user interface
- ❍ **D.** Router ACL

82. Which of the following provides an upgrade path from RADIUS?

Quick Answer: **192**
Detailed Answer: **203**

- ❍ **A.** Diameter
- ❍ **B.** TACACS
- ❍ **C.** Kerberos
- ❍ **D.** NetSP

83. Investigations are a good example of which of the following?

Quick Answer: **192**
Detailed Answer: **203**

- ❍ **A.** Detective control
- ❍ **B.** Preventive control
- ❍ **C.** Deterrent control
- ❍ **D.** Proactive control

Quick Check

84. Although an authorized sniffer has been connected to a network switch, the user can only see traffic directed to the device and some broadcast traffic. What might be the problem?

Quick Answer: **192**
Detailed Answer: **203**

- ❍ **A.** An IDS is blocking the traffic.
- ❍ **B.** The switch port must be spanned.
- ❍ **C.** The switch detected the sniffer.
- ❍ **D.** The sniffer is misconfigured.

85. Which type of attack makes use of a time-memory tradeoff?

Quick Answer: **192**
Detailed Answer: **203**

- ❍ **A.** Rule-based
- ❍ **B.** Dictionary
- ❍ **C.** Rainbow table
- ❍ **D.** Brute-force

Practice Questions (True or False)

86. War dialing is an attack that targets a wireless network.

Quick Answer: **192**
Detailed Answer: **203**

- ❍ True
- ❍ False

87. Encryption is an example of a technical control.

Quick Answer: **192**
Detailed Answer: **203**

- ❍ True
- ❍ False

88. Access controls should default to full access.

Quick Answer: **193**
Detailed Answer: **203**

- ❍ True
- ❍ False

89. TACACS is an example of centralized access technology.

Quick Answer: **193**
Detailed Answer: **203**

- ❍ True
- ❍ False

90. Kerberos addresses availability.

Quick Answer: **193**
Detailed Answer: **203**

- ❍ True
- ❍ False

Quick Check

91. An example of an IDS engine is signature-based.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **203**

92. Stateful matching is a type of signature-based IDS.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **203**

93. SATAN is an example of a vulnerability scanner.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **203**

94. Software faults can be uncovered with watchdog timers.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **203**

95. PAP is considered a secure protocol.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **203**

96. Diameter is not an AAA protocol.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

97. Attribute value pairs are used with SESAME.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

98. A token, ticket, or key can be a capability.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

99. MAC allows the owner to determine who has access.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

100. Static separation of duties is one way to restrict the combination of duties.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

Quick Check

101. IDaaS solutions provide a range of identity and access management services such as single sign-on (SSO) functionality through the cloud.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

102. Retina scanning matches the person's blood vessels on the back of the eye and is very accurate.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

103. TACACS+ supports two-factor authentication.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

104. Centralized authentication allows a subject to be authenticated by a system only once and then access resource after resource repeatedly.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

105. Tokens are an example of type II authentication.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

106. Keyboard dynamics is an example of type III authentication.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

107. Scrubbing is the act of clearing a hard drive for destruction or resale.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **204**

108. Keystroke monitoring is a form of biometrics.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **205**

Quick Check

109. A federated identity is an identity management system (IdM) that is considered portable.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **205**

110. Type I authentication systems typically have a clipping level set to 3.

- ❍ True
- ❍ False

Quick Answer: **193**
Detailed Answer: **205**

Practice Questions (Mix and Match)

111. Match each attack with its definition.

Quick Answer: **193**
Detailed Answer: **205**

A. Smurf: _____
B. LAND: _____
C. TRINOO: _____
D. SYN Attack: _____
E. Chargen: _____
F. Ping of death: _____

1. Uses two systems to bounce a continuous stream of traffic between ports 7 and 19.
2. A SYN packet that is to and from the same address and port.
3. A series of SYN packets are sent that fill the receiving buffer.
4. Uses a ping packet to broadcast addresses spoofed from the victim.
5. An early type of DDoS attack.
6. Sends ICMP packets that are at or exceed maximum size.

112. Match each access control type with its definition.

Quick Answer: **193**
Detailed Answer: **205**

A. Discretionary access control: _____
B. Mandatory access control: _____
C. Role-based access control: _____
D. Rule-based access control: _____
E. Constrained user interfaces: _____

Quick Check

1. Assigns access to groups, not users.
2. Used with firewalls and routers.
3. Uses sensitivity labels.
4. Classification labeling of objects by owner.
5. Works by restricting users to specific functions based on their role in the system.

113. Match each item with the correct authentication type.

Quick Answer: **193**
Detailed Answer: **205**

A. CER: _____
B. Weakest form of encryption: _____
C. Common access card: _____
D. Type II error: _____
E. Memory card: _____
F. Pronounceable passwords: _____

1. Something you know.
2. Something you are.
3. Something you have.

114. Match each authentication type with its definition.

Quick Answer: **193**
Detailed Answer: **206**

A. Centralized authentication and no backwards compatibility: _____
B. Uses ticket-granting service: _____
C. Allows secure web domains to exchange user authentication data: _____
D. Uses a single authentication server: _____
E. Uses port 389: _____
F. Introduced by Cisco: _____

1. Kerberos
2. LDAP
3. XTACACS
4. SAML

Quick-Check Answer Key

1. B
2. B
3. C
4. A
5. A
6. A
7. D
8. A
9. D
10. B
11. C
12. D
13. C
14. C
15. B
16. C
17. A
18. A
19. D
20. A
21. C
22. B
23. C
24. A
25. B
26. B
27. A
28. B
29. B
30. B
31. D
32. A
33. B
34. D
35. C
36. C
37. D
38. B
39. A
40. D
41. C
42. C
43. B
44. B
45. C
46. A
47. C
48. A
49. A
50. B
51. C
52. D
53. A
54. D
55. B
56. C
57. A
58. D
59. B
60. C
61. B
62. D
63. A
64. B
65. A
66. D
67. C
68. B
69. A
70. C
71. A
72. D
73. B
74. D
75. D
76. C
77. C
78. D
79. A
80. D
81. B
82. A
83. A
84. B
85. C
86. False
87. True

88. False

89. True

90. False

91. True

92. True

93. True

94. True

95. False

96. False

97. False

98. True

99. False

100. True

101. True

102. True

103. True

104. False

105. True

106. True

107. False

108. False

109. True

110. True

111.

- **A.** 4
- **B.** 2
- **C.** 5
- **D.** 3
- **E.** 1
- **F.** 6

112.

- **A.** 4
- **B.** 3
- **C.** 1
- **D.** 2
- **E.** 5

113.

- **A.** 2
- **B.** 1
- **C.** 3
- **D.** 2
- **E.** 3
- **F.** 1

114.

- **A.** 3
- **B.** 1
- **C.** 2
- **D.** 1
- **E.** 2
- **F.** 3

Answers and Explanations

1. **Answer: B.** The three types of controls are as follows:
   - **Administrative:** These controls are composed of the policies and procedures the organization has put in place to prevent problems and to ensure that the technical and physical controls are known, understood, and implemented.
   - **Technical:** These controls are used to control access and monitor potential violations. They may be either hardware- or software-based.
   - **Physical:** These control systems are used to protect the welfare and safety of the employees and the organization. Physical controls include such items as smoke alarms, security guards, cameras, and mantraps.
2. **Answer: B.** Authentication can take one of three forms: something you know, something you have, or something you are. Something you are, such as biometrics, is by far the strongest form of authentication. Systems such as retina and iris scans have high levels of accuracy. The accuracy of a biometric device can be assessed by means of the crossover error rate. Remember: On the exam, questions are sometimes vague, and you will be asked to pick the best available answer.
3. **Answer: C.** The question states that a password and PIN are required. Both passwords and PINs are examples of something you know. Authentication is something you know, something you have, or something you are. Therefore, passwords and PINs are examples of authentication. Answer B is incorrect because two-factor authentication requires two of the three primary categories of authentication to be used. Two-factor authentication is considered more secure than single-factor authentication. Three-factor authentication requires all three categories. Authorization is what you allow the user to do or accomplish.
4. **Answer: A.** Authentication can be based on one or more of the following three factors:
   - Something you know: This could be a password, passphrase, or secret number.
   - Something you have: This could be a token, bank debit card, or smart card.
   - Something you are: This could be a retina scan, fingerprint, DNA sample, or facial recognition.
5. **Answer: A.** Passwords, which belong to the "something you know" category, are the weakest form of authentication. Although there are many more stringent forms of authentication, passwords remain the most widely used. Passwords are insecure because people choose weak ones, don't change them, and have a tendency to write them down or allow others to gain knowledge of them. If more than one person is using the same password, there is no way to properly execute the audit function, and at this point, loss of security occurs. Passwords are also susceptible to cracking and brute-force attacks.
6. **Answer: A.** The general order of accuracy of biometric systems is fingerprint, palm scan, hand geometry, retina scan, and iris scan. However, the accuracy of an individual system is not the only item a security professional needs to consider before implementing a biometric system. Security professionals must examine usability, employee acceptance, and the crossover error rate of the proposed system.

The employee acceptance rate examines the employees' willingness to use the system. For example, technology innovations with Radio Frequency Identifier (RFID) tags have made it possible to inject an extremely small tag into an employee's arm. This RFID tag could be used for identification, for authorization, and to monitor employee movement throughout the organization's facility. However, most employees would be hesitant to allow their employer to embed such a device in their arm. Currently issued passports have RFID tags, which has created an issue with identity theft (RFID sniffers).

The crossover error rate examines the capability of the proposed systems to accurately identify the individual. If the system has a high false reject rate, employees will soon grow weary of the system and look for ways to bypass it. Therefore, each of these items is important to consider.

7. **Answer: D.** Before implementing any type of access control system, the security professional needs to consider potential vulnerabilities because these give rise to threats. Threats must also be considered because they lead to risks. Risk is the potential that the vulnerability may be exploited. Answer D is incorrect because it relates to the formula used for risk analysis.

8. **Answer: A.** Kerberos is a single sign-on system for distributed systems. It is unlike authentication systems such as NT LAN MAN (NTLM) that perform only one-way authentication. It provides mutual authentication for both parties involved in the communication process. Kerberos operates under the assumption that there is no trusted party; therefore, both client and server must be authenticated. After mutual authentication occurs, Kerberos makes use of a ticket stored on the client machine to access network resources. Answers B and C are incorrect because they describe access control models. Answer D describes centralized authentication.

9. **Answer: D.** Only Password Authentication protocol (PAP) is not susceptible to a dictionary attack; no attack is needed because the password is transmitted in plaintext. Challenge Handshake Authentication Protocol (CHAP), Lightweight Extensible Authentication Protocol (LEAP), and WiFi Protected Access Pre-shared Key (WPA-PSK) are all susceptible to dictionary attacks. When you are forced to use one of these mechanisms, the only security precaution you can take is to choose passwords that will not be in any contrived dictionary—although precomputed hashes are now being used for that purpose.

10. **Answer: B.** FAR (False Acceptance Rate) is the percentage of illegitimate users who are granted access to the organization's resources. Keeping this number low is important to keeping unauthorized individuals out of the company's resources.

11. **Answer: C.** The only choice for copper cabling would be Category 6. Single-mode and multimode fiber are not examples of copper cabling. However, fiber is considered a more secure transmission medium than copper cabling because it does not emit any Electromagnetic Interference (EMI). All types of copper cabling emit a certain amount of EMI. Unauthorized personnel can clamp probes to these cables and decode the transmitted messages. Wireless is not an example of copper cabling.

12. **Answer: D.** There are four types of access control models. Discretionary access control places the data owners in charge of access control. Mandatory access control uses labels to determine who has access to data. Role-based access control is based on the user's role in the organization. Answer D is incorrect because there is no category called delegated access control. A valid answer would have been rule-based access control.

13. **Answer: C.** Auditing is considered an administrative control. The three types of controls are discussed in answer 1.

14. **Answer: C.** Bank tellers would most likely fall under a role-based access control system. These systems work well for organizations in which employee roles are identical.

15. **Answer: B.** Dictionary attacks are an easy way to pick off insecure passwords. Passwords based on dictionary words allow attackers to simply perform password guessing or to use more advanced automated methods employing software programs. LCP, Cain and Able, and John the Ripper are commonly used password-cracking programs that can launch dictionary attacks. A hybrid attack must try a combination of words and special characters. A brute-force attack must try all combinations of characters, numbers, and special characters. A man-in-the-middle attack is one in which the attacker stands between the victim and the service and attempts to steal or sniff passwords or information.

16. **Answer: C.** Tempest is the standard for electromagnetic shielding of computer equipment. Answer B is a distracter, answer A is the name of a radioactive gas, and answer D is the name of the individual who discovered the radiation belts that surround the Earth.

17. **Answer: A.** Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between between an identity provider and a service provider. Lightweight Directory Access Protocol (LDAP) is a protocol designed to allow individuals to locate organizations, individuals, and other resources such as files and devices in a network. Open Authentication (OAUTH) is an authentication protocol that allows users to approve applications to act on their behalf without sharing their password. Single sign-on is implemented by using ticket-based systems such as KryptoKnight.

18. **Answer: A.** A discretionary access system places the data owners in charge of access control. Mandatory access control uses labels to determine who has access to data, and role-based access control is based on organizational roles. This is also known as "nondiscretionary" and is based on the user's role in the organization.

19. **Answer: D.** Challenge/response authentication is a secure authentication scheme that works in the following way: First, a randomly generated string of values is presented to the user, who then returns a calculated number based on those random values. Second, the server performs the same process locally and compares the result to the saved value. Finally, if these values match, the user is granted access; otherwise, access is denied. Answer A is a distracter. Answer B is an example of Kerberos. Answer C is an example of Challenge Handshake Authentication Protocol (CHAP).

20. **Answer: A.** FRR (False Rejection Rate) measures the number of authorized users who were incorrectly denied access. If a system has a high FRR, many valid users will be denied access. Valid users who are denied access may attempt to bypass or subvert the authentication system because they believe it does not work correctly. The FRR is separate from the False Acceptance Rate (FAR). The FAR is used to measure statistics of unauthorized users. Answer D is incorrect because FRR has nothing to do with the rate of return.

21. **Answer: C.** Password attacks are the easiest way to attempt to bypass access control systems. Password attacks can range from simple password guessing to

more advanced automated methods in which software programs are used. Dictionary attacks may be the fastest, but brute-force attacks are considered the most time-intensive. If the user has chosen a complex password, however, this may be the attacker's only choice. Brute-force uses a combination of all numbers and letters, making substitutions as it progresses. It continues until all possible combinations have been attempted. If the password is very long or complex, this may take a considerable amount of time. A plaintext password would require no cracking at all.

22. **Answer: B.** CVE stands for Common Vulnerabilities and Exposures. CVE is a database developed to standardize the naming system of security vulnerabilities. It also serves as a centralized depository of information on vendor software and discovered vulnerabilities. You can find more information about the CVE database at http://cve.mitre.org.

23. **Answer: C.** Telnet transmits username and password information in clear text and thus can be used by attackers to gain unauthorized access. Secure Shell (SSH) and HTTP Secure (HTTPS) are secure protocols. Although some versions of SSH are more secure than others, it is always better to go with some form of encryption. Even though Trivial FTP (TFTP) transmits in plaintext, no username and password information is exchanged because TFTP does not require authentication.

24. **Answer: A.** Fingerprints are most closely associated with law enforcement. Close behind this is facial recognition. Facial recognition technology has made great strides since the terrorist attacks of September 11. Common methods include the Markov model, eigenface, and fisherface. Iris and retina recognition are not typically associated with law enforcement.

25. **Answer: B.** Under the mandatory access control model, the system administrator establishes file, folder, and account rights. It is a very restrictive model in which users cannot share resources dynamically.

26. **Answer: B.** Password-based authentication systems can be made more secure if complex passwords are used, account lockouts are put in place, and tools such as Passprop are implemented. Passprop places remote lockout restrictions on the administrator account. Passprop is Microsoft-specific, and the test will not quiz you on that level of detail. Just understand that tools are available on both Windows and OS X platforms to accomplish this task. Many routers, switches, and network gear also support varying degrees of lockout (usually tied to RADIUS). Disabling password-protected screensavers would decrease security, as would allowing users to reuse passwords.

27. **Answer: A.** Signature-based Intrusion Detection System (IDSs) can detect only attack signatures that have been previously stored in their databases. These systems rely on the vendor for updates. Until then they are vulnerable to new zero-day or polymorphic attacks. Answer B is incorrect because it describes a statistical-based IDS. Answer C is incorrect because signature-based IDSs are available as both host and network configurations. Answer D is incorrect because the costs of signature-based IDS and statistical anomaly-based IDS are comparable.

28. **Answer: B.** Policies provide a high-level overview of how security should be practiced throughout the organization. Answers A, C, and D all describe the details of how these policies are to be implemented. What is most important about these particular concepts is that security policy must flow from the top of the organization.

29. **Answer: B.** A Network Intrusion Prevention System (NIPS) provides protective/reactive responses to a network. This malicious attack was submitted via port 80 HTTP service and is identified by network monitoring. A Host Intrusion Detection System (HIDS) focuses on services that cannot be seen from the network. A Host Intrusion Prevention System (HIPS) is focused on the system but can respond. A Network Intrusion Detection System (NIDS) identifies suspicious activity in a log file, but cannot take action.

30. **Answer: B.** Sniffing is an example of a passive attack. Attackers performing the sniff simply wait and capture data when they find the information they are looking for. This might be usernames, passwords, credit card numbers, or proprietary information. All other answers are incorrect because installing programs, dumpster diving, and social engineering (which uses the art of deception) are all active attacks.

31. **Answer: D.** Forcing collusion is one of the primary reasons why separation of duties should be practiced. Simply stated, collusion requires two or more employees to work together to bypass security. This means that one person working alone cannot pull off an attack. The practice of separation of duties vastly reduces this risk.

32. **Answer: A.** The best access control policy is "deny all." This strategy starts by denying all access and privileges to all employees. Then, access and privilege are granted only as required by job needs. Some organizations start with "allow all." This presents a huge security risk.

33. **Answer: B.** Honeypots, which also have been expanded into honeynets, are network decoys or entire networks that are closely monitored systems. These devices allow security personnel to monitor when the systems are being attacked or probed. They can also provide advance warning of a pending attack and act as a jail until you have decided how to respond to the intruder.

34. **Answer: D.** Access Control List (ACLs), as seen in the context of the CISSP exam, are used to set discretionary access controls. The three basic types are read, write, and execute. RBAC refers to role-based access controls, MITM is an acronym for man-in-the-middle, and ABS is simply a distracter.

35. **Answer: C.** Although job rotation does provide backup for key personnel and may help in all the other ways listed, its primary purpose is to prevent fraud or financial deception.

36. **Answer: C.** The primary legal issues surrounding honeypots includes entrapment. Entrapment is illegal as it might encourage a person to commit a crime that was not intended. Enticement is legal and is used to lure someone into leaving evidence after committing a crime. Although liability could be an issue if the honeypot is compromised and then used to attack an outside organization, entrapment is illegal and unethical, and ISC^2-certified professionals are bound by a code of ethics. Statute 1029 is related to hacking and is not the primary concern of honeypots. Although liability is an issue, it is not the primary concern in the context of this question.

37. **Answer: D.** The major disadvantages of ACLs are the lack of centralized control and the fact that many operating systems default to full access. This method of access control is burdened by the difficulty of implementing a robust audit function. Therefore, answers A, B, and C are incorrect.

38. **Answer: B.** A warning banner is an example of a technical deterrent. Answer A, an acceptable use policy (AUP) is an example of an administrative deterrent. Answer C is a technical detective control. Answer D is a technical recovery control.

39. **Answer: A.** Terminal Access Controller Access-Control System+ (TACACS+) uses TCP port 49 for communication. The strength of TACACS+ is that it supports authentication, authorization, and accounting. Each is implemented as a separate function, which allows the organization to determine which services it wants to deploy. This makes it possible to use TACACS+ for authorization and accounting, while choosing a technology such as RADIUS for authentication.

40. **Answer: D.** Mandatory Access Control (MAC) is typically built in and is a component of most operating systems. MAC's attributes include the following: It's nondiscretionary because it is hard-coded and cannot easily be modified, it's capable of multilevel control, it's label-based because it can be used to control access to objects in a database, and it's universally applied because changes affect all objects.

41. **Answer: C.** CCTV, mantraps, biometrics, and badges are just some of the items that are part of physical access control. Data classification and labeling are preventive access control mechanisms.

42. **Answer: C.** The CER (Crossover Error Rate) is used to determine the device's accuracy. A lower CER means that the device is more accurate. The CER is determined by mapping the point at which the FAR (False Acceptance Rate) and the FRR (False Rejection Rate) meet. The CER does not determine speed, customer acceptance, or cost per employee.

43. **Answer: B.** Kerberos is a network authentication protocol that provides single sign-on service for client/server networks. A ticket is a block of data that allows users to prove their identity to a service. The ticket is valid only for a limited amount of time. Allowing tickets to expire helps raise the barrier for possible attackers because the ticket becomes invalid after a fixed period. An authentication server provides each client with a ticket-granting ticket. Clients use a ticket-granting server to grant session tickets and reduce the workload of the authentication server. The ticket is not used to prove identity to Kerberos server it is used to prove identity to service or principal.

44. **Answer: B.** Identification is defined as the act of claiming a specific identity. Authentication is the act of verifying your identity, validation is the act of finding or testing the truth, and auditing is the act of inspecting or reviewing a user's actions.

45. **Answer: C.** Nonrepudiation is closely tied to accountability. It is defined as a means to ensure that users cannot deny their actions. Therefore, nonrepudiation is what makes users accountable. Digital signatures and timestamps are two popular methods used to prove nonrepudiation. Accountability is more closely related to activities, intrusions, events, and system conditions. Auditing is the act of review. Validation is more closely associated with certification and accreditation.

46. **Answer: A.** SESAME uses public key cryptography to distribute secret keys. It also uses the MD5 algorithm to provide a one-way hashing function. It does not distribute keys in plaintext, use SHA, or use secret key encryption.

47. **Answer: C.** There are six categories of security controls: preventive, detective, corrective, deterrent, recovery, and compensation. Job rotation would help in the

detective category because it could be used to uncover violations. It would not help in recovery, corrective, or compensation.

48. **Answer: A.** RADIUS (Remote Authentication Dial-in User Service) uses UDP ports 1812 and 1813. RADIUS performs authentication, authorization, and accounting for remote users. RADIUS can also use UDP 1645 for authentication and UDP 1646 for accounting. Answers B, C, and D are wrong because RADIUS does not use TCP or ICMP as a transport protocol.

49. **Answer: A.** Diameter is a centralized access control system that supports UDP, SCTP, and TCP. SESAME is a single sign-on (SSO) technology that uses both symmetric and asymmetric cryptograph, thereby allowing for the use of non-repudiation and authentication within the principles. RADIUS only supports UDP, **not** TCP or SCTP. Kerberos does not support asymmetric cryptography. The CIO requires non-repudiation and authentication, a service that symmetric cryptography does not support. Kerberos does not support asymmetric cryptography. Answer D is not the best answer as the CIO said the he does not require split AAA services. It is important that test takers are very familiar with the advantages and disadvantages of the SSO and centralized access control technologies that are referenced in the Common body of knowledge (CBK). Each alternative are potential solutions based in the different environments of the customer.

50. **Answer: B.** The principle of least privilege refers to a user having the minimum access control to information systems to do their job. Separation of duties states that critical functions should be divided up among employees. Need-to-know states that users should only have access to information needed to do their job, and answer D is incorrect because privilege creep refers to a user's obtaining privileges over time as they rotate jobs within a company.

51. **Answer: C.** Each answer is a good authentication method, but C is the best description of two-factor authentication. Answer A describes asymmetric encryption. Answer B does not specify what types or categories are being used. Answer D could be the description of IPsec or another tunneling protocol.

52. **Answer: D.** Single sign-on (SSO) can be difficult in a heterogeneous environment, where not all manufacturers may support the same authentication method. But it is a great solution in a homogeneous environment, where all vendors support the same mechanism. But the password must be complex, or you've given a malicious hacker a single point where he can breach your network.

53. **Answer: A.** Type 1 errors result from rejection of authenticated persons. You lower this count by relaxing the precision of the equipment (decreasing precision), which increases type 2 errors (accepting unauthenticated persons). You stop your tuning when type 1 errors equal type 2 errors (the crossover error rate [CER]). Under no circumstances do you want to let in more unauthenticated persons because then you risk rejecting authorized persons.

54. **Answer: D.** Your token uses the nonce to create a one-time password. This is called asynchronous authentication. Answers A, B, and C are incorrect because synchronous token authentication takes place when the token has a timing device that is in sync with a timing mechanism on the server.

55. **Answer: B.** Because SESAME uses asymmetric authentication, it can be used for nonrepudiation, whereas Kerberos cannot. Both Kerberos and SESAME support single sign-on (SSO), and both can be accessed by applications that use GSS-API function calls.

56. **Answer: C.** A mantrap is a preventive control because it prevents the entry of unauthorized individuals. Deterrent controls slow down unauthorized behavior, corrective controls remove inappropriate actions, and detective controls discover that unauthorized behavior occurred. The CISSP exam expects you to understand the difference between various types of controls.

57. **Answer: A.** A salted, one-way encrypted file is the best way to store passwords. Cryptographic solutions to accomplish this include MD5, SHA, and HAVAL. Symmetric, asymmetric, and digital signatures are not the preferred way of storing passwords.

58. **Answer: D.** The act of professing to be a specific user is identification. It is not validation, authorization, or authentication.

59. **Answer: B.** A Zephyr chart can be used to compare and measure different types of biometric systems. For example, consider a situation in which you are asked to compare a fingerprint scanner to a palm scanner. Answer A is incorrect because the Crossover Error Rate (CER) is better suited for that task. Answer C also refers to the CER. A Zephyr chart is not used for intrusion detection.

60. **Answer: C.** Authentication can best be described as the act of verifying identity.

61. **Answer: B.** The best answer is a self-service password reset. Many websites allow users to reset their passwords by supplying some basic information. This is not an example of single sign-on, centralized authentication, or assisted passwords.

62. **Answer: D.** A federated identity is portable and can be used across business boundaries. Federated identity is not SSO or one that is restricted for use within a single domain. Federated identity also is not restricted to type I authentication.

63. **Answer: A.** The lower the crossover error rate (CER), the more accurate the biometric system. Therefore, a system with a CER of 1 would be the most accurate.

64. **Answer: B.** Preventive systems are designed to stop an unwanted event from occurring. Detective controls are designed to discover an event. Corrective controls are designed to provide a countermeasure to the unwanted event, and deterrent controls are used for discouragement.

65. **Answer: A.** Nondiscretionary access control includes role- and task-based mechanisms. Mandatory access controls are an example of label-based security and are not considered nondiscretionary. Rule-based access control is most commonly seen in ACLs and is used with routers.

66. **Answer: D.** A trust can be defined as a security bridge that is established between two domains. The trust can be one-way, two-way, or transitive and is not restricted to any mode.

67. **Answer: C.** Labels are associated with Mandatory Access Control (MAC). MAC is not permissive; it is considered prohibitive. MAC is more secure and less flexible than DAC; if access is not specifically granted, it is forbidden. Answers A, B, and D are not associated with labels.

68. **Answer: B.** A static token can be a swipe card, smart card, or USB token. These tokens are not active and are not considered type I (something you know) or type III (something you are) authentication.

69. **Answer: A.** The Equal Error Rate (EER) is simply another name for the Crossover Error Rate (CER). It is not the CER minus 10 percent, or where the FAR is lowest or highest.

70. **Answer: C.** Biometric systems are the most expensive means of performing authentication. They cost more than tokens, single sign-on, or passwords.

71. **Answer: A.** The optic disk and the fovea are parts of the eye, but an iris scan looks at the colored portion of the eye. A retina scan looks at the blood vessels at the back of the eye.

72. **Answer: D.** A rainbow table is a type of precomputed hash. It utilizes the time memory trade-off principle. It is not an attack against a biometric or fingerprint system and has nothing to do with digital certificates.

73. **Answer: B.** The ticket-granting service is a component of Kerberos.

74. **Answer: D.** SESAME uses a PAC in much the same way that Kerberos uses a key distribution center. RADIUS and TACACS do not use PACs.

75. **Answer: D.** Phishing is a nontechnical attack that attempts to trick the victim into giving up account or password information. Pretexting is the act of using established personal information to gain access to accounts, cell phone records, or other information. Social engineering is a more general term used to describe this entire category of attacks. Dumpster diving is accomplished by digging through the trash.

76. **Answer: C.** Web-access management allows web users to share user credentials across multiple domains without having to log into each site. Cookies will not work because they are domain-specific, and a unique certificate for each domain would not address the problems.

77. **Answer: C.** Under the Biba model, users cannot write up. Answer A describes the Bell-LaPadula model. Answer B describes the Clark Wilson Model. Answer D described the Brewer Nash model.

78. **Answer: D.** Provisioning is the management of user access. Answers A. B, and C are incorrect because they do not define the term.

79. **Answer: A.** Object reuse refers to the allocation or reallocation of system resources (storage objects) to a subject. RAM-scraping attacks, such as the cold boot attack, demonstrates that object reuse can be a real problem. The authentication method, biometric system, or strength of the password do not apply.

80. **Answer: D.** Core RBAC makes use of a many-to-many relationship and is useful in organizations that have well-defined roles. Answer A describes MAC, which makes use of labels. Answer B describes DAC, which is a nondiscretionary model. Answer C describes rule-based access control, which makes use of ACLs.

81. **Answer: B.** A good example of a capability table is Kerberos. When a ticket is issued, it is bound to the user and specifies what resources a user can access. Answers A, C, and D do not meet that specification.

82. **Answer: A.** Diameter is the only option that provides an upgrade path from RADIUS.

83. **Answer: A.** Investigations are a good example of a detective control.

84. **Answer: B.** Switched networks are segmented, and as such require a port to be spanned. An IDS does not block traffic. An IPS would, but that type of control is not discussed in this question. MAC filtering would have most likely disabled the port. No traffic would have been captured.

85. **Answer: C.** A rainbow table uses a table of precomputed hashes. Answers A, B, and D are incorrect.

86. **Answer: False.** War dialing is the act of using a phone dialer program to dial a series of numbers in search of an open modem. Some people now use VoIP for war dialing, such as the I-War tool, WarVOX and IAX protocol (Asterisk).

87. **Answer: True.** Encryption is an example of a technical control. Policies are an example of an administrative control, whereas a fence is a physical control.

88. **Answer: False.** Access control should default to no access. You should also restrict the user to allow access to only what is needed and nothing more. As a default, no access should be provided unless a business justification can be shown as to why access should be provided.

89. **Answer: True.** TACACS, RADIUS, and Diameter are all examples of centralized access controls. For example, RADIUS is widely used by ISPs to authenticate dialup users. This central point of authentication provides an easy mechanism if users do not pay their monthly fees.

90. **Answer: False.** Although Kerberos provides single sign-on capability, it does not provide availability. Kerberos is a network authentication protocol created at the Massachusetts Institute of Technology that uses secret-key cryptography. Kerberos has three parts: a client, a server, and a trusted third party (KDC) to mediate between them. Clients obtain tickets from the Kerberos Key Distribution Center (KDC) and present these tickets to servers when connections are established.

91. **Answer: True.** IDS engines typically include signature and anomaly. Valid types of IDSs include host and network. Knowing the difference in these terms is an important distinction for the exam.

92. **Answer: True.** Signature-based IDSs can be pattern-matching or stateful. Pattern matching looks to map the results to a known signature. Stateful compares patterns to the user's activities.

93. **Answer: True.** SATAN was actually the first vulnerability assessment tool ever created. The cocreator was fired for releasing the program. The creator released a second tool named repent to rename the program SANTA. Although the CISSP exam is not platform-specific, you may be asked about well-known tools and open-source technologies, such as SATAN or Tripwire.

94. **Answer: True.** Watchdog timers can prevent timing problems, infinite loops, deadlocks, and other software issues.

95. **Answer: False.** Password Authentication Protocol (PAP) is not a secure protocol because passwords are passed in plaintext.

96. **Answer: False.** Diameter got its name as a takeoff on RADIUS. Diameter is considered a centralized AAA protocol. Diameter was designed for all forms of remote connectivity, not just dialup.

97. **Answer: False.** Attribute pairs are used with RADIUS. RADIUS is a UDP-based client/server protocol defined in RFCs 2058 and 2059. RADIUS provides three services: authentication, authorization, and accounting. RADIUS facilitates centralized user administration and keeps all user profiles in one location that all remote services share. SESAME is a single sign-on mechanism created in Europe.

98. **Answer: True.** A capability can be a token, ticket, or key. Capabilities define specific use. For example, a movie ticket lets the holder watch the show. As another example, before access is granted to read a file, the capability is verified.

99. **Answer: False.** MAC is mandatory access control and, as such, the user has little freedom. Therefore, in a MAC-based system, access is determined by the system rather than the user. The MAC model typically is used by organizations that handle highly sensitive data, such as the DoD, NSA, CIA, and FBI.

100. **Answer: True.** Static separation of duties is one way to restrict the combination of duties. This means of control is commonly found in RBAC environments. For example, the individual who initiates the payment cannot also authorize the payment.

101. **Answer: False.** ID as a Service (IDaaS) solutions provide a range of identity and access management services such as single sign on functionality through the cloud and federated identity management.

102. **Answer: True.** Retina scanning matches blood vessels on the back of the eye and is very accurate. Iris scanning looks at the colored portion of the eye.

103. **Answer: True.** Terminal Access Controller Access Control System (TACACS) is available in three variations: TACACS, XTACACS (Extended TACACS), and TACACS+, which features two-factor authentication. TACACS also allows the division of the authentication, authorization, and accounting function, which gives the administrator more control over its deployment.

104. **Answer: False.** This is actually a description of single sign-on (SSO).

105. **Answer: True.** Tokens are an example of type II authentication. Tokens, which are something you have, can be synchronous dynamic password tokens or asynchronous password devices. These devices use a challenge-response scheme and are form-factored as smart cards, USB plugs, key fobs, or keypad-based units. These devices generate authentication credentials that often are used as one-time passwords. Another great feature of token-based devices is that they can be used for two-factor authentication.

106. **Answer: True.** Keyboard dynamics is an example of type III authentication. Keyboard dynamics analyzes the speed and pattern of typing. Different biometric systems such as keyboard dynamics have varying levels of accuracy. The accuracy of a biometric device is measured by the percentage of type 1 and type 2 errors it produces.

107. **Answer: False.** Scrubbing is an activity undertaken by a user to erase evidence of illegal or unauthorized acts.

108. Answer: False. Keystroke monitoring can be used to watch employees' activities. Keystroke monitors can be either hardware or software devices. One important issue with their use is acceptable use policies (AUPs). Users must understand that their activities can be monitored and that privacy is not implied.

109. Answer: True. A federated identity is an IdM that is considered portable. For example, consider someone who travels by both plane and rental car. If both the airline and the rental car company use a federated identity management system, the traveler's authentication can be used between the two organizations.

110. Answer: True. Type I authentication systems typically have a clipping level set to 3. This limits logon attempts to three tries or successive attempts.

111. The answers are as follows:

- **A. Smurf: 4.** Uses a ping packet to broadcast addresses spoofed from the victim. The victim is flooded with ping replies.
- **B. LAND: 2.** Sends a spoofed SYN packet that is addressed with the target's address and port as the source and destination.
- **C. TRINOO: 5.** An early type of DDoS attack.
- **D. SYN attack: 3.** Sends a rapid series of spoofed SYN packets that are designed fill up the receiver queue.
- **E. Chargen: 1.** Loops traffic between echo and chargen on ports 7 and 19.
- **F. Ping of death: 6.** Sends ICMP ping packets that are at or exceed maximum size.

Being able to identify common DoS and DDoS attacks will help you be prepared for the exam.

112. Match each access control type with its definition.

A. Discretionary access control:	**4.** Classification labeling of objects by owner
B. Mandatory access control:	**3.** Uses sensitivity labels
C. Role-based access control:	**1.** Assigns access to groups not users
D. Rule-based access control:	**2.** Used with firewalls and routers
E. Constrained user interfaces:	**5.** Works by restricting users to specific functions based on their role in the system

113. Match each item with the correct authentication type

A. CER:	**2.** Something you are
B. Weakest form of encryption:	**1.** Something you know
C. Common access card:	**3.** Something you have
D. Type II error:	**2.** Something you are
E. Memory card:	**3.** Something you have
F. Pronounceable passwords:	**1.** Something you know

114. Match each authentication type with its definition.

A. Centralized authentication:	**3.** XTACACS
B. Uses ticket-granting service:	**1.** Kerberos
C. Allows secure web domains to exchange user authentication data:	**2.** SAML
D. Uses a single authentication server:	**1.** Kerberos
E. Uses port 389:	**2.** LDAP
F. Introduced by Cisco:	**3.** XTACACS