EXAM CRAM

CompTIA

Security+™

SY0-301

Practice Questions

Third Edition

CD FEATURES 800+ PRACTICE QUESTIONS

PEARSON

CompTIA AUTHORIZED

DIANE BARRETT

EXAM CRAM

CompTIA Security+ SY0-301

Practice Questions Third Edition

Diane Barrett

800 East 96th Street, Indianapolis, Indiana 46240 USA

CompTIA Security+ SY0-301 Practice Questions Exam Cram, Third Edition

ISBN-13: 978-0-7897-4828-7
ISBN-10: 0-7897-4828-2

Printed in the United States of America

Second Printing: October 2013

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson 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 CD or programs accompanying it.

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the U.S., please contact

International Sales
international@pearsoned.com

Publisher
Paul Boger

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Senior Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Technical Editor
Chris Crayton

Project Editor
Mandie Frank

Copy Editor
Barbara Hacha

Proofreader
Leslie Joseph

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Tim Warner

Cover Designer
Gary Adair

Page Layout
Studio Galou, LLC

Contents at a Glance

Table of Contents

Chapter Two

About the Author

Diane Barrett is the director of training for Paraben Corporation and an adjunct professor for American Military University. She has done contract forensic and security assessment work for several years and has authored other security and forensic books. She is a regular committee member for ADFSL's Conference on Digital Forensics, Security and Law, as well as an academy director for Edvancement Solutions. She holds many industry certifications, including CISSP, ISSMP, DFCP, PCME, along with many CompTIA certifications, including the Security+ (2011 objectives). Diane's education includes a MS in Information Technology with a specialization in Information Security. She expects to complete a PhD in business administration with a specialization in Information Security shortly.

Dedication

To my niece Elizabeth, who never ceases to amaze me.

Acknowledgments

Publishing a book takes the collaboration and teamwork of many individuals. Thanks to everyone involved in this process at Pearson Education, especially Betsy and Drew. To the editorial and technical reviewers, especially Chris Crayton, thank you for making sure that my work was sound and on target. Special thanks to my husband for all his support and patience while I worked on this project.

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.

As an Associate Publisher for Pearson, I welcome your comments. You can email or write me directly to let me 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 I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.examcram.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

CompTIA.

CompTIA Security+

- Designed for IT professionals focused on system security.
- Covers network infrastructure, cryptography, assessments, and audits.
- Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.

It Pays to Get Certified

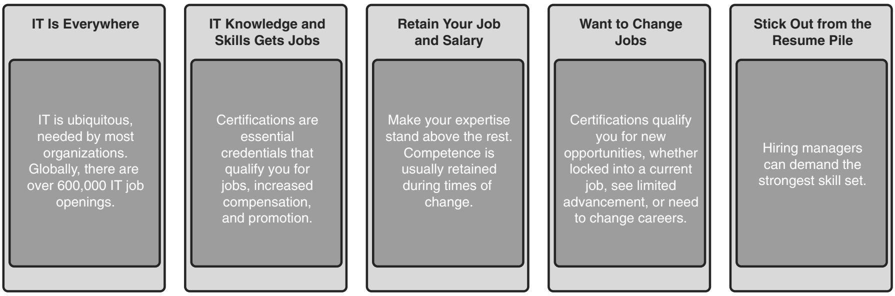
In a digital world, **digital literacy is an essential survival skill—**Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation and promotion.

Security is one of the highest demand job categories—growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

CompTIA Security+™

- **Jobs for security administrators are expected to increase by 18%—** the skill set required for these types of jobs map to CompTIA Security+ certification.
- **Network Security Administrators—**can earn as much as $106,000 per year.
- **CompTIA Security+ is the first step—**in starting your career as a Network Security Administrator or Systems Security Administrator.
- **CompTIA Security+ is regularly used in organizations—**such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career



IT Is Everywhere

IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.

IT Knowledge and Skills Gets Jobs

Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.

Retain Your Job and Salary

Make your expertise stand above the rest. Competence is usually retained during times of change.

Want to Change Jobs

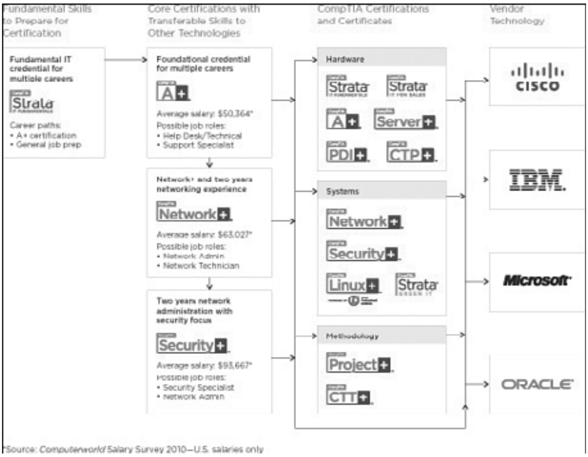
Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

Stick Out from the Resume Pile

Hiring managers can demand the strongest skill set.

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



*Source: *Computerworld* Salary Survey 2010—U.S. salaries only

Steps to Getting Certified and Staying Certified

Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam. http://certification.comptia.org/Training/testingcenters/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam. http://certification.comptia.org/Training/testingcenters/samplequestions.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: http://www.comptiastore.com/
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://certification.comptia.org/Training/testingcenters.aspx
Stay Certified! Continuing education	Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of your certification. There are a number of ways the certification can be renewed. For more informa tion go to: http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx

Join the Professional Community

Join IT Pro Community

http://itpro.comptia.org

The free IT Pro online community provides valuable content to students and professionals.

Career IT Job Resources

- Where to start in IT
- Career Assessments
- Salary Trends
- US Job Board

Forums on Networking, Security, Computing and Cutting Edge Technologies

Access to blogs written by Industry Experts

Current information on Cutting Edge Technologies

Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content.** This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition—**CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by Hiring Managers—**Hiring managers value CompTIA certification, because it is vendor- and technology-independent validation of your technical skills.
- **Recommended or Required by Government and Businesses—**Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)
- **Three CompTIA Certifications ranked in the top 10—**In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

- **Visit CompTIA online—**www.comptia.org to learn more about getting CompTIA certified.
- **Contact CompTIA—**Call 866-835-8020 ext. 5 or email questions@comptia.org.
- **Join the IT Pro Community—**http://itpro.comptia.org to join the IT community to get relevant career information.
- **Connect with us—**in f You Tube

Introduction

Welcome to *CompTIA Security+ SYO-301 Practice Questions Exam Cram*. The sole purpose of this book is to provide you with practice questions and answers and explanations that will help you learn, drill, and review for the Security+ Certification (2011 Edition) exam. The book offers a large number of questions to practice each exam objective and will help you assess your knowledge before you take the real exam. The detailed answers to every question will help reinforce your knowledge about different concepts covered on the Security+ (2011 Edition) exam.

Who This Book Is For

If you have studied the SY0-301 exam's content and think you are ready to put your knowledge to the test, but you are not sure that you want to take the real exam yet, this book is for you! Maybe you have answered other practice questions or unsuccessfully taken the real exam, reviewed, and want to do more practice questions before going to take the real exam; this book is for you, too! Even when the exam is done and you have passed with flying colors and have the Security+ Certification in your pocket, keep the book handy on your desktop to look for answers to your everyday security issues.

What You Will Find in This Book

This book is all about practice questions. The practice questions in the book, some very easy and others a bit more difficult (perhaps with a little complicated problem scenario, for example), are all aimed at raising your confidence level before you take the real exam. In fact, you will even find questions that you will face in real life.

This book is organized according to the objectives published by CompTIA for the SY0-301: CompTIA Security+ (2011 Edition) exam (find the updated exam information at http://certification.comptia.org/Training/testingcenters/exam-objectives.aspx). Each chapter corresponds to an exam domain, and in every chapter you will find the following three elements:

- **Practice questions**: These are the numerous questions that will help you learn, drill, and review exam objectives. All the questions in this section are multiple-choice type. Choose the correct answer based on your knowledge of security.

- **Quick-check answer key**: After you have finished answering the questions, you can quickly grade your exam from this section. Only correct answers are given in this section. No explanations are offered yet. Even if you have answered a question incorrectly, do not be discouraged. Just move on! Keep in mind that this is not the real exam. You can always review the topic and do the questions again.
- **Answers and explanations**: This section provides you with correct answers and further explanations about the content addressed in that question. Use this information to learn why an answer is correct and to reinforce the content in your mind for the exam day.

It is not possible to reflect a real exam on a paper product. As mentioned earlier, the purpose of the book is to help you prepare for the exam, not to provide you with real exam questions. Neither the author nor the publisher can guarantee that you will pass the exam just by memorizing the practice questions in this book.

You will also find a Cram Sheet at the beginning of the book specifically written for the exam day. The Cram Sheet contains core knowledge that you need for the exam and is also found in the book *CompTIA Security+ SYO-301 Exam Cram, Third Edition* (ISBN: 0789748290). The Cram Sheet condenses all the necessary facts covered on the exam into an easy-to-handle tear card. It is something you can carry with you to the testing center and use as a last-second study aid. Be aware that you cannot take the Cram Sheet into the exam room, though.

Hints for Using This Book

Because this book is a practice product on paper, you might want to complete your exams on a separate piece of paper so that you can reuse the exams without having previous answers in your way. Also, a general rule across all practice question products is to make sure that you are scoring well into the high 80% to 90% range on all topics before attempting the real exam. The higher percentages you score on practice question products, the better your chances for passing the real exam. Of course, we cannot guarantee a passing score on the real exam, but we can offer you plenty of opportunities to practice and assess your knowledge levels before you enter the real exam.

When you have completed the exam on paper, use the companion CD to take a timed exam. Doing so will help build your confidence and help you determine whether you need to study more. Your results will indicate the exam objectives in which you need further study or hands-on practice.

Need Further Study?

Are you having a hard time correctly answering these questions? If so, you probably need further review of all exam objectives. Be sure to see the following sister products to this book:

CompTIA Security+ SYO-301 Exam Cram, *Third Edition*, by Diane Barrett, Kalani K. Hausman, Martin Weiss (ISBN: 0789748290)

This page intentionally left blank

3

CHAPTER THREE

Domain 3.0: Threats and Vulnerabilities

Securing your resources is a challenge in any working environment. After all, resources are now commonly attacked through software, hardware, and peripherals. Domain 3 of the Security+ exam requires that you understand how to identify and minimize system threats to thwart would-be attackers and that you recognize the different types of assessment tools that are available to discover security threats and vulnerabilities. Be sure to give yourself plenty of time to review all these concepts because there are quite a few. The following list identifies the key areas from Domain 3.0 (which counts as 21% of the exam) that you need to master:

- Analyze and differentiate among types of malware
- Analyze and differentiate among types of attacks
- Analyze and differentiate among types of social engineering attacks
- Analyze and differentiate among types of wireless attacks
- Analyze and differentiate among types of application attacks
- Analyze and differentiate among types of mitigation and deterrent techniques
- Implement assessment tools and techniques to discover security threats and vulnerabilities
- Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

Quick Check

Practice Questions

Objective 3.1: Analyze and differentiate among types of malware.

1. Which of the following is the most common result of a buffer overflow?

Quick Answer: **180**
Detailed Answer: **184**

   ❍ **A.** Privilege escalation

   ❍ **B.** Disguised malicious programs

   ❍ **C.** Code replication

   ❍ **D.** Collection of personal data

2. Which of the following best describes a virus?

Quick Answer: **180**
Detailed Answer: **184**

   ❍ **A.** An action that exceeds the storage-space allocation of an application

   ❍ **B.** A program disguised as a useful application

   ❍ **C.** A program designed to attach itself to other code and replicate

   ❍ **D.** Software that communicates information from a user's system without notifying the user

3. Which of the following is best describes a Trojan?

Quick Answer: **180**
Detailed Answer: **184**

   ❍ **A.** It infects other systems only after a user executes the application that it is buried in.

   ❍ **B.** It sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

   ❍ **C.** It collects personal information, or changes your computer configuration without appropriately obtaining prior consent.

   ❍ **D.** It is self-replicating and therefore needs no user intervention.

4. Which of the following best describes a rootkit?

Quick Answer: **180**
Detailed Answer: **185**

   ❍ **A.** Software used for the collection of personal data

   ❍ **B.** Software hidden on a computer for the purpose of compromising the system

Quick Check

❍ **C.** Software that provides the originator with the venue to propagate

❍ **D.** Software that reports data such as surfing habits and sites visited

5. Which of the following is considered a worm?

Quick Answer: **180**
Detailed Answer: **185**

❍ **A.** Melissa

❍ **B.** Acid Rain

❍ **C.** Code Red

❍ **D.** Mocmex

6. A disgruntled employee creates a utility for purging old emails from the server. Inside the utility is code that will erase the server's hard drive contents on January 1, 2012. This is an example of which of the following attacks?

Quick Answer: **180**
Detailed Answer: **185**

❍ **A.** Virus

❍ **B.** Logic bomb

❍ **C.** Spoofing

❍ **D.** Trojan horse

7. Which of the following best describes spyware?

Quick Answer: **180**
Detailed Answer: **185**

❍ **A.** Software used for the collection of personal data

❍ **B.** Software hidden on a computer for the purpose of compromising the system

❍ **C.** Software that provides the originator with the venue to propagate

❍ **D.** Software that reports data such as surfing habits and sites visited

8. Which of the following is the best reason not to request to be removed from a mailing list in a reply to an unsolicited email?

Quick Answer: **180**
Detailed Answer: **185**

❍ **A.** It allows the sender to spoof your email address.

❍ **B.** It is a waste of time because the sender very seldom removes you from the list.

❍ **C.** It verifies that you have a legitimate, working email address.

❍ **D.** It allows the sender to collect personal data.

Quick Check

9. Which of the following are methods by which email spam lists are created? (Select all correct answers.)

❍ **A.** Searching the Web for addresses
❍ **B.** Scanning newsgroup postings
❍ **C.** Stealing Internet mailing lists
❍ **D.** Stealing user email address books

Quick Answer: **180**
Detailed Answer: **185**

10. Which of the following best describes programming errors that result in allowing someone to gain unauthorized administrative access?

❍ **A.** Buffer overflow
❍ **B.** Virus
❍ **C.** Trojan
❍ **D.** Logic bomb

Quick Answer: **180**
Detailed Answer: **186**

11. Which of the following best describes malware that takes advantage of a security hole, and then automatically replicates to other systems running the same software?

❍ **A.** Spyware
❍ **B.** Virus
❍ **C.** Trojan
❍ **D.** Worm

Quick Answer: **180**
Detailed Answer: **186**

12. Which of the following is a type of malware that is disguised as a useful application?

❍ **A.** Spyware
❍ **B.** Virus
❍ **C.** Trojan
❍ **D.** Worm

Quick Answer: **180**
Detailed Answer: **186**

13. Which of the following is a type of malware associated with collecting personal information without appropriately obtaining prior consent?

❍ **A.** Spyware
❍ **B.** Virus
❍ **C.** Trojan
❍ **D.** Worm

Quick Answer: **180**
Detailed Answer: **186**

Quick Check

14. Which of the following is a type of malware hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges?

Quick Answer: **180**
Detailed Answer: **187**

❍ **A.** Spyware
❍ **B.** Spam
❍ **C.** Adware
❍ **D.** Rootkit

15. Which of the following is a type of malware that provides the spam or virus originator with a venue to propagate?

Quick Answer: **180**
Detailed Answer: **187**

❍ **A.** Logic bomb
❍ **B.** Botnet
❍ **C.** Adware
❍ **D.** Rootkit

16. Which of the following is true with regard to antispyware programs?

Quick Answer: **180**
Detailed Answer: **187**

❍ **A.** They must be updated regularly.
❍ **B.** They can detect rootkits.
❍ **C.** They can detect botnets.
❍ **D.** They do not have to be updated.

17. Which of the following best describes the primary security issue with botnets?

Quick Answer: **180**
Detailed Answer: **187**

❍ **A.** They are malicious.
❍ **B.** They can remain undetected.
❍ **C.** They can execute code.
❍ **D.** They are remotely controlled.

18. Which of the following is also referred to as slag code?

Quick Answer: **180**
Detailed Answer: **187**

❍ **A.** Logic bomb
❍ **B.** Botnet
❍ **C.** Adware
❍ **D.** Rootkit

Quick Check

19. A buffer overflow can result in which of the following? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **187**

- ❍ **A.** Overwriting of data or memory storage
- ❍ **B.** A denial of service
- ❍ **C.** Automatic code replication to other hosts
- ❍ **D.** Execution of arbitrary code at a privileged level

20. Which of the following are virus types? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **188**

- ❍ **A.** Polymorphic
- ❍ **B.** Polynomial
- ❍ **C.** Stealth
- ❍ **D.** Covert

21. Which of the following best describes a boot sector virus?

Quick Answer: **180**
Detailed Answer: **188**

- ❍ **A.** Can change each time it is executed to avoid detection
- ❍ **B.** Uses techniques to avoid detection
- ❍ **C.** Is placed into the first sector of the hard drive
- ❍ **D.** Infects executable program files and becomes active in memory

22. Which of the following is another name for a botnet?

Quick Answer: **180**
Detailed Answer: **188**

- ❍ **A.** Privilege escalation
- ❍ **B.** Global hook
- ❍ **C.** Honeynet
- ❍ **D.** Zombie army

23. Which of the following is most like spyware?

Quick Answer: **180**
Detailed Answer: **188**

- ❍ **A.** Virus
- ❍ **B.** Trojan
- ❍ **C.** Spam
- ❍ **D.** Worm

24. Which of the following best describes what rootkits use for stealth activity?

Quick Answer: **180**
Detailed Answer: **188**

- ❍ **A.** Global hooks
- ❍ **B.** Tracking software/adware
- ❍ **C.** Privilege escalation
- ❍ **D.** Social engineering

Quick Check

25. Which of the following is the most effective method to avoid rootkit infection?

Quick Answer: **180**
Detailed Answer: **188**

❍ **A.** Never responding to the sender of an unsolicited email message

❍ **B.** Running operating systems from an account with lesser privileges

❍ **C.** Properly disabling the accounts of all terminated employees

❍ **D.** Only downloading trusted applications

26. Which of the following best describes a botnet?

Quick Answer: **180**
Detailed Answer: **188**

❍ **A.** A program designed to execute malicious actions when a certain event occurs or a period of time goes by

❍ **B.** A large number of programs disguised as useful applications

❍ **C.** A large number of computers that forward transmissions to other computers on the Internet

❍ **D.** Exploitation in software code that takes advantage of a programming flaw

27. Which of the following terms is most closely related to software exploitation that crashes the system and leaves it in a state where arbitrary code can be executed?

Quick Answer: **180**
Detailed Answer: **189**

❍ **A.** Logic bomb

❍ **B.** Privilege escalation

❍ **C.** Spam

❍ **D.** Trojan

28. Which of the following are the most effective ways to prevent an attacker from exploiting software? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **189**

❍ **A.** Apply current patches

❍ **B.** Do not allow Internet access

❍ **C.** Apply current service packs

❍ **D.** Monitor the Web for newly discovered vulnerabilities

29. Which of the following virus is a hybrid of boot and program viruses?

Quick Answer: **180**
Detailed Answer: **189**

❍ **A.** Polymorphic

❍ **B.** Macro

❍ **C.** Stealth

❍ **D.** Multipartite

Quick Check

30. Which of the following malware finds other systems running the same vulnerable software and then replicates itself without any user interaction?

Quick Answer: **180**
Detailed Answer: **189**

- ❍ **A.** Virus
- ❍ **B.** Trojan
- ❍ **C.** Worm
- ❍ **D.** Logic bomb

31. Which of the following is the main difference between a Trojan and a virus?

Quick Answer: **180**
Detailed Answer: **189**

- ❍ **A.** A Trojan requires user interaction and a virus does not.
- ❍ **B.** A Trojan does not replicate itself and a virus does.
- ❍ **C.** A virus does not require user interaction and a Trojan does.
- ❍ **D.** A virus does not replicate itself and a Trojan does.

32. Which of the following are indications that a computer may contain spyware? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **189**

- ❍ **A.** The browser home page changes.
- ❍ **B.** It takes a long time for the Windows desktop to come up.
- ❍ **C.** Clicking a link does nothing or goes to an unexpected website.
- ❍ **D.** The email inbox contains an unsolicited email message.

33. Which of the following are acceptable ways of dealing with spam? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **190**

- ❍ **A.** Delete the email without opening it.
- ❍ **B.** Reply back and try to identify the spammer.
- ❍ **C.** Turn off the preview function of your email software.
- ❍ **D.** Immediately call the local law enforcement office.

34. Which of the following are ways a rootkit can be installed? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **190**

- ❍ **A.** By accessing documents on the local intranet.
- ❍ **B.** Included as part of software package.
- ❍ **C.** An unpatched vulnerability.
- ❍ **D.** The user downloads it.

Quick Check

35. Which of the following is a type of malware that can use encryption to protect outbound communications and piggyback on commonly used ports to communicate without interrupting other applications that use that port?

Quick Answer: **180**
Detailed Answer: **190**

❍ **A.** Logic bomb

❍ **B.** Botnet

❍ **C.** Adware

❍ **D.** Rootkit

36. The system administrator abruptly leaves the organization after being passed over for a promotion. Two weeks later, employees report they cannot access files. It has been determined that at midnight the system suddenly began deleting files. Which of the following is the most likely type of malicious code that caused this event?

Quick Answer: **180**
Detailed Answer: **190**

❍ **A.** Logic bomb

❍ **B.** Botnet

❍ **C.** Adware

❍ **D.** Rootkit

37. Which of the following would best describe the type of malicious code that enters a system through a freeware program that the user installed?

Quick Answer: **180**
Detailed Answer: **190**

❍ **A.** Virus

❍ **B.** Trojan

❍ **C.** Worm

❍ **D.** Logic bomb

38. Which of the following type of virus avoids antivirus software detection by changing form each time it is executed?

Quick Answer: **180**
Detailed Answer: **190**

❍ **A.** Polymorphic

❍ **B.** Macro

❍ **C.** Stealth

❍ **D.** Multipartite

39. Which of the following is an automated computer program controlled by outside sources with the intention of forwarding transmissions to other computers on the Internet?

Quick Answer: **180**
Detailed Answer: **191**

❍ **A.** Logic bomb

❍ **B.** Adware

❍ **C.** Bot

❍ **D.** Virus

Quick Check

40. Which of the following are steps taken to protect a network from malicious code? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **191**

❍ **A.** Do not use any type of removable media from another user without first scanning the disk.

❍ **B.** Open all attachments sent to you by people you might know.

❍ **C.** Install firewalls or intrusion-prevention systems on client machines.

❍ **D.** Subscribe to security newsgroups.

Objective 3.2: Analyze and differentiate among types of attacks.

1. Which of the following ports should be blocked when it has been determined that an intruder has been using Telnet for unauthorized access?

Quick Answer: **180**
Detailed Answer: **191**

❍ **A.** 110

❍ **B.** 21

❍ **C.** 23

❍ **D.** 443

2. Which of the following ports should be blocked when it has been determined that an intruder has been using SNMP for unauthorized access? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **191**

❍ **A.** 161

❍ **B.** 162

❍ **C.** 443

❍ **D.** 4445

3. Which of the following best describes TCP/IP hijacking?

Quick Answer: **180**
Detailed Answer: **191**

❍ **A.** Providing false identity information to gain unauthorized access

❍ **B.** An established connection without specifying a username or password

❍ **C.** An attacker takes control of a session between the server and a client

❍ **D.** Redirecting traffic by changing the IP record for a specific domain

Quick Check

4. Which of the following best describes spoofing?

❍ **A.** Providing false identity information to gain unauthorized access

❍ **B.** An established connection without specifying a username or password

❍ **C.** An attacker takes control of a session between the server and a client

❍ **D.** Redirecting traffic by changing the IP record for a specific domain

Quick Answer: **180**
Detailed Answer: **191**

5. Which of the following best describes a null session?

❍ **A.** Providing false identity information to gain unauthorized access

❍ **B.** An established connection without specifying a username or password

❍ **C.** An attacker takes control of a session between the server and a client

❍ **D.** Redirecting traffic by changing the IP record for a specific domain

Quick Answer: **180**
Detailed Answer: **192**

6. Which of the following best describes DNS poisoning?

❍ **A.** Providing false identity information to gain unauthorized access

❍ **B.** An established connection without specifying a username or password

❍ **C.** An attacker taking control of a session between the server and a client

❍ **D.** Redirecting traffic by changing the IP record for a specific domain

Quick Answer: **180**
Detailed Answer: **192**

7. Which of the following best describes a man-in-the-middle attack?

❍ **A.** An attacker takes advantage of the add/grace period to monopolize names without ever paying for them.

❍ **B.** Packets are captured, the pertinent information is extracted, and then packets are placed back on the network.

❍ **C.** An attack that typically involves flooding a listening port on a machine with packets to disrupt service.

❍ **D.** An attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

Quick Answer: **180**
Detailed Answer: **192**

Quick Check

8. Which of the following best describes a replay attack?

Quick Answer: **180**
Detailed Answer: **192**

- ❍ **A.** An attacker takes advantage of the add/grace period to monopolize names without ever paying for them.
- ❍ **B.** Packets are captured, the pertinent information is extracted, and then packets are placed back on the network.
- ❍ **C.** An attack that typically involves flooding a listening port on a machine with packets to disrupt service.
- ❍ **D.** An attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

9. Which of the following best describes a DDoS attack?

Quick Answer: **180**
Detailed Answer: **192**

- ❍ **A.** An attacker takes advantage of the add/grace period to monopolize names without ever paying for them.
- ❍ **B.** Packets are captured, the pertinent information is extracted, and then packets are placed back on the network.
- ❍ **C.** An attack that typically involves flooding a listening port on a machine with packets to disrupt the resources.
- ❍ **D.** An attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

10. Which of the following methods can be used to mitigate DDoS attacks? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **192**

- ❍ **A.** Setting up filters on external routers to drop all ICMP packets
- ❍ **B.** Reducing the amount of time before the reset of an unfinished TCP connection
- ❍ **C.** Increasing the amount of time before the reset of an unfinished TCP connection
- ❍ **D.** Setting up a filter that denies traffic originating from the Internet that shows an internal network address

11. Which of the following best describes ARP poisoning?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** Broadcasting a fake reply to an entire network
- ❍ **B.** Changing the IP record for a specific domain
- ❍ **C.** Sending fragmented UDP packets
- ❍ **D.** Distributing zombie software

Quick Check

12. Which of the following attacks is associated with services using an interprocess communication share such as network file and print-sharing services?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** DNS spoofing
- ❍ **B.** Null sessions
- ❍ **C.** ARP poisoning
- ❍ **D.** DNS kiting

13. Which of the following sends hundreds of ICMP packets to the host to block or reduce activity?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** DNS spoofing
- ❍ **B.** ARP poisoning
- ❍ **C.** Man-in-the-middle
- ❍ **D.** Denial of service

14 Which of the following type of attacks is most likely being executed when an unauthorized service is relaying information to a source outside the network?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** DNS spoofing
- ❍ **B.** ARP poisoning
- ❍ **C.** Man-in-the-middle
- ❍ **D.** Denial of service

15. Which of the following best describes the primary security issue with null sessions?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** The sessions are not terminated properly.
- ❍ **B.** The connection is not authenticated.
- ❍ **C.** The connection is not encrypted.
- ❍ **D.** The sessions are remotely controlled.

16. Which of the following is the most effective way to reduce null session vulnerability?

Quick Answer: **180**
Detailed Answer: **193**

- ❍ **A.** Reducing the reset time of an unfinished TCP connection
- ❍ **B.** Using the signing capabilities of certificates
- ❍ **C.** Setting up filters to drop all ICMP packets
- ❍ **D.** Disabling NetBIOS over TCP/IP

Quick Check

17. Which of the following are effective ways to mitigate spoofing attacks? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **194**

- ❍ **A.** Editing the Registry on Windows-based computers to restrict anonymous access
- ❍ **B.** Using IPsec to secure transmissions between critical servers and clients
- ❍ **C.** Denying traffic originating from the Internet that shows an internal network address
- ❍ **D.** Using the signing capabilities of certificates on servers and clients

18. Which of the following is the most effective method to mitigate session hijacking?

Quick Answer: **180**
Detailed Answer: **194**

- ❍ **A.** Denying traffic originating from the Internet that shows an internal network address
- ❍ **B.** Forcing users to reauthenticate before allowing transactions to occur
- ❍ **C.** Reducing the amount of time before the reset of an unfinished TCP connection
- ❍ **D.** Setting up filters on external routers to drop all incoming ICMP packets

19. When mitigating null session vulnerability, which of the following ports should be closed? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **194**

- ❍ **A.** 161
- ❍ **B.** 162
- ❍ **C.** 139
- ❍ **D.** 445

20. Which of the following sessions can typically result in a man-in-the-middle attack? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **194**

- ❍ **A.** Telnet
- ❍ **B.** Wireless
- ❍ **C.** Email
- ❍ **D.** Samba

Quick Check

21. Which of the following are ways to minimize the effects of DNS poisoning when hosting your own DNS? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **194**

❍ **A.** Checking that the hosting server is not open-recursive

❍ **B.** Running operating systems from an account with lesser privileges

❍ **C.** Using different servers for authoritative and recursive lookups

❍ **D.** Disabling recursive access for networks to resolve names that are not in zone files

22. Which of the following are the most effective methods to mitigate ARP poisoning on a large network? (Select all correct answers.)

Quick Answer: **180**
Detailed Answer: **194**

❍ **A.** Using equipment that offers port security

❍ **B.** Using static mapping for IP addresses and ARP tables

❍ **C.** Using script-based mapping for IP addresses and ARP tables

❍ **D.** Deploying monitoring tools or an intrusion detection system (IDS)

23. Which of the following best describes privilege escalation?

Quick Answer: **180**
Detailed Answer: **195**

❍ **A.** A default set of user credentials

❍ **B.** Data transmitted that can be easily sniffed

❍ **C.** Accidental or intentional access to resources

❍ **D.** Application code functions allowing unauthorized access

24. Which of the following best describes a back door?

Quick Answer: **180**
Detailed Answer: **195**

❍ **A.** A default set of user credentials

❍ **B.** Data transmitted that can be easily sniffed

❍ **C.** Accidental or intentional access to resources

❍ **D.** Application code functions allowing unauthorized access

25. In a corporate environment, which of the following is most vulnerable to DoS attacks?

Quick Answer: **180**
Detailed Answer: **195**

❍ **A.** Internal user systems

❍ **B.** Network resources

❍ **C.** Network storage

❍ **D.** Internal servers

Quick Check

26. Which of the following best describes a denial-of-service (DoS) attack?

Quick Answer: **180**
Detailed Answer: **195**

❍ **A.** Intentional access to resources not intended for access by the user

❍ **B.** Application code functions that allow unauthorized access to network resources

❍ **C.** Attempt to block access by overwhelming network availability

❍ **D.** Attempt to directly access the resources through unauthorized means

27. Which of the following is the best method to mitigate attacks against networking devices and services installed with a default set of user credentials?

Quick Answer: **180**
Detailed Answer: **195**

❍ **A.** Replacing them on an as-needed basis

❍ **B.** Replacing them when an attack has been detected

❍ **C.** Replacing them with unique strong logon credentials

❍ **D.** Replacing them with the same strong logon credential

28. Which of the following is the most common origin of back doors?

Quick Answer: **180**
Detailed Answer: **196**

❍ **A.** Created during application development

❍ **B.** Created during system certification

❍ **C.** Created during user interface testing

❍ **D.** Created during implementation

29. Which of the following should be performed when implementing distributed wireless network configurations spanning multiple buildings or open natural areas?

Quick Answer: **180**
Detailed Answer: **196**

❍ **A.** Land survey

❍ **B.** Building inspection

❍ **C.** OSHA inspection

❍ **D.** Site survey

30. Which of the following is most closely linked to privilege escalation?

Quick Answer: **180**
Detailed Answer: **196**

❍ **A.** SSID broadcast

❍ **B.** Application flaws

❍ **C.** Application development

❍ **D.** Automated attacks

Quick Check

31. Which of the following is most closely linked to weak passwords?

Quick Answer: **181**
Detailed Answer: **196**

- ❍ **A.** SSID broadcast
- ❍ **B.** Application flaws
- ❍ **C.** Application development
- ❍ **D.** Automated attacks

32. Which of the following is most closely linked to back doors?

Quick Answer: **181**
Detailed Answer: **197**

- ❍ **A.** SSID broadcast
- ❍ **B.** Application flaws
- ❍ **C.** Application development
- ❍ **D.** Automated attacks

33. Which of the following is most closely linked to default accounts?

Quick Answer: **181**
Detailed Answer: **197**

- ❍ **A.** Network resources
- ❍ **B.** Application flaws
- ❍ **C.** Network credentials
- ❍ **D.** Automated attacks

34. Which of the following is most closely linked to denial of service?

Quick Answer: **181**
Detailed Answer: **197**

- ❍ **A.** Network resources
- ❍ **B.** SSID broadcast
- ❍ **C.** Network credentials
- ❍ **D.** Application development

35. Which of the following best describes the situation where User A can read User B's email without specific authorization?

Quick Answer: **181**
Detailed Answer: **197**

- ❍ **A.** Privilege escalation
- ❍ **B.** Default accounts
- ❍ **C.** Weak passwords
- ❍ **D.** Back door

36. Which of the following best describes the situation where a software designer puts in shortcut entry points to allow rapid code evaluation and testing?

Quick Answer: **181**
Detailed Answer: **198**

- ❍ **A.** Privilege escalation
- ❍ **B.** Default accounts
- ❍ **C.** Weak passwords
- ❍ **D.** Back door

Quick Check

37. Which of the following attacks are associated with weak passwords? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **198**

❍ **A.** Packet sniffing

❍ **B.** Automated attacks

❍ **C.** Social engineering

❍ **D.** Denial of service

38. Which of the following attacks are associated with fringe service industries such as online casinos?

Quick Answer: **181**
Detailed Answer: **198**

❍ **A.** Packet sniffing

❍ **B.** Automated attacks

❍ **C.** Social engineering

❍ **D.** Denial of service

39. Which of the following is an email attack that is targeted toward a specific individual?

Quick Answer: **181**
Detailed Answer: **199**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Pharming

40. Which of the following is an attack where the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone?

Quick Answer: **181**
Detailed Answer: **199**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Pharming

41. Which of the following is an attack that redirects victims to a bogus website, even if they correctly entered the intended site?

Quick Answer: **181**
Detailed Answer: **199**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Pharming

Quick Check

42. Which of the following attacks involves using phishing methods through text messaging?

Quick Answer: **181**
Detailed Answer: **199**

- ❍ **A.** Spear Phishing
- ❍ **B.** Vishing
- ❍ **C.** Smishing
- ❍ **D.** Pharming

43. Which of the following is a type of advertising message that targets users of instant messaging (IM) services?

Quick Answer: **181**
Detailed Answer: **199**

- ❍ **A.** Vishing
- ❍ **B.** Spim
- ❍ **C.** Spam
- ❍ **D.** Phishing

44. Which of the following observing attacks observes how a host responds to an odd TCP/IP packet?

Quick Answer: **181**
Detailed Answer: **200**

- ❍ **A.** DNS spoofing
- ❍ **B.** Null sessions
- ❍ **C.** ARP poisoning
- ❍ **D.** Xmas attack

45. Which of the following attacks is accomplished by gaining the trust of a computer that is trusted by the target network?

Quick Answer: **181**
Detailed Answer: **200**

- ❍ **A.** Packet sniffing
- ❍ **B.** Transitive access
- ❍ **C.** Social engineering
- ❍ **D.** Denial of service

Quick Check

Objective 3.3: Analyze and differentiate among types of social engineering attacks.

1. A help desk employee receives a call from someone who is posing as a technical aide attempting to update some type of information, and asks for identifying user details that may then be used to gain access. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **200**

❍ **A.** Pharming

❍ **B.** Social engineering

❍ **C.** Phishing

❍ **D.** Shoulder surfing

2. A help desk employee receives a call from the administrative assistant. She has received an email stating if she doesn't respond within 48 hours with certain personal information, the corporate bank account will be closed. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **200**

❍ **A.** Pharming

❍ **B.** Social engineering

❍ **C.** Phishing

❍ **D.** Shoulder surfing

3. The help desk is flooded with calls from users that received an email warning them of a new virus. The mail instructed the users to search for and delete several files from their systems. Many of the users who attempted to reboot their systems after deleting the specified files are having difficulties and the machines are not rebooting properly. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **200**

❍ **A.** Pharming

❍ **B.** Hoax

❍ **C.** Phishing

❍ **D.** Spam

4. An organization discovers that many employees have been responding to chain letter emails. Which of the following is the greatest concern to the organization?

Quick Answer: **181**
Detailed Answer: **201**

❍ **A.** Undue burden on resources.

❍ **B.** They may contain viruses.

Quick Check

❍ **C.** Theft of proprietary information.

❍ **D.** Nothing. Chain letters are harmless.

5. An organization allows employees to access confidential data remotely. Many of the sales staff spend extended time in public places and use this downtime to catch up on work. Which of the following is the greatest concern to the organization?

Quick Answer: **181**
Detailed Answer: **201**

❍ **A.** Virus infection

❍ **B.** Social engineering

❍ **C.** Dumpster diving

❍ **D.** Shoulder surfing

6. Which of the following type of attacks is intended to go after high-profile targets such as an executive within a company?

Quick Answer: **181**
Detailed Answer: **201**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Whaling

7. An employee receives an automated call from the organization's bank asking the employee to enter the bank account number and pin on the telephone keypad to verify account information for their records. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **201**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Whaling

8. The employees in the financial department of your organization have received emails from the local credit union, asking them to click on a link inside the email to update their passwords and user IDs because of a recent security breach. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **201**

❍ **A.** Spear Phishing

❍ **B.** Vishing

❍ **C.** Smishing

❍ **D.** Whaling

Quick Check

9. An organization does not have a policy on proper document disposal. When Mary goes outside to empty her trash, a nice young man has been offering to do it for her. Which of the following best describes the attack that is taking place?

Quick Answer: **181**
Detailed Answer: **202**

❍ **A.** Virus infection

❍ **B.** Social engineering

❍ **C.** Dumpster diving

❍ **D.** Shoulder surfing

10. As Joe is about to enter a secured building, a nice young woman runs up behind him, smiles, and follows him into the building without using her own ID. Which of the following type of attack has occurred?

Quick Answer: **181**
Detailed Answer: **202**

❍ **A.** Pharming

❍ **B.** Social engineering

❍ **C.** Shoulder surfing

❍ **D.** Tailgating

Objective 3.4: Analyze and differentiate among types of wireless attacks.

1. Which of the following best describes a major security issue when implementing WAPs?

Quick Answer: **181**
Detailed Answer: **202**

❍ **A.** WEP is the default encryption.

❍ **B.** The SSID is broadcast in plain text.

❍ **C.** They are hard to physically locate.

❍ **D.** Any node can view the data of another node.

2. Which of the following best describes why data emanation is a security risk in wireless networks? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **202**

❍ **A.** It uses 802.1x transmissions that generate detectable radio-frequency signals funneled into one direction.

❍ **B.** Sniffing the data may use many solutions to increase the distance over which detection is possible.

❍ **C.** Sniffing the data may use many solutions to reduce the distance over which transmission is possible.

❍ **D.** It uses 802.1x transmissions that generate detectable radio-frequency signals in all directions.

Quick Check

3. Which of the following is the primary method to mitigate the vulnerabilities associated with communication over an 802.1x wireless link?

❍ **A.** Authorization

❍ **B.** Authentication

❍ **C.** Encryption

❍ **D.** Identification

Quick Answer: **181**
Detailed Answer: **203**

4. Which of the following type of attacks is associated with the use of wireless communication? (Select all correct answers.)

❍ **A.** Packet sniffing

❍ **B.** Session hijacking

❍ **C.** Man-in-the-middle

❍ **D.** Spam relaying

Quick Answer: **181**
Detailed Answer: **203**

5. Which best describes why session hijacking is possible in wireless communication?

❍ **A.** There is no authorization mechanism.

❍ **B.** There is no authentication mechanism.

❍ **C.** The authentication mechanism is one-way.

❍ **D.** The authorization mechanism is one-way.

Quick Answer: **181**
Detailed Answer: **203**

6. Which of the following best describes why a man-in-the-middle attack is possible in wireless communication?

❍ **A.** The request for connection by the client is a bidirectional open broadcast.

❍ **B.** The request for connection by the access point is a bidirectional open broadcast.

❍ **C.** The request for connection by the access point is an omnidirectional open broadcast.

❍ **D.** The request for connection by the client is an omnidirectional open broadcast.

Quick Answer: **181**
Detailed Answer: **203**

7. Which of the following best describes war-driving?

❍ **A.** Driving around with a laptop system configured to listen for open access points

❍ **B.** Dialing a large range of telephone numbers in search of devices that can be exploited

❍ **C.** Marking landmarks to indicate the presence of an available access point

❍ **D.** Accessing an open public WAP for a monthly fee or commission from the end user

Quick Answer: **181**
Detailed Answer: **203**

Quick Check

8. Which of the following best describes war-chalking?

- ❍ **A.** Driving around with a laptop system configured to listen for open access points
- ❍ **B.** Dialing a large range of telephone numbers in search of devices that can be exploited
- ❍ **C.** Marking landmarks to indicate the presence of an available access point
- ❍ **D.** Accessing an open public for a monthly fee or commission from the end user

Quick Answer: **181**
Detailed Answer: **203**

9. Which of the following best describes bluejacking?

- ❍ **A.** Driving around with a laptop configured to listen for open access points
- ❍ **B.** Sending broadcast spam from a nearby Bluetooth-enabled device
- ❍ **C.** Deleting data on a Bluetooth device that has opened a connection
- ❍ **D.** Marking landmarks to indicate an available open access point

Quick Answer: **181**
Detailed Answer: **203**

10. Which of the following best describes bluesnarfing?

- ❍ **A.** Driving around with a laptop configured to listen for open access points
- ❍ **B.** Sending broadcast spam from a nearby Bluetooth-enabled device
- ❍ **C.** Deleting data on a Bluetooth device that has opened a connection
- ❍ **D.** Marking landmarks to indicate an available open access point

Quick Answer: **181**
Detailed Answer: **204**

11. Which of the following best describes a WLAN technology that uses Ethernet protocols?

- ❍ **A.** Wi-Fi
- ❍ **B.** i-Mode
- ❍ **C.** Bluetooth
- ❍ **D.** WAP

Quick Answer: **181**
Detailed Answer: **204**

Quick Check

12. Which of the following best describes the situation that allows using reflective tube waveguides such as a Pringle's can to capture data?

❍ **A.** Weak encryption

❍ **B.** Session hijacking

❍ **C.** War-driving

❍ **D.** Data emanation

Quick Answer: **181**
Detailed Answer: **204**

13. Which of the following best describes the situation that allows a hijacker to wait until the authentication cycle is completed, then generate a signal that causes the client to think it has been disconnected from the access point?

❍ **A.** Weak encryption

❍ **B.** Session hijacking

❍ **C.** War-driving

❍ **D.** Data emanation

Quick Answer: **181**
Detailed Answer: **204**

14. Which of the following best describes what might allow data transacted over an 802.1x wireless link to be passed in clear form?

❍ **A.** Weak encryption

❍ **B.** Session hijacking

❍ **C.** War-driving

❍ **D.** Data emanation

Quick Answer: **181**
Detailed Answer: **205**

15. Which of the following best describes the situation where an attack is aimed at pairing with the attacker's device for unauthorized access, modification, or deletion of data?

❍ **A.** Bluejacking

❍ **B.** Bluesnarfing

❍ **C.** War-driving

❍ **D.** War-chalking

Quick Answer: **181**
Detailed Answer: **205**

16. Which of the following best describes the situation that allows an attack aimed at the identification of existing wireless networks, the SSID used, and any known WEP keys?

❍ **A.** Weak encryption

❍ **B.** Session hijacking

❍ **C.** War-driving

❍ **D.** Data emanation

Quick Answer: **181**
Detailed Answer: **205**

Quick Check

17. Which of the following best describes the situation where an attack is aimed at generating messages that appear to be from the device itself?

Quick Answer: **181**
Detailed Answer: **205**

❍ **A.** Bluejacking

❍ **B.** Bluesnarfing

❍ **C.** War-driving

❍ **D.** War-chalking

18. In which of the following attacks would the implementation of a rogue AP with stronger signal strength than more remote permanent installations be found?

Quick Answer: **181**
Detailed Answer: **206**

❍ **A.** Weak encryption

❍ **B.** Man-in-the-middle

❍ **C.** War-driving

❍ **D.** Data emanation

19. The Wi-Fi Protected Access standards were developed by the Wi-Fi Alliance to replace which of the following?

Quick Answer: **181**
Detailed Answer: **206**

❍ **A.** DES

❍ **B.** WAP

❍ **C.** AES

❍ **D.** WEP

20. WSL is equivalent to which of the following layers of the OSI model?

Quick Answer: **181**
Detailed Answer: **206**

❍ **A.** Session

❍ **B.** Transport

❍ **C.** Network

❍ **D.** Presentation

Objective 3.5: Analyze and differentiate among types of application attacks.

1. Which of the following are identified vulnerabilities of the Java language? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **206**

❍ **A.** Buffer overflows

❍ **B.** Unauthorized file upload

❍ **C.** Email exposure

❍ **D.** Unexpected redirection

2. Which of the following most accurately describes how Java applets execute?

Quick Answer: **181**
Detailed Answer: **206**

❍ **A.** When the web server retrieves the directory web page

❍ **B.** When the web server's browser loads the hosting web page

❍ **C.** When the client machine's browser loads the hosting web page

❍ **D.** When the operating system loads the hosting web page

3. Which of the following best describes the reason Java applets are a security risk?

Quick Answer: **181**
Detailed Answer: **207**

❍ **A.** Java is compiled on the client browser.

❍ **B.** Java is a precompiled language.

❍ **C.** Java is compiled by the client operating system.

❍ **D.** Java applets execute on the hosting web server.

4. Which of the following are identified vulnerabilities of JavaScript? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **207**

❍ **A.** Buffer overflows

❍ **B.** Unauthorized file upload

❍ **C.** Email exposure

❍ **D.** Unexpected redirection

5. Which of the following is the most effective method to mitigate vulnerabilities exposed by earlier forms of Java?

Quick Answer: **181**
Detailed Answer: **207**

❍ **A.** Keeping machines up-to-date with new version releases

❍ **B.** Disabling third-party browser extensions

❍ **C.** Setting the pop-up blocker setting to high

❍ **D.** Enabling Integrated Windows Authentication

6. ActiveX and its controls share many of the same vulnerabilities present in which of the following?

Quick Answer: **181**
Detailed Answer: **207**

❍ **A.** Cookies

❍ **B.** JavaScript

❍ **C.** Embedded Java applets

❍ **D.** Common Gateway Interface script

Quick Check

7. Which of the following is the most realistic method to mitigate having cookies expose long-term browsing habits?

❍ **A.** Disabling third-party browser extensions

❍ **B.** Regularly clearing the browser cookie cache

❍ **C.** Configuring client browsers to block all cookies

❍ **D.** Disabling automatic code execution on client browsers

Quick Answer: **181**
Detailed Answer: **207**

8. Which of the following is the most effective method to mitigate buffer overflows or cross-site scripting attacks?

❍ **A.** Blocking third-party cookies

❍ **B.** Accepting only numeric data input

❍ **C.** Disabling third-party browser extensions

❍ **D.** Validating data input

Quick Answer: **181**
Detailed Answer: **207**

9. Which of the following is most likely to use a tracking cookie?

❍ **A.** Spyware

❍ **B.** Credit Union

❍ **C.** Trojan

❍ **D.** Shopping cart

Quick Answer: **181**
Detailed Answer: **208**

10. Which of the following best describes what the exploitation of Simple Mail Transfer Protocol (SMTP) relay agents is used for?

❍ **A.** Buffer overflow

❍ **B.** Logic bomb

❍ **C.** Spyware

❍ **D.** Spam

Quick Answer: **181**
Detailed Answer: **208**

11. Which of the following best describes a tracking cookie?

❍ **A.** Beneficial

❍ **B.** Permanent

❍ **C.** Temporary

❍ **D.** Valuable

Quick Answer: **181**
Detailed Answer: **208**

12. S-HTTP communicates over which of the following ports?

❍ **A.** 80

❍ **B.** 443

❍ **C.** 110

❍ **D.** 4445

Quick Answer: **181**
Detailed Answer: **208**

Quick Check

13. HTTPS communicates over which of the following ports?

Quick Answer: **181**
Detailed Answer: **208**

- ❍ **A.** 80
- ❍ **B.** 443
- ❍ **C.** 110
- ❍ **D.** 4445

14. Which of the following exploits are associated with SSL certificates? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **208**

- ❍ **A.** Ill-formatted requests
- ❍ **B.** Small key sizes
- ❍ **C.** Outdated CRLs
- ❍ **D.** Buffer overflows

15. Which of the following vulnerabilities are associated with LDAP? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **209**

- ❍ **A.** Ill-formatted requests
- ❍ **B.** Small key sizes
- ❍ **C.** Outdated CRLs
- ❍ **D.** Buffer overflows

16. Which of the following vulnerabilities are associated with FTP? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **209**

- ❍ **A.** Buffer overflows
- ❍ **B.** Anonymous file access
- ❍ **C.** Unencrypted authentication
- ❍ **D.** Improper formatted requests

17. FTP over SSL communicates over which of the following ports?

Quick Answer: **181**
Detailed Answer: **209**

- ❍ **A.** 21
- ❍ **B.** 80
- ❍ **C.** 22
- ❍ **D.** 81

18. Which of the following are security concerns when allowing IM applications on the network? (Select all correct answers.)

Quick Answer: **181**
Detailed Answer: **209**

- ❍ **A.** The capture of cached logs containing conversations
- ❍ **B.** Malware spreading through IM contacts
- ❍ **C.** Unauthorized data and video sharing
- ❍ **D.** Improper formatted requests

Quick Check

19. Which of the following are exploits for CGI scripts? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **209**

- ❍ **A.** Buffer overflows.
- ❍ **B.** Anonymous file access.
- ❍ **C.** Arbitrary commands may be executed on the server.
- ❍ **D.** Arbitrary commands may be executed on the client.

20. An attacker places code within a web page that redirects the client's browser to attack yet another site when a client's browser opens the web page. This is an example of what type of attack?

Quick Answer: **182**
Detailed Answer: **209**

- ❍ **A.** Unencrypted authentication
- ❍ **B.** Session hijacking
- ❍ **C.** Buffer overflow
- ❍ **D.** Cross-site scripting

21. Which of the following best describes Java or JavaScript?

Quick Answer: **182**
Detailed Answer: **210**

- ❍ **A.** Java applets allow access to cache information.
- ❍ **B.** JavaScript can provide access to files of known name.
- ❍ **C.** JavaScript runs even after the applet is closed.
- ❍ **D.** Java applets can execute arbitrary instructions on the server.

22. Which of the following is another name for identification of configuration details of the server that may be helpful to later identify unauthorized access attempts?

Quick Answer: **182**
Detailed Answer: **210**

- ❍ **A.** Profiling
- ❍ **B.** Reporting
- ❍ **C.** Abstracting
- ❍ **D.** Hyperlinking

23. Which of the following is the most likely reason it is dangerous to maintain cookie session information?

Quick Answer: **182**
Detailed Answer: **210**

- ❍ **A.** It provides custom user configuration settings.
- ❍ **B.** It may expose sensitive information about secured sites.
- ❍ **C.** It allows multiple actual connections to a web server.
- ❍ **D.** It may allow automatic code execution on client browsers.

Quick Check

24. Which of the following are browser-based vulnerabilities? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **210**

❍ **A.** Session hijacking

❍ **B.** SQL injection

❍ **C.** Buffer overflows

❍ **D.** Social engineering

25. Which of the following is of most concern for a security administrator when allowing peer-to-peer networking?

Quick Answer: **182**
Detailed Answer: **210**

❍ **A.** Buffer-overflow attacks can go unnoticed.

❍ **B.** Unauthorized file upload to network servers.

❍ **C.** Connections are negotiated directly between clients.

❍ **D.** Arbitrary commands may be executed on the server.

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques.

1. Physically unsecured equipment is vulnerable to which of the following type of attacks?

Quick Answer: **182**
Detailed Answer: **210**

❍ **A.** Brute force

❍ **B.** Social engineering

❍ **C.** Malware

❍ **D.** Rootkits

2. Which of the following is the primary goal of a physical security plan?

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** To deny access to most users allowing only corporate officers

❍ **B.** To allow access to all visitors without causing undue duress

❍ **C.** To allow only trusted use of resources via positive identification

❍ **D.** To deny access to all except users deemed credible

Quick Check

3. Which of the following may be used to prevent an intruder from monitoring users in very high-security areas? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** Picket fencing

❍ **B.** Painted glass

❍ **C.** Frosted glass

❍ **D.** Chain-link fencing

4. Which of the best describes the physical area known as no-man's land?

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** An area of cleared land surrounding a building

❍ **B.** An area of bushes surrounding a building

❍ **C.** A holding area between two entry points

❍ **D.** A receiver mechanism that reads an access card

5. Which of the following best describes a mantrap?

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** An area of cleared land surrounding a building

❍ **B.** An area of bushes surrounding a building

❍ **C.** A holding area between two entry points

❍ **D.** A receiver mechanism that reads an access card

6. Which of the following best describes the difference between a cipher lock and a wireless lock?

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** A cipher lock is opened by a receiver mechanism, whereas a wireless lock has a punch code entry.

❍ **B.** A cipher lock is opened with a key, whereas a wireless lock has a remote control mechanism.

❍ **C.** A cipher lock is opened with a remote control mechanism, whereas a wireless lock is opened with a key.

❍ **D.** A cipher lock has a punch code entry, whereas a wireless lock is opened by a receiver mechanism.

7. Which of the following type of surveillance would the organization implement if it was required that the parking lot be constantly monitored?

Quick Answer: **182**
Detailed Answer: **211**

❍ **A.** CCTV cameras

❍ **B.** Security guards

❍ **C.** Keycard gate

❍ **D.** Motion detectors

Quick Check

8. Which of the following technologies are used in external motion detectors? (Select all correct answers.)

❍ **A.** Infrared

❍ **B.** Sound

❍ **C.** RFID

❍ **D.** Ultrasonic

Quick Answer: **182**
Detailed Answer: **211**

9. Which of the following best describes mandatory physical control?

❍ **A.** User access is closely monitored and very restricted with no exceptions.

❍ **B.** Common needs are predetermined, and access is allowed with the same key.

❍ **C.** Access is delegated to parties responsible for that building or room.

❍ **D.** Each individual has a unique key that corresponds to his or her access needs.

Quick Answer: **182**
Detailed Answer: **211**

10. Which of the following best describes role-based physical control?

❍ **A.** User access is closely monitored and very restricted with no exceptions.

❍ **B.** Common needs are predetermined and access is allowed with the same key.

❍ **C.** Access is delegated to parties responsible for that building or room.

❍ **D.** Each individual has a unique key that corresponds to his or her access need.

Quick Answer: **182**
Detailed Answer: **212**

11. Which of the following physical safeguards would provide the best protection for a building that houses top-secret sensitive information and systems? (Choose all that apply.)

❍ **A.** Mantrap

❍ **B.** No-man's land

❍ **C.** Wooden fence

❍ **D.** Door access system

Quick Answer: **182**
Detailed Answer: **212**

12. Which of the following physical safeguards would be most commonly implemented in security for banks?

❍ **A.** Mantraps

❍ **B.** Security dogs

Quick Answer: **182**
Detailed Answer: **212**

Quick Check

❍ **C.** Painted glass

❍ **D.** Video surveillance

13. Which of the following is the main security concern of implementing motion detectors?

Quick Answer: **182**
Detailed Answer: **212**

❍ **A.** They can easily be deactivated.

❍ **B.** They can easily be fooled.

❍ **C.** They are extremely sensitive.

❍ **D.** They are extremely expensive.

14. Running which of the following commands is the quickest way to tell which ports are open and which services are running on the machine?

Quick Answer: **182**
Detailed Answer: **212**

❍ **A.** `netstat`

❍ **B.** `nbtstat`

❍ **C.** `ipconfig`

❍ **D.** `msconfig`

15. Which of the following protocols is used for monitoring the health of network equipment, computer equipment, and devices?

Quick Answer: **182**
Detailed Answer: **212**

❍ **A.** SNAP

❍ **B.** SMTP

❍ **C.** SDLC

❍ **D.** SNMP

16. Which of the following are effective ways to protect the network infrastructure from attacks aimed at antiquated or unused ports and protocols? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **212**

❍ **A.** Keeping only protocols installed by default

❍ **B.** Allowing traffic only on necessary ports

❍ **C.** Removing any unnecessary protocols

❍ **D.** Allowing only traffic requested by users

17. Which of the following would be considered a best practice for improved server performance when deciding where to store log files?

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** Store in the system directory of a machine in the DMZ

❍ **B.** Store in the system directory on the local machine

❍ **C.** Store on a nonsystem striped or mirrored disk volume

❍ **D.** Store on a nonsystem disk volume on the local machine

Quick Check

18. Which of the following would be considered a best security practice when deciding where to store log files?

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** Stored in the system directory on the local machine

❍ **B.** Stored in a data directory on a server in the intranet

❍ **C.** Stored in the system directory of a machine in the DMZ

❍ **D.** Stored in a centralized repository of an offline volume

19. An organization requires the implementation of an enterprise application logging strategy. Which of the following would be a critical analysis consideration when choosing a solution?

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** A proprietary custom-built solution

❍ **B.** Already built-in application logging solutions

❍ **C.** A solution that uses standard protocols and formats

❍ **D.** A variety of solutions that each use different formats

20. Internet Information Services (IIS) logs can be used for which of the following purposes? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** Assess content

❍ **B.** Identify bottlenecks

❍ **C.** End processes

❍ **D.** Investigate attacks

21. Which of the following most accurately describes best practice for using Microsoft DNS logging?

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** Only the user events should be logged.

❍ **B.** Only pertinent events should be logged.

❍ **C.** All events should be logged so nothing is missed.

❍ **D.** Nothing should be logged until there is a need for it.

22. Which of the following would be the first place an administrator would look when troubleshooting UNIX- or Linux-based systems?

Quick Answer: **182**
Detailed Answer: **213**

❍ **A.** Mtools.conf

❍ **B.** Msconfig

❍ **C.** Event Viewer

❍ **D.** Syslogd

Quick Check

23. Which of the following would be considered best practices for system logging? (Select all correct answers.)

❍ **A.** For easy compilation, keep log files in plain text.

❍ **B.** When permissible, encrypt the log files.

❍ **C.** Store log files on a standalone system.

❍ **D.** Store log files on individual system data partitions.

Quick Answer: **182**
Detailed Answer: **213**

24. Which of the following would an administrator use to end applications that get hung up without having to reboot the machine?

❍ **A.** Network Monitor

❍ **B.** Task Manager

❍ **C.** Event Viewer

❍ **D.** Performance Console

Quick Answer: **182**
Detailed Answer: **213**

25. Which of the following would provide information for troubleshooting remote-access policy issues?

❍ **A.** Internet Information Services logging

❍ **B.** Critical and error-level logging

❍ **C.** Authentication and accounting logging

❍ **D.** Event Viewer Application logging

Quick Answer: **182**
Detailed Answer: **214**

26. Which of the following types of logging events are most commonly found in antivirus software? (Select all correct answers.)

❍ **A.** Updates

❍ **B.** Dropped packets

❍ **C.** Quarantined viruses

❍ **D.** Update history

Quick Answer: **182**
Detailed Answer: **214**

27. An organization primarily contracts workers and is concerned about remote-access usage and remote-authentication attempts. Which of the following would the organization implement to track this type of activity?

❍ **A.** Firewall logging

❍ **B.** RRAS logging

❍ **C.** IIS logging

❍ **D.** System logging

Quick Answer: **182**
Detailed Answer: **214**

Quick Check

28. Which of the following best describes auditing?

Quick Answer: **182**
Detailed Answer: **214**

❍ **A.** The process of measuring the performance of a network

❍ **B.** The process of collecting data to be used for monitoring

❍ **C.** The process of tracking users and actions on the network

❍ **D.** The process of observing the state of a system

29. Which of the following are unintended consequences when auditing is not clear-cut or built around the organizational goals and policies? (Select all correct answers.)

Quick Answer: **182**
Detailed Answer: **214**

❍ **A.** Irrelevant information is gathered.

❍ **B.** Important security events are deleted.

❍ **C.** User hard drives quickly run out of space.

❍ **D.** System administrators have reduced workloads.

30. A systems administrator is tasked with auditing user privileges. Which of the following steps must be taken? (Select two correct answers.)

Quick Answer: **182**
Detailed Answer: **214**

❍ **A.** Enable logging within the operating system.

❍ **B.** Enable auditing within the operating system.

❍ **C.** Specify the resources to be audited.

❍ **D.** Specify the audit file storage directory.

31. An organization has primarily contract workers and is concerned about unauthorized and unintentional access on these accounts. Which of the following would the organization audit to track this type of activity?

Quick Answer: **182**
Detailed Answer: **214**

❍ **A.** Group policies

❍ **B.** Retention policies

❍ **C.** DHCP events and changes

❍ **D.** Access use and rights changes

32. Which of the following is true about the auditing of failed logon events and successful login events?

Quick Answer: **182**
Detailed Answer: **214**

❍ **A.** Only failed events should be audited.

❍ **B.** Only successful events should be audited.

❍ **C.** Both successful and failed events should be audited.

❍ **D.** Neither one should be audited unless absolutely necessary.

Quick Check

33. Which of the following best describes the activity that involves collecting information used for monitoring and reviewing purposes?

Quick Answer: **182**
Detailed Answer: **215**

- ❍ **A.** Auditing
- ❍ **B.** Logging
- ❍ **C.** Baselining
- ❍ **D.** Inspecting

34. Which of the following best describes the unintended consequence of turning on all auditing counters for all objects?

Quick Answer: **182**
Detailed Answer: **215**

- ❍ **A.** Reduced user productivity
- ❍ **B.** Reduced I/O activity on user machines
- ❍ **C.** Reduced administrative overhead
- ❍ **D.** Reduced server performance

35. Which of the following best describes how settings will actually be applied to an object in a group policy?

Quick Answer: **182**
Detailed Answer: **215**

- ❍ **A.** Individually applied to the object and only from the last policy
- ❍ **B.** A combination of all the settings that can affect the object
- ❍ **C.** Only from settings within the domain where the object is located
- ❍ **D.** A combination of only local group policies that affect the object

36. An administrator is attempting to resolve some issue with multiple group policies on several computers. Which of the following tools would be used to script GPO troubleshooting of multiple computers?

Quick Answer: **182**
Detailed Answer: **215**

- ❍ **A.** Gpupdate
- ❍ **B.** Gpresult
- ❍ **C.** Resultant Set of Policy
- ❍ **D.** Group Policy object

Quick Check

37. Which of the following tools is used to review the effects of Group Policy settings on a particular computer?

❍ **A.** Resultant Set of Policy

❍ **B.** Group Policy object

❍ **C.** Gpupdate

❍ **D.** Local Security settings

Quick Answer: **182**
Detailed Answer: **215**

38. An organization is concerned with unusual activity indicating that an intruder is attempting to gain access to the network. Which of the following event categories should be audited?

❍ **A.** Audit success events in the account management

❍ **B.** Success events in the policy change on domain controllers

❍ **C.** Success and failure events in the system events

❍ **D.** Audit success events in the logon event category

Quick Answer: **182**
Detailed Answer: **215**

39. An organization wants a record of when each user logs on to or logs off from any computer. Which of the following event categories should be audited?

❍ **A.** Audit success events in the account management event

❍ **B.** Success events in the policy change on domain controllers

❍ **C.** Success and failure events in the system events

❍ **D.** Audit success events in the logon event category

Quick Answer: **182**
Detailed Answer: **215**

40. An organization wants to verify when users log on to or log off from the domain. Which of the following event categories should be audited?

❍ **A.** Audit success events in the account management event

❍ **B.** Success events in the policy change on domain controllers

❍ **C.** Success events in the account logon on domain controllers

❍ **D.** Audit success events in the logon event category

Quick Answer: **182**
Detailed Answer: **216**

Quick Check

Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities.

1. Which of the following is a software utility that will scan a single machine or a range of IP addresses checking for a response on service connections?

Quick Answer: **182**
Detailed Answer: **216**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

2. Which of the following is a software utility that will scan a range of IP addresses testing for the presence of known weaknesses in software configuration and accessible services?

Quick Answer: **182**
Detailed Answer: **216**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

3. Which of the following is a software utility that is used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications?

Quick Answer: **182**
Detailed Answer: **216**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

4. Which of the following is a software utility that is used to conduct network assessments over a range of IP addresses and compiles a listing of all systems, devices, and hardware present within a network segment?

Quick Answer: **182**
Detailed Answer: **217**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

Quick Check

5. Which of the following best describes the purpose of OVAL?

   ❍ **A.** An abstract description for layered communications and computer network protocol design

   ❍ **B.** A family of standards dealing with local area networks and metropolitan area networks

   ❍ **C.** An international standard setting body composed of representatives from various national standards organizations

   ❍ **D.** An international language for representing vulnerability information allowing the development of vulnerability test tools

Quick Answer: **182**
Detailed Answer: **217**

6. An administrator working in the Department of Homeland Security needs to document standards for the assessment process of systems. Which of the following would be most useful to the administrator?

   ❍ **A.** OVAL

   ❍ **B.** IEEE

   ❍ **C.** ISO

   ❍ **D.** ISSA

Quick Answer: **182**
Detailed Answer: **217**

7. An organization wants to select an assessment tool for creating an inventory of services hosted on networked systems. Which of the following should the organization choose?

   ❍ **A.** Port scanner

   ❍ **B.** Network mapper

   ❍ **C.** Protocol analyzer

   ❍ **D.** Vulnerability scanner

Quick Answer: **182**
Detailed Answer: **217**

8. An organization wants to select an assessment tool that will examine individual protocols and specific endpoints. Which of the following should the organization choose?

   ❍ **A.** Port scanner

   ❍ **B.** Network mapper

   ❍ **C.** Protocol analyzer

   ❍ **D.** Vulnerability scanner

Quick Answer: **182**
Detailed Answer: **217**

Quick Check

9. An organization wants to select an assessment tool for checking particular versions and patch levels of a service. Which of the following should the organization choose?

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

Quick Answer: **182**
Detailed Answer: **218**

10. Which of the following assessment techniques are typically conducted using automated software programs designed to check code, as well as manual human checks, by someone not associated with development?

❍ **A.** Architecture reviews

❍ **B.** Code reviews

❍ **C.** Design reviews

❍ **D.** Attack Surface determination

Quick Answer: **182**
Detailed Answer: **218**

11. Which of the following refers to the amount of running code, services, and user-interaction fields and interfaces?

❍ **A.** Architecture reviews

❍ **B.** Code reviews

❍ **C.** Design reviews

❍ **D.** Attack Surface determination

Quick Answer: **182**
Detailed Answer: **218**

12. Which of the following assessment techniques typically provides the capability to identify faulty components and interaction between various elements?

❍ **A.** Architecture reviews

❍ **B.** Code reviews

❍ **C.** Design reviews

❍ **D.** Attack Surface determination

Quick Answer: **182**
Detailed Answer: **218**

13. When using a password cracker to test mandatory complexity guidelines, which of the following should the password cracker provide?

❍ **A.** The password only

❍ **B.** The password and hash value

❍ **C.** The username and password

❍ **D.** The strength of the password

Quick Answer: **182**
Detailed Answer: **219**

Quick Check

14. An organization wants to select an assessment tool that will report information used to identify single points of failure. Which of the following should the organization choose?

Quick Answer: **182**
Detailed Answer: **219**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

15. Which of the following tools is often referred to as a packet sniffer?

Quick Answer: **182**
Detailed Answer: **219**

❍ **A.** Port scanner

❍ **B.** Network mapper

❍ **C.** Protocol analyzer

❍ **D.** Vulnerability scanner

Objective 3.8: Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.

1. Which of the following is best described as a friendly attack against a network to test the security measures put into place?

Quick Answer: **183**
Detailed Answer: **219**

❍ **A.** Vulnerability assessment

❍ **B.** Penetration test

❍ **C.** Security assessment

❍ **D.** Compliance test

2. Which of the following are the most serious downsides to conducting a penetration test? (Select all correct answers.)

Quick Answer: **183**
Detailed Answer: **220**

❍ **A.** They can cause some disruption to network operations.

❍ **B.** The help desk can be flooded by affected users.

❍ **C.** They can generate false data in IDS systems.

❍ **D.** External users can have difficulty accessing resources.

Quick Check

3. Which of the following is true about inexperienced internal systems administrators performing penetration tests against the organizational network? (Select all correct answers.)

Quick Answer: **183**
Detailed Answer: **220**

- ❍ **A.** It is a safe practice.
- ❍ **B.** It is a bad practice.
- ❍ **C.** It may be a violation of privacy laws.
- ❍ **D.** It does not violate any privacy laws.

4. Which of the following is true about the relationship between vulnerability assessment and penetration testing?

Quick Answer: **183**
Detailed Answer: **220**

- ❍ **A.** They are inversely related.
- ❍ **B.** They are contradictory.
- ❍ **C.** They are separate functions.
- ❍ **D.** They are complementary.

5. Which of the following is the main security risk of penetration testing?

Quick Answer: **183**
Detailed Answer: **220**

- ❍ **A.** It can conceal aggression that is unrelated to the test.
- ❍ **B.** It can affect user connectivity and resource access.
- ❍ **C.** It can disrupt the normal business environment.
- ❍ **D.** It can weaken the network's security level.

6. Which of the following is conducted with the assessor having no information or knowledge about the inner workings of the system or knowledge of the source code?

Quick Answer: **183**
Detailed Answer: **220**

- ❍ **A.** Black box
- ❍ **B.** White box
- ❍ **C.** Gray box
- ❍ **D.** Green box

7. In which of the following types of testing would a developer test if programming constructs are placed correctly and carry out the required actions?

Quick Answer: **183**
Detailed Answer: **220**

- ❍ **A.** Black box
- ❍ **B.** White box
- ❍ **C.** Gray box
- ❍ **D.** Green box

Quick Check

8. An organization wants to select an assessment tool that will create graphical details suitable for reporting on network configurations. Which of the following should the organization choose?

   ❍ **A.** Port scanner

   ❍ **B.** Network mapper

   ❍ **C.** Protocol analyzer

   ❍ **D.** Vulnerability scanner

Quick Answer: **183**
Detailed Answer: **221**

9. An organization wants to select an assessment tool that will directly test user logon password strength. Which of the following should the organization choose?

   ❍ **A.** Password Locker

   ❍ **B.** Password generator

   ❍ **C.** Password cracker

   ❍ **D.** Password keychain

Quick Answer: **183**
Detailed Answer: **221**

10. Which of the following best describes the difference between a port scanner and a vulnerability scanner?

   ❍ **A.** Port scanners test only for the availability of services; vulnerability scanners check for a particular version or patch level of a service.

   ❍ **B.** Port scanners compile a listing of all hardware present within a network segment; vulnerability scanners check for the availability of services.

   ❍ **C.** Vulnerability scanners test only for the availability of services; port scanners check for a particular version or patch level of a service.

   ❍ **D.** Vulnerability scanners compile a listing of all hardware present within a network segment; port scanners test for the availability of services.

Quick Answer: **183**
Detailed Answer: **221**

Quick-Check Answer Key

Objective 3.1: Analyze and differentiate among types of malware.

1. A
2. C
3. A
4. B
5. C
6. B
7. A
8. C
9. A, B, C
10. A
11. D
12. C
13. A
14. D
15. B
16. A
17. B
18. A
19. A, B, D
20. A, C
21. C
22. D
23. B
24. A
25. B
26. C
27. B
28. A, C, D
29. D
30. C
31. B
32. A, B, C
33. A, C
34. B, C, D
35. D
36. A
37. B
38. A
39. C
40. A, C, D

Objective 3.2: Analyze and differentiate among types of attacks.

1. C
2. A, B
3. C
4. A
5. B
6. D
7. D
8. B
9. C
10. A, B, D
11. A
12. B
13. D
14. C
15. B
16. D
17. B, C, D
18. B
19. C, D
20. A, B
21. A, C, D
22. A, D
23. C
24. D
25. B
26. C
27. C
28. A
29. D
30. B

31. D
32. C
33. C
34. A
35. A
36. D
37. B, C
38. D
39. A
40. B
41. D
42. C
43. B
44. D
45. B

Objective 3.3: Analyze and differentiate among types of social engineering attacks.

1. B
2. C
3. B
4. A
5. D
6. D
7. B
8. A
9. C
10. D

Objective 3.4: Analyze and differentiate among types of wireless attacks.

1. B
2. D
3. C
4. A, B, C
5. C
6. D
7. A
8. C
9. B
10. C
11. A
12. D
13. B
14. A
15. B
16. C
17. A
18. B
19. D
20. A

Objective 3.5: Analyze and differentiate among types of application attacks.

1. A, D
2. C
3. B
4. B, C
5. A
6. C
7. B
8. D
9. A
10. D
11. B
12. A
13. B
14. B, C
15. A, D
16. B, C
17. A
18. A, B, C

19. A, C

20. D

21. B

22. A

23. B

24. A, C

25. C

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques.

1. B

2. C

3. B, C

4. A

5. C

6. D

7. A

8. A, B, D

9. A

10. B

11. A, B, D

12. D

13. C

14. A

15. D

16. B, C

17. C

18. D

19. C

20. A, B, D

21. D

22. D

23. B, C

24. B

25. C

26. A, C, D

27. B

28. C

29. A, B

30. B, C

31. D

32. C

33. B

34. D

35. B

36. B

37. A

38. C

39. D

40. C

Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities.

1. A

2. D

3. C

4. B

5. D

6. A

7. A

8. C

9. D

10. B

11. D

12. A

13. D

14. B

15. C

Objective 3.8: Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.

1. B
2. A, C
3. B, C
4. D
5. A
6. A
7. B
8. B
9. C
10. A

Answers and Explanations

Objective 3.1: Analyze and differentiate among types of malware.

1. **Answer: A.** Perhaps the most popular method of privilege escalation is a buffer overflow attack. Buffer overflows cause disruption of service and lost data. This condition occurs when the data presented to an application or service exceeds the storage-space allocation that has been reserved in memory for that application or service. Answer B is incorrect because programs disguised as useful applications are Trojans. Trojans do not replicate themselves like viruses, but they can be just as destructive. Code is hidden inside the application that can attack your system directly or allow the system to be compromised by the code's originator. The Trojan is typically hidden, so its ability to spread depends on the popularity of the software (such as a game) and a user's willingness to download and install the software. Answer C is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer D is incorrect because spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user.

2. **Answer: C.** A program or piece of code that runs on your computer without your knowledge is a virus. It is designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer A is incorrect. Buffer overflows cause disruption of service and lost data. This condition occurs when the data presented to an application or service exceeds the storage-space allocation that has been reserved in memory for that application or service. Answer B is incorrect because programs disguised as useful applications are Trojans. Trojans do not replicate themselves like viruses, but they can be just as destructive. Code is hidden inside the application that can attack your system directly or allow the system to be compromised by the code's originator. The Trojan is typically hidden, so its ability to spread depends on the popularity of the software and a user's willingness to download and install the software. Answer D is incorrect because spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user.

3. **Answer: A.** A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer B is incorrect because it describes IP spoofing. Answer C is incorrect because it describes spyware. Answer D is incorrect because it describes a worm. Worms are similar in function and behavior to a virus with the exception that worms are self-replicating.

4. **Answer: B.** A rootkit is a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights. Answer A is incorrect because spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer C is incorrect. A bot provides a spam or virus originator with the venue to propagate. Many computers compromised in this way are unprotected home computers (although recently it has become known that many computers in the corporate world are bots, too). A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer D is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited.

5. **Answer: C.** Code Red is an exploit used to spread a worm. This threat affected only web servers running Microsoft's Internet Information Server. Answers A, B, and D are incorrect; Melissa, Acid Rain, and Mocmex are not worms. Melissa is a virus. Acid Rain and Mocmex are Trojans.

6. **Answer: B.** A logic bomb is a virus or Trojan horse that is built to go off when a certain event occurs or a period of time goes by. Answers A and D are incorrect because a specified time element is not involved. Answer C is incorrect because spoofing involves modifying the source address of traffic or the source of information.

7. **Answer: A.** Spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer B is incorrect because a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights is a rootkit. Answer C is incorrect because a large number of computers that forward transmissions to other computers on the Internet, allowing the originator a venue to propagate, is a botnet. Answer D is incorrect because a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection is adware. It reports data to the company, such as your surfing habits and which sites you have visited.

8. **Answer: C.** Requesting to be removed from junk email lists often results in more spam because it verifies that you have a legitimate, working email address. Therefore answers A, B, and D are incorrect.

9. **Answer: A, B, C.** Email spam lists are often created by scanning newsgroup postings, stealing Internet mailing lists, or searching the Web for addresses. Spammers use automated tools to subscribe to as many mailing lists as possible. From those lists, they capture addresses or use the mailing list as a direct target for their attacks. Answer D is incorrect because email spam lists are not created in this manner.

10. **Answer: A.** Perhaps the most popular method of privilege escalation is a buffer overflow attack. Buffer overflows cause disruption of service and lost data. This condition occurs when the data presented to an application or service exceeds the storage-space allocation that has been reserved in memory for that application or service. Answer B is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer C is incorrect. A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer D is incorrect. A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by.

11. **Answer: D.** Worms are similar in function and behavior to a virus with the exception that worms are self-replicating. A worm is built to take advantage of a security hole in an existing application or operating system and then find other systems running the same software and automatically replicate itself to the new host. Answer A is incorrect. Spyware is associated with behaviors such as collecting personal information or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer B is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer C is incorrect. A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed.

12. **Answer: C.** A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer A is incorrect. Spyware is associated with behaviors such as collecting personal information or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer B is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer D is incorrect. Worms are similar in function and behavior to a virus with the exception that worms are self-replicating. A worm is built to take advantage of a security hole in an existing application or operating system and then find other systems running the same software and automatically replicate itself to the new host.

13. **Answer: A.** Spyware is associated with behaviors such as collecting personal information or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer B is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer C is incorrect. A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer D is incorrect. Worms are similar in function and behavior to a virus with the exception that worms are self-replicating. A worm is

built to take advantage of a security hole in an existing application or operating system and then find other systems running the same software and automatically replicate itself to the new host.

14. **Answer: D.** A rootkit is a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights. Answer A is incorrect. Spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent. Basically, spyware is software that communicates information from a user's system to another party without notifying the user. Answer B is incorrect. Spam is a term that refers to the sending of unsolicited commercial email. Email spam targets individual users with direct mail messages. Answer C is incorrect because adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection.

15. **Answer: B.** A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer A is incorrect. A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer C is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited. Answer D is incorrect. A rootkit is a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights.

16. **Answer: A.** Many spyware-eliminator programs are available. These programs scan your machine, similarly to how antivirus software scans for viruses; just as with antivirus software, you should keep spyware-eliminator programs updated and regularly run scans. Therefore, answer D is incorrect. Answers B and C are incorrect because antispyware programs cannot detect rootkits or botnets.

17. **Answer: B.** The main issue with botnets is that they are securely hidden. This allows the botnet masters to perform tasks, gather information, and commit crimes while remaining undetected. Answers A, C, and D are concerns, but the main security concern it is they can remain undetected.

18. **Answer: A.** A logic bomb is also referred to as slag code. It is malicious in intent, and usually planted by a disgruntled employee. Answer B is incorrect. A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer C is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited. Answer D is incorrect. A rootkit is a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights.

19. **Answer: A, B, D.** A buffer overflow can result in the overwriting of data or memory storage, a denial of service due to overloading the input buffer's ability to cope with

the additional data, or the originator can execute arbitrary code, often at a privileged level. Answer C is incorrect because a buffer overflow is targeted toward an individual machine.

20. **Answer: A, C.** There are several types of viruses, including boot sector, polymorphic, macro, program, stealth, and multipartite. Answers B and D are incorrect because they do not describe types of viruses.

21. **Answer: C.** A boot sector virus is placed into the first sector of the hard drive so that when the computer boots, the virus loads into memory. Answer A is incorrect because it describes a polymorphic virus. Answer B is incorrect because it describes a stealth virus. Answer D is incorrect because it describes a program virus.

22. **Answer: D.** A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer A is incorrect because a popular method of privilege escalation is a buffer-overflow attack. Answer B is incorrect because most rootkits use global hooks for stealth activity. Answer C is incorrect because a honeynet is used for monitoring large networks.

23. **Answer: B.** A Trojan horse appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer A is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer C is incorrect because spam is a term that refers to the sending of unsolicited commercial email. Email spam targets individual users with direct mail messages. Answer D is incorrect. Worms are similar in function and behavior to a virus with the exception that worms are self-replicating. A worm is built to take advantage of a security hole in an existing application or operating system, find other systems running the same software, and automatically replicate itself to the new host.

24. **Answer: A.** Most rootkits use global hooks for stealth activity. So, if you use security tools that can prevent programs from installing global hooks and stop process injection, you can prevent rootkit functioning. Answer B is incorrect because adware uses tracking software. Answer C is incorrect because privilege escalation is associated with buffer overflows. Answer D is incorrect because social engineering is taking advantage of human nature.

25. **Answer: B.** Rootkit functionality requires full administrator rights. Therefore, you can avoid rootkit infection by running Windows from an account with lesser privileges. Answer A is incorrect; it describes an effective way to deal with spam. Answer C is incorrect; it describes an effective way to deal with user account exploitation. Answer D is incorrect because it describes an effective way to deal with spyware.

26. **Answer: C.** A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer A is incorrect because it describes a logic bomb. Answer B is incorrect because it describes Trojans. Answer D is incorrect because it describes a buffer overflow.

27. **Answer: B.** Privilege escalation takes advantage of a program's flawed code, which then crashes the system and leaves it in a state where arbitrary code can be executed or an intruder can function as an administrator. Answer A is incorrect because a logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer C is incorrect; spam is a term that refers to the sending of unsolicited commercial email. Email spam targets individual users with direct mail messages. Answer D is incorrect; Trojans are programs disguised as useful applications.

28. **Answer: A, C, D.** Currently, the most effective way to prevent an attacker from exploiting software is to keep the manufacturer's latest patches and service packs applied and to monitor the Web for newly discovered vulnerabilities. Answer B is incorrect because it not feasible to disconnect the network from the Internet.

29. **Answer: D.** A multipartite virus is a hybrid of boot and program viruses. It first attacks a boot sector and then attacks system files or vice versa. Answer A is incorrect because a polymorphic virus can change each time it is executed. It was developed to avoid detection by antivirus software. Answer B is incorrect because a macro virus is inserted into a Microsoft Office document and emailed to unsuspecting users. Answer C is incorrect because a stealth virus uses techniques to avoid detection, such as temporarily removing itself from an infected file or masking a file's size.

30. **Answer: C.** Worms are similar in function and behavior to a virus with the exception that worms are self-replicating. A worm is built to take advantage of a security hole in an existing application or operating system, find other systems running the same software, and automatically replicate itself to the new host. Answer A is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer B is incorrect because a Trojan appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer D is incorrect because a logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by.

31. **Answer: B.** Trojans are programs disguised as useful applications. Trojans do not replicate themselves like viruses, but they can be just as destructive. Code hidden inside the application can attack your system directly or allow the system to be compromised by the code's originator. The Trojan is typically hidden, so its ability to spread depends on the popularity of the software and a user's willingness to download and install the software. Answer A is incorrect because Trojans can perform actions without the user's knowledge or consent, such as collecting and sending data or causing the computer to malfunction. Answers C and D are incorrect; a virus is a program or piece of code that runs on your computer without your knowledge. It is designed to attach itself to other code and replicate.

32. **Answer: A, B, C.** Indications that a computer may contain spyware include the following: the system is slow, (especially when browsing the Internet), it takes a long time for the Windows desktop to come up, clicking a link does nothing or goes to an unexpected website, the browser home page changes (and you might not be able to reset it), and web pages are automatically added to your favorites list. Answer D is incorrect because it describes spam.

33. **Answer: A, C.** When dealing with spam, the user should delete the email without opening it and turn off the preview function of the mail software. Answer B is incorrect because this is an inappropriate action. There are specific laws that deal with spamming, and trying to conduct your own investigation can be dangerous. Answer D is incorrect because local law enforcement does not investigate a single spam incident.

34. **Answer: B, C, D.** Rootkits can be included as part of a software package and can be installed by way of an unpatched vulnerability or by the user downloading and installing it. Answer A is incorrect because accessing documents on the local intranet should not result in a rootkit installation.

35. **Answer: D.** Rootkits have also been known to use encryption to protect outbound communications and piggyback on commonly used ports to communicate without interrupting other applications that use that port. Answer A is incorrect. A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer B is incorrect. A botnet is a large number of computers that forward transmissions to other computers on the Internet. You may also hear a botnet referred to as a zombie army. Answer C is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited.

36. **Answer: A.** A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer B is incorrect. A botnet is a large number of computers that forward transmissions to other computers. Answer C is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited. Answer D is incorrect. A rootkit is a piece of software that can be installed and hidden on a computer, mainly for the purpose of compromising the system and getting escalated privileges such as administrative rights.

37. **Answer: B.** A Trojan appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed. Answer A is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. Answer C is incorrect because a worm is built to take advantage of a security hole in an existing application or operating system and then find other systems running the same software and automatically replicate itself to the new host. Answer D is incorrect because a logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by.

38. **Answer: A.** A polymorphic virus can change each time it is executed. It was developed to avoid detection by antivirus software. Answer B is incorrect because a macro virus is inserted into a Microsoft Office document and emailed to unsuspecting users. Answer C is incorrect because a stealth virus uses techniques to avoid detection, such as temporarily removing itself from an infected file or masking a file’s size. Answer D is incorrect because a multipartite virus is a hybrid of boot and program viruses. It first attacks a boot sector and then attacks system files, or vice versa.

39. **Answer: C.** A bot, short for robot, is an automated computer program that needs no user interaction. Bots are systems that outside sources can control. A bot provides a spam or virus originator with the venue to propagate. Answer A is incorrect because a logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer B is incorrect. Adware is a form of advertising that installs additional tracking software on your system that keeps in contact with the company through your Internet connection. It reports data to the company, such as your surfing habits and which sites you have visited. Answer D is incorrect because a virus is a program or piece of code designed to attach itself to other code and replicate.

40. **Answer: A, C, D.** You can take steps to protect your network from malicious code, such as not using any type of removable media from another user without first scanning for malware, performing backups on a daily basis, installing firewalls or intrusion-prevention systems on client machines, and subscribing to newsgroups and checking antivirus websites regularly. Answer B is incorrect. Opening all attachments will mostly likely infect a machine.

Objective 3.2: Analyze and differentiate among types of attacks.

1. **Answer: C.** Telnet uses port 23. Answer A is incorrect because port 110 is used for POP3 incoming mail. Answer B is incorrect because port 21 is used for FTP. Port 443 is used by HTTPS; therefore, answer D is incorrect.

2. **Answer: A, B.** UDP ports 161 and 162 are used by SNMP. Answer C is incorrect because port 443 is used by HTTPS. Answer D is incorrect because port 4445 uses TCP/UDP for service type upnotifyp.

3. **Answer: C.** TCP/IP hijacking is the term used when an attacker takes control of a session between the server and a client. This can occur due to the TCP three-way handshake. The three-way handshake is the method used to establish and tear down network connections. Answer A is incorrect because it describes spoofing. Spoofing is a method of providing false identity information to gain unauthorized access. Answer B is incorrect because it describes a null session. A null session is a connection without specifying a username or password. Answer D is incorrect because it describes DNS poisoning. DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain, thus permitting attackers to send legitimate traffic anywhere they choose.

4. **Answer: A.** Spoofing is a method of providing false identity information to gain unauthorized access. Answer B is incorrect because it describes a null session. A null session is a connection without specifying a username or password. Answer C is incorrect because it describes TCP/IP hijacking. TCP/IP hijacking is the term used when an attacker takes control of a session between the server and a client. Answer D is incorrect because it describes DNS poisoning. DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain, thus permitting attackers to send legitimate traffic anywhere they choose.

5. **Answer: B.** A null session is a connection without specifying a username or password. Answer A is incorrect because it describes spoofing. Spoofing is a method of providing false identity information to gain unauthorized access. Answer C is incorrect because it describes TCP/IP hijacking. TCP/IP hijacking is the term used when an attacker takes control of a session between the server and a client. Answer D is incorrect because it describes DNS poisoning. DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain, thus permitting attackers to send legitimate traffic anywhere they choose.

6. **Answer: D.** DNS poisoning allows a perpetrator to redirect traffic by changing the IP record for a specific domain. Query results that are forged and returned to the requesting client or recursive DNS query can poison the DNS records, thus permitting attackers to send legitimate traffic anywhere they choose. Answer A is incorrect because it describes spoofing. Spoofing is a method of providing false identity information to gain unauthorized access. Answer B is incorrect because it describes a null session. A null session is a connection without specifying a username or password. Answer C is incorrect because it describes TCP/IP hijacking. TCP/IP hijacking is the term used when an attacker takes control of a session between the server and a client.

7. **Answer: D.** The man-in-the-middle attack takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other. Answer A is incorrect; it describes DNS kiting. DNS kiting refers to the practice of taking advantage of the add/grace period (AGP) to monopolize domain names without ever paying for them. Answer B is incorrect; it describes a replay attack. In a replay attack, packets are captured by using sniffers. After the pertinent information is extracted, the packets are placed back on the network. Answer C is incorrect; it describes a denial-of-service attack. The purpose of a DoS attack is to disrupt the resources or services that a user would expect to have access to.

8. **Answer: B.** In a replay attack, packets are captured by using sniffers. After the pertinent information is extracted, the packets are placed back on the network. Answer A is incorrect; it describes DNS kiting. DNS kiting refers to the practice of taking advantage of the AGP to monopolize domain names without ever paying for them. Answer C is incorrect; it describes a denial-of-service attack. The purpose of a DoS attack is to disrupt the resources or services that a user would expect to have access to. Answer D is incorrect; it describes a man-in-the-middle attack. The man-in-the-middle attack takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

9. **Answer: C.** The purpose of a distributed denial of service (DDoS) attack is to disrupt the resources or services that a user would expect to have access to. Answer A is incorrect; it describes DNS kiting. DNS kiting refers to the practice of taking advantage of the AGP to monopolize domain names without ever paying for them. Answer B is incorrect; it describes a replay attack. In a replay attack, packets are captured by using sniffers. After the pertinent information is extracted, the packets are placed back on the network. Answer D is incorrect; it describes a man-in-the-middle attack. The man-in-the-middle attack takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other.

10. **Answer: A, B, D.** To help protect your network, you can set up filters on external routers to drop packets involved in these types of attacks. You should also set up

another filter that denies traffic originating from the Internet that shows an internal network address. If the operating system allows it, reduce the amount of time before the reset of an unfinished TCP connection. Doing so makes it harder to keep resources unavailable for extended periods of time. Answer C is incorrect; increasing the amount of time before the reset of an unfinished TCP connection makes the resources unavailable for a longer period of time.

11. **Answer: A.** Because ARP does not require any type of validation, as ARP requests are sent, the requesting devices believe that the incoming ARP replies are from the correct devices. This can allow a perpetrator to trick a device into thinking any IP is related to any MAC address. Answer B is incorrect because it describes DNS poisoning. Answer C is incorrect. A Teardrop attack sends fragmented UDP packets. Answer D is incorrect. In a DDoS attack, the attackers distribute zombie software that allows the attacker partial or full control of the infected computer system.

12. **Answer: B.** A null session is a connection without specifying a username or password. Null sessions are a possible security risk because the connection is not really authenticated. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. Answer C is incorrect because ARP poisoning allows a perpetrator to trick a device into thinking that an incorrect IP address is related to a MAC address. The implementation of the ARP protocol is simple. The receipt of an ARP reply at any time causes the receiving computer to add the newly received information to its ARP cache without any type of verification. Answer D is incorrect because domain kiting refers to the practice of taking advantage of this AGP period to monopolize domain names without ever paying for them.

13. **Answer: D.** A denial-of-service (DoS) attack that attempts to block service or reduce activity on a host by sending ping requests directly to the victim using ICMP is called a ping flood. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. Answer C is incorrect because a man-in-the middle attack is commonly used to gather information in transit between two hosts. Answer B is incorrect because the purpose of a DoS attack is to disrupt the resources or services that a user would expect to have access to.

14. **Answer: C.** A man-in-the-middle attack is commonly used to gather information in transit between two hosts. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. ARP poisoning allows a perpetrator to trick a device into thinking any IP is related to any MAC address; therefore, Answer B is incorrect. Because the purpose of a DoS attack is to deny use of resources or services to legitimate users, answer D is incorrect.

15. **Answer: B.** A null session is a connection without specifying a username or password. Null sessions are a possible security risk because the connection is not really authenticated. Answer A is incorrect because the session is not abnormally terminated. Although answer C may be a concern, it is not the primary issue. Answer D is incorrect because null sessions are direct connections and are not remote controlled.

16. **Answer: D.** The most effective way to reduce null session vulnerability is by disabling NetBIOS over TCP/IP. Editing the Registry to restrict anonymous access is another method used to control null session access. After you have done this, verify that ports 139 and 445 are closed. Answer A is incorrect; reducing the amount of time before the

reset of an unfinished TCP connection deals with DoS attacks. Answers B and C are incorrect; using the signing capabilities of certificates and denying traffic originating from the Internet that shows an internal network address are protective measures against spoofing.

17. **Answer: B, C, D.** To mitigate the effects of spoofing, you should set up a filter that denies traffic originating from the Internet that shows an internal network address. Using the signing capabilities of certificates on servers and clients allows web and email services to be more secure. The use of IPsec can secure transmissions between critical servers and clients. Answer A is incorrect because editing the Registry to restrict anonymous access is a method used to control null session access.

18. **Answer: B.** Forcing a user to reauthenticate before allowing transactions to occur could help prevent this type of attack. Protection mechanisms include the use of unique initial sequence numbers (ISNs) and web session cookies. Answer A is incorrect because to mitigate the effects of spoofing, you should set up a filter that denies traffic originating from the Internet that shows an internal network address. Answers C and D are incorrect; to mitigate the vulnerability of DDoS attacks, reduce the amount of time before the reset of an unfinished TCP connection and set up filters on external routers.

19. **Answer: C, D.** The most effective way to reduce null session vulnerability is by disabling NetBIOS over TCP/IP. After you have done this, verify that ports 139 and 445 are closed. Answers A and B are incorrect; Simple Network Management Protocol (SNMP) is often overlooked when checking for vulnerabilities because it uses User Datagram Protocol (UDP) ports 161 and 162.

20. **Answer: A, B.** The man-in-the-middle attack takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other. This attack is common in Telnet and wireless technologies. Answer C is incorrect because email is susceptible to spoofing not hijacking. Answer D is incorrect. Samba provides file and print services to SMB/CIFS clients for Linux-based operating systems.

21. **Answer: A, C, D.** To minimize the effects of DNS poisoning, check the DNS setup if you are hosting your own DNS. Be sure the DNS server is not open-recursive. An open-recursive DNS server responds to any lookup request, without checking where it originates. Disable recursive access for other networks to resolve names that are not in your zone files. You can also use different servers for authoritative and recursive lookups and require that caches discard information except from the .com servers and the root servers. Answer B is incorrect because it describes an effective way to deal with rootkits.

22. **Answer: A, D.** ARP poisoning is limited to attacks that are locally based, so an intruder needs either physical access to your network or control of a device on your local network. To mitigate ARP poisoning on a small network, you can use static or script-based mapping for IP addresses and ARP tables. For large networks, use equipment that offers port security. Answers B and C are incorrect; they are solutions for small networks, not large networks.

23. **Answer: C.** Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. An example of the latter would be if User A could read User B's email without specific authorization. Answer A is incorrect because it describes default accounts. Answer B is incorrect because data transmitted over a wireless network using 802.1x that can be easily "sniffed" is referred to as data emanations. Answer D is incorrect because a back door is an application code function, created intentionally or unintentionally, which allows unauthorized access to networked resources.

24. **Answer: D.** A back door is an application code function, created intentionally or unintentionally, which allows unauthorized access to networked resources. Answer A is incorrect because it describes default accounts. Answer B is incorrect because data transmitted over a wireless network using 802.1x that can be easily "sniffed" is referred to as data emanations. Answer C is incorrect. Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. An example of the latter would be if User A could read User B's email without specific authorization.

25. **Answer: B.** Unlike resources located on the local system, network resources are much more vulnerable to DoS attacks. These attacks attempt to block access to resources by overwhelming network availability, instead of attempting to directly access the resources through unauthorized means. By blocking access to a website or network resource, the attacker effectively prevents authorized availability. Answer A is incorrect because a DoS focuses on network resources, not local resources. Answer C is incorrect; viruses and worms ranked the highest for sheer number of attacks against network storage. Answer D is incorrect; DoS attacks are launched against servers in the DMZ, not the internal network, unless there is not a DMZ in place. However, corporate networks usually have some type of segmentation keeping the internal network and DMZ separated, making this answer choice incorrect.

26. **Answer: C.** Unlike resources located on the local system, network resources are much more vulnerable to DoS attacks. These attacks attempt to block access to resources by overwhelming network availability, instead of attempting to directly access the resources through unauthorized means. By blocking access to a website or network resource, the attacker effectively prevents authorized availability. Answer A is incorrect because privilege escalation is the intentional access to resources not intended for access by the user. Answer B is incorrect; a back door is an application code function, created intentionally or unintentionally, which allows unauthorized access to networked resources. Answer D is incorrect; attempting to directly access the resources through unauthorized means would fall along the lines of a spoofing attack.

27. **Answer: C.** Many networking devices and services are initially installed with a default set of user credentials, such as Oracle's Scott/Tiger and IBM's qsecofr/qsecofr. Unless these credentials are removed and replaced with unique strong logon credentials, they present an avenue for network attack because they are known to potential attackers. Answer A is incorrect because replacing them on an as-needed basis is not proper

policy. Answer B is incorrect; replacing them when an attack has been detected is reactive instead of proactive. Answer D is incorrect because using the same logon credential for all devices and services leaves them all vulnerable should the password be compromised.

28. **Answer: A.** Back doors are application code functions created intentionally or unintentionally that enable unauthorized access to networked resources. Many times during application development, software designers put in shortcut entry points to allow rapid code evaluation and testing. If not removed before application deployment, such entry points can present the means for an attacker to gain unauthorized access later. Other back doors may be inserted by the application designers purposefully, presenting later threats to the network if applications are never reviewed by another application designer before deployment. Answer B is incorrect because back doors are associated with code development, not system certification. Answer C is incorrect because during user interface testing, the users do not have access to the code and cannot create back doors. Answer D is incorrect because the code has already been developed and tested during the implementation phase. At this point, there is not access to the code itself.

29. **Answer: D.** To optimize network layout within each unique location, a site survey is necessary before implementing any WLAN solution. This is particularly important in distributed wireless network configurations spanning multiple buildings or open natural areas, where imposing structures and tree growth may affect network access in key areas. Answers A, B, and C are incorrect. Land surveys, building inspections, and OSHA inspections are agency-related functions and cannot be conducted by the organization.

30. **Answer: B.** Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. Answer A is incorrect because it describes the vulnerability of a broadcast packet sniffer readily identifying a WAP. Answer C is incorrect. Back doors represent application code functions, created intentionally or unintentionally, which allow unauthorized access to networked resources. Answer D is incorrect because automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity, derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details.

31. **Answer: D.** Automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity, derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details. Answer A is incorrect because it describes the vulnerability of a broadcast packet sniffer readily identifying a WAP. Answer B is incorrect. Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. Answer C is incorrect. Back doors represent application code functions, created intentionally or unintentionally, which allow unauthorized access to networked resources.

32. **Answer: C.** Back doors represent application code functions, created intentionally or unintentionally, which allow unauthorized access to networked resources. Many times during application development, software designers put in shortcut entry points to allow rapid code evaluation and testing. If not removed before application deployment, such entry points can present the means for an attacker to gain unauthorized access later. Answer A is incorrect because it describes the vulnerability of a broadcast packet sniffer readily identifying a WAP. Answer B is incorrect. Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. Answer D is incorrect because automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity, derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details.

33. **Answer: C.** Many networking devices and services are initially installed with a default set of user credentials, such as Oracle's Scott/Tiger and IBM's qsecofr/qsecofr. Unless these credentials are removed and replaced with unique strong logon credentials, they present an avenue for network attack. Answer A is incorrect. Network resources are much more vulnerable to DoS attacks. These attacks attempt to block access to resources by overwhelming network availability, instead of attempting to directly access the resources through unauthorized means. Answer B is incorrect. Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. Answer D is incorrect because automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity, derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details.

34. **Answer: A.** Network resources are much more vulnerable to DoS attacks. These attacks attempt to block access to resources by overwhelming network availability, instead of attempting to directly access the resources through unauthorized means. Answer B is incorrect. Privilege escalation is a vulnerability represented by the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. Answer C is incorrect. Many networking devices and services are initially installed with a default set of user credentials. Unless these credentials are removed and replaced with unique strong logon credentials, they present an avenue for network attack. Answer D is incorrect because automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity, derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details.

35. **Answer: A.** Privilege escalation represents the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access

features of an application reserved for other users. An example of the latter is if User A can read User B's email without specific authorization. Answer B is incorrect. Many networking devices and services are initially installed with a default set of user credentials. Unless these credentials are removed and replaced with unique strong logon credentials, they present an avenue for network attack. Answer C is incorrect. Any resource exposed on a network may be attacked to gain unauthorized access. The most common form of authentication and user access control is the username/password combination, which can be significantly weakened as a security measure if a "weak" password is selected. Answer D is incorrect. Back doors are application code functions, created intentionally or unintentionally, that enable unauthorized access to networked resources. Many times during application development, software designers put in shortcut entry points to allow rapid code evaluation and testing. If not removed before application deployment, such entry points can present the means for an attacker to gain unauthorized access later.

36. **Answer: D.** Back doors are application code functions, created intentionally or unintentionally, that enable unauthorized access to networked resources. Many times during application development, software designers put in shortcut entry points to allow rapid code evaluation and testing. If not removed before application deployment, such entry points can present the means for an attacker to gain unauthorized access later. Answer A is incorrect. Privilege escalation represents the accidental or intentional access to resources not intended for access by the user. Application flaws can allow a normal user access to administrative functions reserved for privileged accounts, or to access features of an application reserved for other users. An example of the latter is if User A can read User B's email without specific authorization. Answer B is incorrect. Many networking devices and services are initially installed with a default set of user credentials. Unless these credentials are removed and replaced with unique strong logon credentials, they present an avenue for network attack. Answer C is incorrect. Any resource exposed on a network may be attacked to gain unauthorized access. The most common form of authentication and user access control is the username/password combination, which can be significantly weakened as a security measure if a "weak" password is selected.

37. **Answer: B, C.** Automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity (complexity here meaning a mixture of character case, numbers, and symbols), derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details. Answer A is incorrect because it is an attack associated with WAPs announcing their service set identifier (SSID). Answer D is incorrect because DoS attacks are often used for Internet extortion schemes, where an attacking botnet of tens of thousands of zombied client systems can be used to consume all available connections to a business website.

38. **Answer: D.** DoS attacks are often used for Internet extortion schemes, where an attacking botnet of tens of thousands of zombied client systems can be used to consume all available connections to a business website. Many fringe service industries, such as online casinos, are regularly targeted with this type of attack. Answer A is incorrect because it is an attack associated with WAPs announcing their service set identifier (SSID). Answers B and C are incorrect; automated and social-engineering assaults on passwords are easier when a password is short, lacking in complexity

(complexity here meaning a mixture of character case, numbers, and symbols), derived from a common word found in the dictionary, or derived from easily guessable personal information such as birthdays, family names, pet names, and similar details.

39. **Answer: A.** Spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer B is incorrect because Vishing is voice phishing; the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging. Answer D is incorrect because pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning.

40. **Answer: B.** Vishing is voice phishing; the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging. Answer D is incorrect because pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning.

41. **Answer: D.** Pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer B is incorrect because vishing is voice phishing, the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging.

42. **Answer: C.** Smishing, also known as SMS phishing, involves using phishing methods through text messaging. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer B is incorrect because vishing is voice phishing, the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer D is incorrect because pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning.

43. **Answer: B.** Messaging spam, sometimes called SPIM, is a type of spam targeting users of instant messaging (IM) services. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer C is incorrect because spam targets email. Answer D is incorrect because pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning.

44. **Answer: D.** When used as part of scanning a system, the TCP header of Christmas tree packets has the flags SYN, FIN, URG and PSH set. By observing how a host responds to an odd packet, such as a Christmas tree packet, assumptions can be made regarding the host's operating system. Answer A is incorrect because spoofing involves modifying the source address of traffic or source of information. Answer B is incorrect because a null session is a connection without specifying a username or password. Null sessions are a possible security risk because the connection is not really authenticated. Answer C is incorrect because ARP poisoning allows a perpetrator to trick a device into thinking that an incorrect IP address is related to a MAC address. The implementation of the ARP protocol is simple. The receipt of an ARP reply at any time causes the receiving computer to add the newly received information to its ARP cache without any type of verification.

45. **Answer: B.** Transitive access can be achieved by gaining the trust of a computer that is trusted by the target network allowing the bypass of security measures. Answer A is incorrect because packet sniffing targets packets not hosts. Answer C is incorrect; Social-engineering attacks target humans, not computers. Answer D is incorrect. DoS attacks are often used for Internet extortion schemes, where an attacking botnet of tens of thousands of zombied client systems can be used to consume all available connections to a business website.

Objective 3.3: Analyze and differentiate among types of social engineering attacks.

1. **Answer: B.** Social engineering is a process by which an attacker may extract useful information from users who are often just tricked into helping the attacker. Answer A is incorrect because pharming is a hacker's attack aiming to redirect a website's traffic to another, bogus, website. Answer C is incorrect because phishing is an attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic communication, usually email. Answer D is incorrect because shoulder surfing uses direct observation techniques. It gets its name from looking over someone's shoulder to get information.

2. **Answer: C.** Phishing is an attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic communication, usually email. Answer A is incorrect because pharming is a hacker's attack aiming to redirect a website's traffic to another, bogus, website. Answer B is incorrect. Social engineering is a process by which an attacker may extract useful information from users who are often just tricked into helping the attacker. Answer D is incorrect because shoulder surfing uses direct observation techniques. It gets its name from looking over someone's shoulder.

3. **Answer: B.** Hoax messages may warn of emerging threats that do not exist. They might instruct users to delete certain files to ensure their security against a new virus, while actually only rendering the system more susceptible to later viral agents. Answer A is incorrect because pharming is a hacker's attack aiming to redirect a website's traffic to another, bogus, website. Answer C is incorrect because phishing is an attempt to acquire sensitive information by masquerading as a trustworthy entity via an electronic

communication, usually email. Answer D is incorrect because spam is unwanted email communication.

4. **Answer: A.** Although hoaxes present issues such as loss of functionality or security vulnerabilities, they also use system resources and consume users' time. This results in lost productivity and an undue burden on the organization's resources, especially if many employees respond. Answer B is incorrect; although virus may be a concern, the idea behind a chain letter is to occupy time and resources. Answer C is incorrect because hoaxes try to occupy time and resources, not garner proprietary information. Answer D is incorrect because this statement is simply not true.

5. **Answer: D.** Shoulder surfing uses direct observation techniques. It gets its name from looking over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places such as airports, conventions, or coffee shops because it's relatively easy to stand next to someone and watch as the person enters a PIN or a password. Answer A is incorrect; virus infection is a concern. However, the real danger is the organizational information that is readily accessible. Answer B is incorrect because social engineering is a process by which an attacker may extract useful information from users who are often tricked into helping the attacker. Answer C is incorrect because dumpster diving is scavenging through discarded equipment and documents and extracting sensitive information from it without ever contacting anyone in the company.

6. **Answer: D.** Whaling is identical to spear phishing except for the "size of the fish." Whaling employs spear phishing tactics, but is intended to go after high-profile targets such as an executive within a company. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer B is incorrect because vishing is voice phishing; the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging.

7. **Answer: B.** Vishing is voice phishing; the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer A is incorrect because spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging. Answer D is incorrect because whaling is identical to spear phishing except for the "size of the fish." Whaling employs spear phishing tactics, but is intended to go after high-profile targets such as an executive within a company.

8. **Answer: A.** Spear phishing is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual or groups of individuals. Answer B is incorrect because vishing is voice phishing; the attacker will often use a fake caller-ID to appear as a trusted organization and attempt to get the individual to enter account details via the phone. Answer C is incorrect because smishing, also known as SMS phishing, involves using phishing methods through text messaging. Answer D is incorrect. Whaling is identical to spear phishing except for the

"size of the fish." Whaling employs spear phishing tactics, but is intended to go after high-profile targets such as an executive within a company.

9. **Answer: C.** Dumpster diving is scavenging through discarded equipment and documents and extracting sensitive information from it without ever contacting anyone in the company. Answer A is incorrect; virus infection is a technical concern, not a human concern. Answer B is incorrect because social engineering is a process by which an attacker may extract useful information from users who are often tricked into helping the attacker. Answer D is incorrect because shoulder surfing uses direct observation techniques. It gets its name from looking over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places such as airports, conventions, or coffee shops because it's relatively easy to stand next to someone and watch as the person enters a PIN or a password.

10. **Answer: D.** Tailgating refers to the act of tagging along with another person who is authorized in order to gain entry into a restricted area. Answer A is incorrect because pharming redirects victims to a bogus website, even if they correctly entered the intended site. To accomplish this, the attacker employs another attack such as DNS cache poisoning. Answer B is incorrect because dumpster diving is scavenging through discarded equipment and documents and extracting sensitive information from it without ever contacting anyone in the company. Answer C is incorrect because shoulder surfing uses direct observation techniques. It gets its name from looking over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places such as airports, conventions, or coffee shops because it's relatively easy to stand next to someone and watch as the person enters a PIN or a password.

Objective 3.4: Analyze and differentiate among types of wireless attacks.

1. **Answer: B.** Wireless networks often announce their service set identifier (SSID) to allow mobile devices to discover available Wireless Access Points (WAPs). Turning off this broadcast can reduce the vulnerability of a wireless packet sniffer detecting broadcasts that readily identify a WAP. In this particular instance, the WAP is not secure because the SSID is broadcast in plain text whenever a client connects to the network. Answer A is incorrect because WAPs by default do not have encryption enabled. Answer C is incorrect because if physical access is limited, the risk is mitigated. Answer D is incorrect because it describes the characteristics of a hub.

2. **Answer: D.** 802.1x transmissions generate detectable radio-frequency signals in all directions. Persons who want to "sniff" the data transmitted over the network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides. Answer A is incorrect because the radio-frequency signals are generated in all directions, not in one direction. Answers B and C are incorrect because data emanation is what allows for the sniffing of the data, not why data emanation is a risk.

3. **Answer: C.** Without the use of a mandated encryption standard, data transmitted over an 802.1x wireless link may be passed in clear form. Forms of encryption may be implemented, such as Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) and Temporal Key Integrity Protocol (TKIP). Answers A, B, and D are incorrect because authorization, authentication, and identification are access control methods, not methods to mitigate data transmissions.

4. **Answer: A, B, C.** Wireless communications are susceptible to data emanation, weak encryption, session hijacking, man-in-the-middle attacks, and war-driving. Answer D is incorrect because spam relaying is associated with open SMTP relays in email servers.

5. **Answer: C.** Because the authentication mechanism is one-way, it is easy for a hijacker to wait until the authentication cycle is completed and then generate a signal to the client that causes the client to think it has been disconnected from the access point, while at the same time beginning to transmit data traffic pretending to be from the original client. Answers A and D are incorrect. Both of these answers deal with authorization, and session hijacking deals with authentication. Answer B is incorrect because it is not true that an authentication mechanism is not there. It exists and is one-way.

6. **Answer: D.** The request for connection by the client is an omnidirectional open broadcast. It is possible for a hijacker to act as an access point to the client, and as a client to the true network access point, allowing the hijacker to follow all data transactions with the ability to modify, insert, or delete packets at will. Answer A is incorrect because a request for connection by the client is an omnidirectional open broadcast. Answers B and C are incorrect; the connection request is made by the client, not the access point.

7. **Answer: A.** A popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer B is incorrect because it describes war-dialing. Answer C is incorrect because it describes war-chalking. Answer D is incorrect because it describes a hotspot.

8. **Answer: C.** War-chalking utilizes a set of symbols and shorthand details to provide specifics needed to connect using a business access point. This is done by marking buildings, curbs, and other landmarks to indicate the presence of an available access point and its connection details. Answer A is incorrect. A popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer B is incorrect because it describes war-dialing. Answer D is incorrect because it describes a hotspot.

9. **Answer: B.** Mobile devices equipped for Bluetooth short-range wireless connectivity, such as laptops, cell phones, and PDAs, are subject to receiving text and message broadcast spam sent from a nearby Bluetooth-enabled transmitting device in an attack referred to as bluejacking. Answer A is incorrect. A popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer C is incorrect because it describes bluesnarfing. Answer D is incorrect. War-chalking utilizes a set of symbols and shorthand details to provide specifics needed to connect using a business access point. This is done by marking buildings, curbs, and other landmarks to indicate the presence of an available access point and its connection details.

10. **Answer: C.** Although typically benign, attackers use bluejacking to generate messages that appear to be from the device itself. This leads users to follow obvious prompts and establish an open Bluetooth connection to the attacker's device. Once paired with the attacker's device, the user's data becomes available for unauthorized access, modification, or deletion, which is an attack referred to as bluesnarfing. Answer B is incorrect. Mobile devices equipped for Bluetooth short-range wireless connectivity, such as laptops, cell phones, and PDAs, are subject to receiving text and message broadcast spam sent from a nearby Bluetooth-enabled transmitting device in an attack referred to as bluejacking. Answer A is incorrect. A popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. War-chalking utilizes a set of symbols and shorthand details to provide specifics needed to connect using a business access point. This is done by marking buildings, curbs, and other landmarks to indicate the presence of an available access point and its connection details.

11. **Answer: A.** The 802.11 (Wi-Fi) standard uses the CSMA/CA connectivity methods commonly found in Ethernet connectivity. Answers B and D are incorrect because both i-Mode and WAP are standards used by mobile devices such as cell phones, pagers, and PDAs and are not used to specify WLAN standards. Answer C is incorrect because Bluetooth is based on a different transmission protocol.

12. **Answer: D.** Data emanation happens because 802.1x transmissions generate detectable radio-frequency signals in all directions. Persons wanting to sniff the data transmitted over the network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides (such as the popular Pringle's can) and flying devices overhead to increase detection range without interference from building structures. Answer A is incorrect because without the use of a mandated encryption standard, data transacted over an 802.1x wireless link may be passed in clear form, and attackers can take advantage of this weak or nonexistent encryption. Answer B is incorrect because the wireless authentication mechanism is one-way, allowing session hijacking. Answer C is incorrect because a popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving.

13. **Answer: B.** Because the authentication mechanism is one-way, it is easy for a hijacker to wait until the authentication cycle is completed and then generate a signal to the client that causes the client to think it has been disconnected from the access point, while at the same time beginning to transact data traffic pretending to be the original client. Answer A is incorrect because without the use of a mandated encryption standard, data transacted over an 802.1x wireless link may be passed in clear form, and attackers can take advantage of this weak or nonexistent encryption. Answer C is incorrect because a popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. Persons wanting to "sniff" the data transmitted over the wireless network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides (such as the popular Pringle's can) and flying devices overhead to increase detection range without interference from building structures.

14. **Answer: A.** Without the use of a mandated encryption standard, data transacted over an 802.1x wireless link may be passed in clear form, and attackers can take advantage of this weak or nonexistent encryption. Answer B is incorrect because the wireless authentication mechanism is one-way, allowing session hijacking. Answer C is incorrect because a popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. Persons wanting to "sniff" the data transmitted over the wireless network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides (such as the popular Pringle's can) and flying devices overhead to increase detection range without interference from building structures.

15. **Answer: B.** Although typically benign, attackers can use bluejacking to generate messages that appear to be from the device itself, leading users to follow obvious prompts and establish an open Bluetooth connection to the attacker's device. Once paired with the attacker's device, the user's data becomes available for unauthorized access, modification, or deletion, which is a more aggressive attack referred to as bluesnarfing. Answer A is incorrect. Mobile devices equipped for Bluetooth short-range wireless connectivity, such as laptops, cell phones, and PDAs, are subject to receiving text and message broadcast spam sent from a nearby Bluetooth-enabled transmitting device in an attack referred to as bluejacking. Answer C is incorrect. A popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. War-chalking utilizes a set of symbols and shorthand details to provide specifics needed to connect using a business access point. This is done by marking buildings, curbs, and other landmarks to indicate the presence of an available access point and its connection details.

16. **Answer: C.** War-driving is aimed at identification of existing wireless networks, the service set identifier (SSID) used to identify the wireless network, and any known WEP keys. Answer A is incorrect because without the use of a mandated encryption standard, data transacted over an 802.1x wireless link may be passed in clear form and attackers can take advantage of this weak or nonexistent encryption. Answer B is incorrect because the wireless authentication mechanism is one way, allowing session hijacking. Answer D is incorrect. Persons wanting to "sniff" the data transmitted over the wireless network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides (such as the popular Pringle's can) and flying devices overhead to increase detection range without interference from building structures.

17. **Answer: A.** Mobile devices equipped for Bluetooth short-range wireless connectivity, such as laptops, cell phones, and PDAs, are subject to receiving text and message broadcast spam sent from a nearby Bluetooth-enabled transmitting device in an attack referred to as bluejacking. Answer B is incorrect. Although typically benign, attackers can use bluejacking to generate messages that appear to be from the device itself, leading users to follow obvious prompts and establish an open Bluetooth connection to the attacker's device. Once paired with the attacker's device, the user's data becomes available for unauthorized access, modification, or deletion, which is a more aggressive attack referred to as bluesnarfing. Answer C is incorrect. A popular pastime involves driving around with a laptop system configured to listen for open 802.1x

access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. War-chalking utilizes a set of symbols and shorthand details to provide specifics needed to connect using a business access point. This is done by marking buildings, curbs, and other landmarks to indicate the presence of an available access point and its connection details.

18. **Answer: B.** Because the request for connection by the client is an omnidirectional open broadcast, it is possible for a hijacker to act as an access point to the client, and as a client to the true network access point, allowing the hijacker to follow all data transactions with the ability to modify, insert, or delete packets at will. By implementing a rogue AP with stronger signal strength than more remote permanent installations, the attacker can cause a wireless client to preferentially connect to their own stronger nearby connection using the wireless device's standard roaming handoff mechanism. Answer A is incorrect. Without the use of a mandated encryption standard, data transacted over an 802.1x wireless link may be passed in clear form and attackers can take advantage of this weak or nonexistent encryption. Answer C is incorrect because a popular pastime involves driving around with a laptop system configured to listen for open 802.1x access points announcing their SSID broadcasts, which is known as war-driving. Answer D is incorrect. Persons wanting to "sniff" the data transmitted over the wireless network may use many solutions to increase the distance over which detection is possible, including the use of reflective tube waveguides (such as the popular Pringle's can) and flying devices overhead to increase detection range without interference from building structures.

19. **Answer: D.** The Wi-Fi Protected Access (WPA and later WPA2) standards were developed by the Wi-Fi Alliance to replace the WEP protocol while the 802.11i standard was being developed. The WPA includes many of the functions of the 802.11i protocol but relies on the Rivest Cipher 4 (RC4), which is considered vulnerable to keystream attacks. The later WPA2 standard was certified to include the full 802.11i standard after its final approval. Answers A and C are incorrect because they are encryptions standards not associated with the Wi-Fi Alliance. Answer B is incorrect because a WAP refers to both handheld devices as well as wireless access points.

20. **Answer: A.** Wireless Session Layer (WSL) is equivalent to the session layer of the Open Systems Interconnection (OSI) model. Based on this information, answers B, C, and D are incorrect.

Objective 3.5: Analyze and differentiate among types of application attacks.

1. **Answer: A, D.** Some identified vulnerabilities of the Java language include buffer overflows, ability to execute instructions, resource monopolization, and unexpected redirection. Answers B and C are incorrect because unauthorized file upload and email exposure are associated with JavaScript, not the Java language.

2. **Answer: C.** Java applets execute when the client machine's browser loads the hosting web page. Vulnerabilities are based on the Java language. JavaScript vulnerabilities must be addressed based on the operating system and browser version in use on each

client. Answers A and B are incorrect because JavaScript vulnerabilities must be addressed based on the operating system and browser version in use on each client, not the server. Answer D is incorrect because the operating system does not load the hosting web page—an application and browser do.

3. **Answer: B.** Java is a precompiled language. Before it can be executed, it undergoes a Just In Time (JIT) compilation into the necessary binary bytes. A Java-based miniprogram, called an applet, may present many security risks to the client. Applets execute when the client machine's browser loads the hosting web page. Answers A and C are incorrect because Java is a precompiled language. Answer D is incorrect because applets execute when the client machine's browser loads the hosting web page.

4. **Answer: B, C.** JavaScript is a client-side interpreted language that mainly poses privacy-related vulnerability issues such as unauthorized file upload and email exposure. Answers A and D are incorrect because they are associated with the Java language. Some identified vulnerabilities of the Java language include buffer overflows, ability to execute instructions, resource monopolization, and unexpected redirection.

5. **Answer: A.** To avoid vulnerabilities exposed by earlier forms of Java and ActiveX development, all machines should be kept up-to-date with new version releases. Scripting language vulnerabilities may be addressed in this manner, as well as by turning off or increasing the client's browser security settings to prevent automatic code execution. Answer B is incorrect because this setting controls third-party tool bands and browser helper objects. Answer C is incorrect because increasing the pop-up setting will not mitigate Java vulnerabilities. Answer D is incorrect because Integrated Windows Authentication has to do with logon information, not Java vulnerabilities.

6. **Answer: C.** Microsoft developed a precompiled application technology that can be embedded in a web page in the same way as Java applets. This technology is referred to as ActiveX, and its controls share many of the same vulnerabilities present in embedded Java applets. Answer A is incorrect because cookies are temporary files stored in the client's browser cache to maintain settings across multiple pages, servers, or sites. Answer B is incorrect because JavaScript is a smaller language that does not create applets or standalone applications. Answer D is incorrect because CGI (Common Gateway Interface) scripts are programs that run on the server to service client requests.

7. **Answer: B.** Clients should regularly clear their browser cookie cache to avoid exposing long-term browsing habits in this way. Where possible, client browsers may also be configured to block third-party cookies, although many online commerce sites require this functionality for their operation. Answer A is incorrect because this setting controls third-party tool bands and browser helper objects. Answer C is incorrect because blocking all cookies would hamper the functionality for many online commerce sites. Answer D is incorrect because disabling automatic code execution on client browsers has more to do with Java applets and ActiveX controls.

8. **Answer: D.** By restricting the data that can be input and using proper input validation, application designers can reduce the threat posed by maliciously crafted URL references and redirected web content. Answer A is incorrect because third-party cookies would limit exposing long-term browsing habits. Answer B is incorrect because accepting only numeric data input is not feasible, and if it is not validated, it will not

mitigate attacks. Answer C is incorrect because this setting controls third-party tool bands and browser helper objects.

9. **Answer: A.** Whereas cookies generally provide benefits to the end users, spyware would be most likely to use a tracking cookie. A tracking cookie is a particular type of permanent cookie that stays around, whereas a session cookie stays around only for the particular visit to a website. Answers B and D are incorrect because these sites would use session cookies, not tracking cookies. Answer C is incorrect because a Trojan appears to be useful software but has code hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code after it has been executed.

10. **Answer: D.** Spammers search for unprotected SMTP relay services running on public servers, which may then be used to resend SMTP messages to obscure their true source. Answer A is incorrect because buffer overflows are associated with not using proper input validation. Answer B is incorrect. A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. Answer C is incorrect. Spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent.

11. **Answer: B.** A tracking cookie is a particular type of permanent cookie that stays around, whereas a session cookie stays around only for the particular visit to a website. Therefore, answer C is incorrect. Answers A and D are incorrect because tracking cookies are beneficial or valuable only to the tracking party, not the user.

12. **Answer: A.** Secure Hypertext Transport Protocol (S-HTTP) operates over port 80 along with regular HTTP traffic. Answer B is incorrect because HTTPS (HTTP over SSL) and SSL employ X.509 digital certificates and operate over port 443. Answer C is incorrect. Email clients connect to port 110 of a remote email server, and then use the POP3 protocol to retrieve email. Answer D is incorrect. Port 4445 uses TCP/UDP for service type upnotifyp.

13. **Answer: B.** HTTPS (HTTP over SSL) and SSL employ X.509 digital certificates and operate over port 443. Answer A is incorrect because Secure Hypertext Transport Protocol (S-HTTP) operates over port 80 along with regular HTTP traffic. Answer C is incorrect. Email clients connect to port 110 of a remote email server, and then use the POP3 protocol to retrieve email. Port 4445 uses TCP/UDP for service type upnotifyp; therefore, Answer D is incorrect.

14. **Answer: B, C.** Malformed certificates may be used to exploit the parsing libraries used by SSL agents. SSL certificates may also be used to establish links vulnerable to packet sniffing by using compromised self-signed or expired certificates. Other exploits include the use of small key sizes, outdated certificate revocation lists, and other mechanisms intended to provide weak or compromised SSL certificates. Answers A and D are incorrect because they are associated with programming errors. Buffer-overflow vulnerabilities may be used to enact arbitrary commands on a server. Format string vulnerabilities may result in unauthorized access to enact commands on a server or impair its normal operation. Improperly formatted requests may be used to create an effective denial-of-service (DoS) attack against the server, preventing it from responding to normal requests.

15. **Answer: A, D.** Buffer-overflow vulnerabilities may be used to enact arbitrary commands on the LDAP server. Format string vulnerabilities may result in unauthorized access to enact commands on the LDAP server or impair its normal operation. Improperly formatted requests may be used to create an effective denial-of-service (DoS) attack against the LDAP server, preventing it from responding to normal requests. Answers B and C are incorrect because they are associated with SSL certificate vulnerabilities. Malformed certificates may be used to exploit the parsing libraries used by SSL agents. SSL certificates may also be used to establish links vulnerable to packet sniffing by using compromised self-signed or expired certificates. Other exploits include the use of small key sizes, outdated certificate revocation lists, and other mechanisms intended to provide weak or compromised SSL certificates.

16. **Answer: B, C.** FTP servers provide user access to upload or download files between client systems and a networked FTP server. FTP servers include many potential security issues, including anonymous file access and unencrypted authentication. Answers A and D are incorrect because they are associated with programming errors. Buffer-overflow vulnerabilities may be used to enact arbitrary commands on a server. Format string vulnerabilities may result in unauthorized access to enact commands on a server or impair its normal operation. Improperly formatted requests may be used to create an effective denial-of-service (DoS) attack against the server, preventing it from responding to normal requests.

17. **Answer: A.** FTPS (FTP over SSL) using TCP port 21. Answer B is incorrect because HTTP operates over port 80. Answer C is incorrect. A more secure version of FTP (S/FTP) has been developed, including SSL encapsulation. This is referred to as FTP over SSH using the Secure Shell (SSH) TCP port 22. Answer D is incorrect because port 81 is used as an alternate port for hosting a website.

18. **Answer: A, B, C.** Attackers develop viral malware capable of spreading through contact lists within IM clients. Others focus on capturing IM traffic and cached logs of past conversations, in an attempt to obtain useful or harmful information. The file-transfer and desktop-sharing capabilities of many clients present challenges against unauthorized data sharing, while creative attackers make use of the audio and video capabilities to directly “tap” unwary IM users. Answer D is incorrect. Improperly formatted requests may be used to create an effective denial-of-service (DoS) attack against servers, preventing them from responding to normal requests.

19. **Answer: A, C.** CGI scripts may be exploited to leak information, including details about running server processes and daemons. Samples included in some default installations are not intended for security and include well-known exploits, and buffer overflows may allow arbitrary commands to be executed on the server. Answer B is incorrect because anonymous file access is associated with FTP servers. Answer D is incorrect because CGI scripts do not run on the client system.

20. **Answer: D.** When a website redirects the client’s browser to attack yet another site, this is referred to as cross-site scripting. Answer A is incorrect because unencrypted authentication is associated with FTP servers. Answer B is incorrect because a session hijack occurs when an attacker causes the client’s browser to establish a secure connection to a compromised web server acting as a proxy or redirecting traffic to a secure target site, exposing traffic as it passes through the compromised system. Answer C is incorrect because a buffer overflow occurs when data input exceeds the

memory space allocated and injects unanticipated data or programmatic code into executable memory.

21. **Answer: B.** An early exploit of JavaScript allowed access to files located on the client's system if the name and path were known. Answers A and D are incorrect because JavaScript, not Java, can be used to execute arbitrary instructions on the server, send email as the user, and allow access to cache information. Answer C is incorrect because Java, not JavaScript, can continue running even after the applet has been closed.

22. **Answer: A.** Exploits may allow the identification of configuration details of the server that may be helpful to later unauthorized access attempts, a process often referred to as profiling. Answer B is incorrect because reporting portrays information collected in a particular area. Answer C is incorrect because abstracting is used to understand and solve problems. Answer D is incorrect because hyperlinking is associated with web pages.

23. **Answer: B.** The danger to maintaining session information is that sites may access cookies stored in the browser's cache that may contain details on the user's e-commerce shopping habits, along with many user details that could possibly include sensitive information identifying the user or allowing access to secured sites. Answers A and C are incorrect because these actions prove helpful for the client. Answer D is incorrect because this action is associated with Java.

24. **Answer: A, C.** Browser-based vulnerabilities include session hijacking, buffer overflows, cross-site scripting, and add-in vulnerabilities. Answer B is incorrect because SQL injection is associated with SQL database servers. Answer D is incorrect because social engineering is taking advantage of human nature.

25. **Answer: C.** The common BitTorrent file-sharing application is an example of a resource-sharing peer-to-peer (P2P) solution, allowing users to transport files between remote clients without passing through a central server for access. This presents difficulties for access restriction because any two clients may negotiate connections using random ports and protocols, bypassing traffic analysis and access control restrictions. Answer A is incorrect; it describes a vulnerability exploitation of Java, CGI scripts, and LDAP. Answer B is incorrect; anonymous file upload is associated with FTP servers. Answer D is incorrect because it describes a CGI script exploit.

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques.

1. **Answer: B.** Unsecured equipment is vulnerable to social-engineering attacks. It is much easier for an attacker to walk into a reception area, say she is here to do some work on the server, and get server access than to get into a physically secured area with a guest sign-in and sign-out sheet. Brute-force attacks, malware, and rootkits can be installed or launched without physical access. Therefore, answers A, C, and D are incorrect.

2. **Answer: C.** The goal of a physical security policy is to allow only trusted use of resources via positive identification that the entity accessing the systems is someone or something that has permission to do so based on the security model the organization has chosen. Answers A, B, and D are incorrect because only allowing officers, only what is deemed to be credible users is discretionary, whereas allowing all visitors will create an unsecure environment.

3. **Answer: B, C.** In very high-security areas, frosted or painted glass can be used to eliminate direct visual observation of user actions, and very high-security scenarios may mandate the use of electromagnetic shielding to prevent remote monitoring of emissions generated by video monitors, network switching, and system operation. Answers A and D are incorrect; picket and chain-link fencing should not be used in high-security areas.

4. **Answer: A.** Buildings that house sensitive information and systems usually have an area of cleared land surrounding them. This area is referred to as no-man's land. The purpose of this area is to eliminate the possibility of an intruder hiding in the bushes or behind another building. Answer B is incorrect because it increases the chances of an intruder hiding. Answer C is incorrect; it describes a mantrap. Answer D is incorrect because it describes a wireless lock entry.

5. **Answer: C.** A mantrap is a holding area between two entry points that gives security personnel time to view a person before allowing him into the internal building. Answer A is incorrect because it describes no-man's land. The purpose of this area is to eliminate the possibility of an intruder hiding in the bushes or behind another building. Answer B is incorrect because it increases the chances of an intruder hiding. Answer D is incorrect because it describes a wireless lock entry.

6. **Answer: D.** A cipher lock has a punch code entry system. A wireless lock is opened by a receiver mechanism that reads the card when it is held close to the receiver. Based on this information, answers A, B, and C are incorrect.

7. **Answer: A.** Video or CCTV cameras should be posted in key locations so that the entire area is covered. Place cameras near entrances and exits to capture each visitor who comes in and out of the parking lot. Place cameras strategically so that every area of the parking lot can be seen by a camera's field of vision. Answer B is incorrect. If the parking lot covers a large area, security guard coverage may not be enough. Answer C is incorrect because a keycard entry point can easily be compromised. Answer D incorrect because motion detection is not feasible for a parking lot.

8. **Answer: A, B, D.** External motion detectors can be based on light, sound, infrared, or ultrasonic technology. Answer C is incorrect because radio-frequency identification (RFID) is an automatic identification method.

9. **Answer: A.** Mandatory physical access controls are commonly found in government facilities and military installations, where users are closely monitored and very restricted. Because they are being monitored by security personnel and devices, users cannot modify entry methods or let others in. Answer B is incorrect. In role-based access methods for physical control, groups of people who have common access needs are predetermined, and access to different locations is allowed with the same key or swipe card. Answer C is incorrect. Discretionary physical control to a building or room is delegated to parties responsible for that building or room. Answer D is incorrect.

Allowing access based on individual needs is both costly and causes extensive administrative overhead.

10. **Answer: B.** In role-based access methods for physical control, groups of people who have common access needs are predetermined, and access to different locations is allowed with the same key or swipe card. Answer A is incorrect. Mandatory physical access controls are commonly found in government facilities and military installations, where users are closely monitored and very restricted. Because they are being monitored by security personnel and devices, users cannot modify entry methods or let others in. Answer C is incorrect. Discretionary physical control to a building or room is delegated to parties responsible for that building or room. Answer D is incorrect. Allowing access based on individual needs is both costly and causes extensive administrative overhead.

11. **Answer: A, B, D.** Buildings that house sensitive information and systems usually have an area of cleared land surrounding them. This area is referred to as no-man's land. A building that houses top-secret info would need also require a mantrap and door access system in addition to a no-man's land. Answer C is incorrect because a wooden fence provides little protection.

12. **Answer: D.** Video surveillance such as closed-circuit television (CCTV) is the most common method of surveillance. The picture is viewed or recorded, but not broadcast. It was originally developed as a means of security for banks. Answer A is incorrect because a mantrap is a holding area between two entry points that gives security personnel time to view a person before allowing him into the internal building. Answer B is incorrect because security dogs are not a good solution for a bank. Answer C is incorrect because painted glass is used a method of obscuring views. This it is not a sufficient method of security for a bank.

13. **Answer: C.** Motion detectors can alert security personnel of intruders or suspicious activity on the company's premises. They can be based on light, sound, infrared, or ultrasonic technology. These devices must be properly configured because they are extremely sensitive and can issue false alarms if set too stringently. Answers A and B are incorrect because they are false statements. Answer D is incorrect; although motion detectors may be a more expensive solution, the question asks for the main security concern.

14. **Answer: A.** The quickest way to tell which ports are open and which services are running is to do a `netstat` operation on the machine. Answer B is incorrect; `nbtstat` is designed to help troubleshoot NetBIOS name resolution problems. Answer C is incorrect; `ipconfig` is used to troubleshoot IP address configuration. Answer D is incorrect; `msconfig` is used to configure startup services and on Windows computers.

15. **Answer: D.** SNMP is used for monitoring the health of network equipment, computer equipment, and devices like uninterruptible power supplies (UPS). Answer A is incorrect because SubNetwork Access Protocol (SNAP) defines how data is formatted for transmission and how access to the network is controlled. Answer B is incorrect because SMTP is used for email. Answer C is incorrect because the Synchronous Data Link Control (SDLC) protocol was developed by IBM to be used as the Layer 2 of the SNA hierarchical network.

16. **Answer: B, C.** The best way to protect the network infrastructure from attacks aimed at antiquated or unused ports and protocols is to remove any unnecessary protocols and create Access Control Lists to allow traffic on necessary ports only. By doing so, you eliminate the possibility of unused and antiquated protocols being exploited, and you minimize the threat of an attack. Answer A is incorrect. It is not always necessary to keep protocols installed by default. Answer D is incorrect. Users should never control what goes in and out of the network.

17. **Answer: C.** To improve server performance, logs should be stored on a nonsystem striped or striped/mirrored disk volume. Answer A is incorrect. Storing the log files in the DMZ is poor practice because the servers located here are generally more vulnerable. Answers B and D are incorrect; storing the log files on the local machine will not improve performance.

18. **Answer: D.** Log files should be stored in a centralized repository of an offline volume or on a standalone computer. Answer A is incorrect; storing the log files on the local machine will not improve security. Answer B is incorrect. Storing the log files on the intranet is poor practice as the information is visible and more vulnerable. Answer C is incorrect. Storing the log files in the DMZ is poor practice because the servers located here are generally more vulnerable.

19. **Answer: C.** When implementing an application logging strategy, look for a solution that uses standard protocols and formats so that analysis is simpler. Therefore, answers A, B, and D are incorrect.

20. **Answer: A, B, D.** IIS logs may include information about site visitors and their viewing habits. They can be used to assess content, identify bottlenecks, or investigate attacks. Answer C is incorrect. Task Manager is a tool that you can use to end processes.

21. **Answer: D.** DNS logging may cause performance degradation on the server. It should be used only for troubleshooting purposes. By enabling DNS debug logging, you can log all DNS-related information. Based on this information, answers A, B, and C are incorrect.

22. **Answer: D.** In UNIX- or Linux-based systems, programs send log entries to the system logging daemon, syslogd. Answer A is incorrect because mtools.conf is a configuration file for all the operations. Answers B and C are incorrect; both Msconfig and Event Viewer are tools used on Windows-based systems.

23. **Answer: B, C.** You should employ strict access controls on all logging servers. If allowable, encrypt the log files and store log files on a standalone system. Answer A is incorrect; it is not good practice to store log files in plain text. Answer D is incorrect; log files should not be stored on data partitions of individual systems.

24. **Answer: B.** Task Manager is a tool that you can use to end processes or applications that get hung up or cause the operating system to become unstable, without having to reboot the machine. It also gives you an instant view of CPU and memory usage. Answer A is incorrect because Network Monitor is used to capture network traffic and generate statistics for creating reports. Answer C is incorrect because Event Viewer enables you to view certain events that occur on the system. Event Viewer maintains three log files: one for system processes, one for security information, and one for applications. Answer D is incorrect because Microsoft's Performance console is used for tracking and viewing the utilization of system resources.

25. **Answer: C.** Authentication and accounting logging is particularly useful for troubleshooting remote-access policy issues. Answer A is incorrect because Internet Information Services (IIS) logging is designed to be more detailed than the event-logging or performance-monitoring features of Windows Server operating systems. The IIS logs can include information such as who has visited your site, what they viewed, and when the information was viewed last. Answer B is incorrect because critical and error level logging is one of the eight logging levels available for Cisco logging devices. Answer D is incorrect because authentication and accounting logging information is used to track remote-access usage and authentication attempts. This logging is separate from the events recorded in the system event log.

26. **Answer: A, C, D.** Antivirus software, just like other software applications, usually contains a folder within the application for logging events such as updates, quarantined viruses, and update history. Answer B is incorrect. Dropped packets are normally found in router logs.

27. **Answer: B.** Routing and remote access logging information is used to track remote-access usage and authentication attempts. This logging is separate from the events recorded in the system event log. Therefore, Answer D is incorrect. Answer A is incorrect; firewall logging will not log remote access and authentication. Answer C is incorrect; IIS logging will not log remote access and authentication.

28. **Answer: C.** Auditing is the process of tracking users and their actions on the network. Answer A is incorrect because it describes baselining. Answer B is incorrect because it describes logging. Answer D is incorrect because it describes monitoring.

29. **Answer: A, B.** Without proper planning and policies, you probably will quickly fill your log files and hard drives with useless or unused information. The more quickly you fill up your log files, the more frequently you need to check the logs; otherwise, important security events may get deleted unnoticed. Answer C is incorrect because log files should not be stored on user hard drives. Answer D is incorrect. When auditing is not clear-cut, the workload of the system administrator increases.

30. **Answer: B, C.** Auditing user privileges is generally a two-step process that involves enabling auditing within the operating system and then specifying the resources to be audited. Answer A is incorrect; auditing, not logging, needs to be enabled. Answer D is incorrect; the log file storage directory is specified, not the audit file directory.

31. **Answer: D.** Auditing of access use and rights changes should be implemented to prevent unauthorized or unintentional access for a guest or restricted user account access to sensitive or protected resources. Answer A is incorrect; group policy controls access to resources. Answer B is incorrect; retention policies concern data, not user access. Answer C is incorrect; DHCP deals with the issuing of IP addresses not access to accounts.

32. **Answer: C.** It is equally important to audit both failed and successful events because both may reveal unauthorized access or an unexpected escalation of access rights. Answers A and B are incorrect because it is important to audit both types of events. Answer D is incorrect because auditing is an important part of securing the network.

33. **Answer: B.** Logging is the process of collecting data to be used for monitoring and reviewing purposes. Auditing is the process of verification that normally involves going through log files; therefore, answer A is incorrect. Answer C is incorrect. Baselining is measuring and rating the performance of a network. Typically, the log files are frequently inspected, and inspection is not the process of collecting the data; therefore, answer D is incorrect.

34. **Answer: D.** Turning on all audit counters for all objects could significantly impact server performance. Answer A is incorrect; auditing is done in the background and does not affect user productivity. Answer B is incorrect; if the I/O activity were affected at all, it would be increased. Answer C is incorrect; as with I/O activity, if there were change, it would be an increase, not a decrease.

35. **Answer: B.** In Group Policy, the settings that will actually be applied to an object will be a combination of all the settings that can affect the object. Answer A is incorrect because all group policies are applied to the object. Answer C is incorrect; in a universal group, the policies may be applied from different domains. Answer D is incorrect; this would apply only if there was not a domain environment.

36. **Answer: B.** You can use gpresult to see what policy is in effect and to troubleshoot problems. Answer A is incorrect; you can use gpupdate to refresh policy immediately and to specify certain options at the command line. Answer C is incorrect; the Resultant Set of Policy (RSoP) tool is used to determine the effective settings on the computer that you are working from or any other computer in a Windows Server 2008 Active Directory domain. Answer D is incorrect; the Group Policy object is used to create group policies.

37. **Answer: A.** You can use the Resultant Set of Policy (RSoP) tool to determine the effective settings on the computer that you are working from or any other computer in a Windows Server 2008 Active Directory domain. Answer B is incorrect; the Group Policy object is used to create group policies. Answer C is incorrect; you can use gpupdate to refresh policy immediately and to specify certain options at the command line. Answer D is incorrect; the local security settings are used on the local machine only.

38. **Answer: C.** Auditing success and failure events in the system event category, allows one to notice unusual activity that may indicate attempts to gain access to the network. Auditing success events in the account management event category can be used to verify changes that were made to account properties and group properties; therefore, answer A is incorrect. Answer B is incorrect: Auditing success events in the policy change event category on domain controllers indicates someone has changed the local security authority (LSA). Answer D is incorrect; auditing success events in the logon event category records when each user logs on to or logs off from the computer.

39. **Answer: D.** Auditing success events in the logon event category records when each user logs on to or logs off from the computer. Answer A is incorrect. Auditing success events in the policy change event category will record success and failure events in the system events. Answer B is incorrect. Auditing success events in the policy change event category on domain controllers indicates someone has changed the local security authority (LSA). Answer C is incorrect; auditing success events in the account management event category is used to verify changes that were made to account properties and group properties.

40. **Answer: C.** Auditing success events in the account logon event category on domain controllers is used to verify when users log on to or log off from the domain. Answer A is incorrect. Auditing success events in the policy change event category will record success and failure events in the system events. Answer B is incorrect. Auditing success events in the policy change event category on domain controllers indicates someone has changed the local security authority (LSA). Answer D is incorrect; auditing success events in the logon event category records when each user logs on to or logs off from the computer.

Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities.

1. **Answer: A.** A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

2. **Answer: D.** A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications.

3. **Answer: C.** A protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

4. **Answer: B.** A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses testing for the presence of known vulnerabilities in software configuration and accessible services.

5. **Answer: D.** Open Vulnerability Assessment Language (OVAL) is intended as an international language for representing vulnerability information using an XML schema for expression, allowing tools to be developed to test for identified vulnerabilities in the OVAL repository. Answer A is incorrect because it describes the Open Systems Interconnection reference model (OSI model). Answer B is incorrect because it describes IEEE 802 standards. Answer C is incorrect because it describes the International Organization for Standardization (ISO).

6. **Answer: A.** Within U.S. governmental agencies, vulnerability may be discussed using the Open Vulnerability Assessment Language (OVAL) sponsored by the Department of Homeland Security's National Cyber Security Division (NCSD). Answer B is incorrect because IEEE refers to a family of IEEE standards dealing with local area networks and metropolitan area networks. Answer C is incorrect because the International Organization for Standardization, widely known as ISO, is an international-standard-setting body composed of representatives from various national standards organizations. Answer D is incorrect because the Information Systems Security Association is a security-focused group.

7. **Answer: A.** A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Port scanners are useful in creating an inventory of services hosted on networked systems. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

8. **Answer: C.** A protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Individual protocols, specific endpoints, or sequential access attempts may be identified using this utility, which is often referred to as a packet sniffer. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP

addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

9. **Answer: D.** A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services. Unlike port scanners, which test only for the availability of services, vulnerability scanners may check for the particular version or patch level of a service to determine its level of vulnerability. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications.

10. **Answer: B.** Code reviews are typically conducted using automated software programs designed to check code, as well as manual human checks, in which someone not associated with development combs through the code. Answer A is incorrect because an architecture review is an assessment of system architecture that considers the entire system. It provides the ability to identify faulty components and interaction between various elements. Answer C is incorrect because design review refers more specifically to the components of the architecture at a more micro level. A review of design will consider various elements such as compatibility, modularity, reusability, and, of course, security. Answer D is incorrect. The attack surface refers to the amount of running code, services, and user-interaction fields and interfaces.

11. **Answer: D.** The attack surface refers to the amount of running code, services, and user-interaction fields and interfaces. Answer A is incorrect because an architecture review is an assessment of system architecture that considers the entire system. It provides the ability to identify faulty components and interaction between various elements. Answer B is incorrect. Code reviews are typically conducted using automated software programs designed to check code, as well as manual human checks, in which someone not associated with development combs through the code. Answer C is incorrect because design review refers more specifically to the components of the architecture at a more micro level. A review of design will consider various elements such as compatibility, modularity, reusability, and, of course, security.

12. **Answer: A.** An architecture review is an assessment of system architecture that considers the entire system. It provides the ability to identify faulty components and interaction between various elements. Answer B is incorrect. Code reviews are typically conducted using automated software programs designed to check code, as well as manual human checks, in which someone not associated with development combs through the code. Answer C is incorrect because design review refers more specifically to the components of the architecture at a more micro level. A review of design will consider various elements such as compatibility, modularity, reusability, and, of course, security. Answer D is incorrect. The attack surface refers to the amount of running code, services, and user-interaction fields and interfaces.

13. **Answer: D.** Password crackers should provide only the relative strength of a password, rather than the password itself, to avoid weakening logon responsibility under evidentiary discovery actions. Answers A, B, and C are incorrect because password crackers should not provide the password itself to avoid disclosure under e-discovery proceedings.

14. **Answer: B.** The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. This information can be used to identify single points of failure, conduct a network inventory, and create graphical details suitable for reporting on network configurations. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

15. **Answer: C.** A protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Individual protocols, specific endpoints, or sequential access attempts may be identified using this utility, which is often referred to as a packet sniffer. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer B is incorrect. A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

Objective 3.8: Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.

1. **Answer: B.** Friendly attacks against a network test the security measures put into place. Such attacks are referred to as penetration tests or simply “pen tests.” Answer A and C are incorrect because a vulnerability assessment or a security assessment are not directed efforts to exploit vulnerabilities in an attempt to gain access to networked resources. Answer D is incorrect because a compliance test has nothing to do with penetration testing.

2. **Answer: A, C.** Penetration tests may cause some disruption to network operations as a result of the actual penetration efforts conducted. Penetration tests can also make legitimate attacks by generating false data in intrusion detection systems/intrusion prevention systems (IDS/IPS). Answers B and D are incorrect; although internal and external users may be affected, these are not the most serious downsides of penetration testing.

3. **Answer: B, C.** Some systems administrators may perform amateur pen tests against networks in an attempt to prove a particular vulnerability exists or to evaluate the overall security exposure of a network. This is a bad practice because it generates false intrusion data, may weaken the network's security level, and may be a violation of privacy laws, regulatory mandates, or business entity guidelines. Answers A and D are incorrect because the statements are contrary to the correct answers.

4. **Answer: D.** Vulnerability assessments may be complemented by directed efforts to exploit vulnerabilities in an attempt to gain access to networked resources. Penetration testing includes all of the process in vulnerability assessment plus an important extra step, which is to exploit the vulnerabilities found in the discovery phase. Based in the previous information, answers A, B, and C are incorrect.

5. **Answer: A.** Penetration tests can also make legitimate attacks by generating false data in IDS systems, concealing aggression that is otherwise unrelated to the officially sanctioned penetration test. Answers B and C are incorrect; although they are both concerns, they are not the main security risk. Answer D is incorrect; penetration testing itself does not weaken the network's security level; however, amateur pen testing can.

6. **Answer: A.** A black box test is conducted with the assessor having no information or knowledge about the inner workings of the system or knowledge of the source code, for example. Answer B is incorrect because white box testing, also called clear box or glass box, provides more transparency. White box techniques are often tests to see if programming constructs are placed correctly and carry out the required actions or not. Answer C is incorrect because gray box testing uses a combination of both white and black box techniques. This can be more easily thought of as being translucent. Answer D is incorrect because green box testing is a testing process that takes multiple integrated systems that have passed system testing as input and tests their required interactions.

7. **Answer: B.** White box testing, also called clear box or glass box, provides transparency. White box techniques are often tests to see if programming constructs are placed correctly and carry out the required actions or not. Answer A is incorrect because black box testing is conducted with the assessor having no information or knowledge about the inner workings of the system or knowledge of the source code for example. Answer C is incorrect because gray box testing uses a combination of both white and black box techniques. This can be more easily thought of as being translucent. Answer D is incorrect because green box testing is a testing process that takes multiple integrated systems that have passed system testing as input and tests their required interactions.

8. **Answer: B.** A network mapper is a software utility used to conduct network assessments over a range of IP addresses. The network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. Answer A is incorrect. A port-scanning software utility will scan a single machine or a range of IP addresses, checking for a response on service ports. Answer C is incorrect because a protocol analyzer is a software utility used on a hub, a switch supervisory port, or in line with network connectivity to allow the analysis of network communications. Answer D is incorrect. A vulnerability scanner is a software utility that will scan a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services.

9. **Answer: C.** A password cracker is a software utility that allows direct testing of user logon password strength by conducting a brute-force password test using dictionary terms, specialized lexicons, or mandatory complexity guidelines. Answer A is incorrect. Password Locker is a commercial program that lets you save passwords, recover passwords, and manage and form-fill all your usernames and passwords. Answer B is incorrect because a password generator creates random passwords. Answer D is incorrect. A password keychain, most commonly found on Apple computers, keeps track of your passwords for any type of account.

10. **Answer: A.** Unlike port scanners, which test only for the availability of services, vulnerability scanners may check for the particular version or patch level of a service to determine its level of vulnerability. Answers B, C, and D are incorrect because they do not accurately describe port scanners or vulnerability scanners.

This page intentionally left blank