CompTIA® Cybersecurity Analyst (CSA+) Cert Guide

Troy McMillan

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA Cybersecurity Analyst (CSA+) Cert Guide

ISBN-13: 978-0-7897-5695-4
ISBN-10: 0-7897-5695-1

Library of Congress Control Number: 2017938509

Printed in the United States of America

First Printing: June 2017

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Michelle Newcomb

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Indexer
Publishing Works, Inc.

Proofreader
Chuck Hutchinson

Technical Editors
Chris Crayton
Robin Abernathy

Publishing Coordinator
Vanessa Evans

Cover Designer
Chuti Prasertsith

Compositor
Bronkella Publishing

Contents at a Glance

Table of Contents

About the Author

Troy McMillan is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 16 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. He has written or contributed to more than a dozen projects, including the following recent ones:

- Contributing subject matter expert for CCNA Cisco Certified Network Associate Certification Exam Preparation Guide (Kaplan)
- Author of *CISSP Cert Guide* (Pearson)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)
- Author of *CASP Cert Guide* (Pearson)

Troy has also appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND1; and ICND2.

He delivers CISSP training classes for CyberVista, authorized online training provider for $(ISC)^2$.

Troy now creates certification practice tests and study guides for the Transcender and Self-Test brands. He lives in Pfafftown, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife, Heike, who has supported me every time I've reinvented myself.

Acknowledgments

I must thank everyone on the Pearson team for all of their help in making this book better than it would have been without their help. That includes Michelle Newcomb, Eleanor Bru, Chris Crayton, and Robin Abernathy.

About the Technical Reviewers

Chris Crayton, MCSE, is an author, a technical consultant, and a trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Certification Preparation, the owners of the Transcender and Self Test brands, for more than a decade. Robin has written and edited certification preparation materials for many $(ISC)^2$, Microsoft, CompTIA, PMI, Cisco, and ITIL certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past couple years, she has ventured into the traditional publishing industry, technical editing several publications and coauthoring Pearson's *CISSP Cert Guide* and *CASP Cert Guide*. She presents at technical conferences and hosts webinars on IT certification topics.

We Want to Hear from You!

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

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

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

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

E-mail: feedback@pearsonitcertification.com

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

Reader Services

Register your copy of *CompTIA Cybersecurity Analyst (CSA+) Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789756954 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

CompTIA

CompTIA Network+

Becoming a CompTIA Certified IT Professional is Easy

It's also the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

Growing Demand

Labor estimates predict some technology fields will experience growth of over 20% by the year 2020.* CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries

IT professionals with certifications on their resume command better jobs, earn higher salaries and have more doors open to new multi-industry opportunities.

Verified Strengths

91% of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers.**

Universal Skills

CompTIA certifications are vendor neutral—which means that certified professionals can proficiently work with an extensive variety of hardware and software found in most organizations.

Learn

Learn more about what the exam covers by reviewing the following:

- Exam objectives for key study points.
- Sample questions for a general overview of what to expect on the exam and examples of question format.
- Visit online forums, like LinkedIn, to see what other IT professionals say about CompTIA exams.

Certify

Purchase a voucher at a Pearson VUE testing center or at CompTIAstore.com.

- Register for your exam at a Pearson VUE testing center:
- Visit pearsonvue.com/CompTIA to find the closest testing center to you.
- Schedule the exam online. You will be required to enter your voucher number or provide payment information at registration.
- Take your certification exam.

Work

Congratulations on your CompTIA certification!

- Make sure to add your certification to your resume.
- Check out the CompTIA Certification Roadmap to plan your next career move.

Learn more: **Certification.CompTIA.org/networkplus**

* Source: CompTIA 9th Annual Information Security Trends study: 500 U.S. IT and Business Executives Responsible for Security
** Source: CompTIA Employer Perceptions of IT Training and Certification
*** Source: 2013 IT Skills and Salary Report by CompTIA Authorized Partner

Introduction

CompTIA CSA+ bridges the skills gap between CompTIA Security+ and CompTIA Advanced Security Practitioner (CASP). Building on CSA+, IT professionals can pursue CASP to prove their mastery of the hands-on cybersecurity skills required at the 5- to 10-year experience level. Earn the CSA+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

CompTIA CSA+ certification is designed to be a "vendor-neutral" exam that measures your knowledge of industry-standard technology.

Goals and Methods

The number-one goal of this book is a simple one: to help you pass the 2017 version of the CompTIA CSA+ certification exam CS0-001.

Because the CompTIA CSA+ certification exam stresses problem-solving abilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the CSA+ certification objectives, this book uses the following methods:

- The beginning of each chapter defines the topics to be covered in the chapter; it also lists the corresponding CompTIA CSA+ objectives.
- The body of the chapter explains the topics from a hands-on and theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in a table at the end of the chapter.
- Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the complete key terms in the glossary.

Who Should Read This Book?

The CompTIA CSA+ examination is designed for IT security analysts, vulnerability analysts, and threat intelligence analysts. The exam certifies that a successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities,

threats, and risks to an organization, with the end goal of securing and protecting applications and systems in an organization.

The recommended experience for taking the CompTIA CSA+ exam includes Network+, Security+, or equivalent knowledge as well as a minimum of three or four years of hands-on information security or related experience. While there is no required prerequisite, CSA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

This book is for you if you are attempting to attain a position in the cybersecurity field. It is also for you if you want to keep your skills sharp or perhaps retain your job due to a company policy that mandates that you update security skills.

This book is also for you if you want to acquire additional certifications beyond Security+. The book is designed to offer easy transition to future certification studies.

Strategies for Exam Preparation

Strategies for exam preparation vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of three or four years of hands-on security or related experience followed by rigorous study of the exam objectives.

After you have read through the book, have a look at the current exam objectives for the CompTIA CSA+ Certification Exams, listed at https://certification.comptia.org/certifications/cybersecurity-analyst#tab4. If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams found on the website that accompanies this book. As you work through the practice exam, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed those areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become.

After you have worked through the practice exam a second time and feel confident in your skills, schedule the CompTIA CSA+ CS0-001 exam through Pearson Vue (www.vue.com). To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take it.

The CompTIA CSA+ certification credential for those passing the certification exams is now valid for three years. To renew your certification without retaking the

exam, you need to participate in continuing education (CE) activities and pay an annual maintenance fee of $50 (that is, $150 for three years). See https://certification.comptia.org/continuing-education/how-to-renew/ce-program-fees for fee details. To learn more about the certification renewal policy, see https://certification.comptia.org/continuing-education.

Table I-1 CSA+ Exam Topics

Chapter	Exam Topics	CompTIA CSA+ Exam Objectives Covered
1	1.1 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.	CS0-001 objective 1.1
2	1.2 Given a scenario, analyze the results of a network reconnaissance.	CS0-001 objective 1.2
3	1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.	CS0-001 objective 1.3
4	1.4 Explain the purpose of practices used to secure a corporate environment.	CS0-001 objective 1.4
5	2.1 Given a scenario, implement an information security vulnerability management process.	CS0-001 objective 2.1
6	2.2 Given a scenario, analyze the output resulting from a vulnerability scan.	CS0-001 objective 2.2
	2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.	CS0-001 objective 2.3
7	3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.	CS0-001 objective 3.1
	3.2 Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.	CS0-001 objective 3.2
8	3.3 Explain the importance of communication during the incident response process.	CS0-001 objective 3.3
	3.4 Given a scenario, analyze common symptoms to select the best course of action to support incident response.	CS0-001 objective 3.4
9	3.5 Summarize the incident recovery and post-incident response process.	CS0-001 objective 3.5
10	4.1 Explain the relationship between frameworks, common policies, controls, and procedures.	CS0-001 objective 4.1
11	4.2 Given a scenario, use data to recommend remediation of security issues related to identity and access management.	CS0-001 objective 4.2

Chapter	Exam Topics	CompTIA CSA+ Exam Objectives Covered
12	4.3 Given a scenario, review security architecture and make recommendations to implement compensating controls.	CS0-001 objective 4.3
13	4.4 Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).	CS0-001 objective 4.4
14	4.5 Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.	CS0-001 objective 4.5

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include the following:

- **"Do I Know This Already?" Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks:** The "Exam Preparation Tasks" section lists a series of study activities that should be done after reading the "Foundation Topics" section. Each chapter includes the activities that make the most sense for studying the topics in that chapter.
- **Key Topics Review:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The "Key Topics Review" section lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should

definitely know the information highlighted with Key Topic icons. Review these topics carefully.

- **Definition of Key Terms:** Although certification exams might be unlikely to ask a question such as "How do you define the term ____?" the CSA+ exam requires you to learn and know a lot of terminology. This section lists some of the most important terms from the chapter and asks you to write a short definition and compare your answer against the Glossary.
- **End-of-Chapter Review Questions:** The review questions help you confirm that you understand the content that you just covered.

Companion Website

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

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN 9780789756954.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

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

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

Accessing the Pearson Test Prep Software and Questions

This book comes complete with the Pearson Test Prep practice test software, which includes several exams. These practice tests are available to you either online or as

an offline Windows application. To access the practice exams that were developed to accompany this book, you need the unique access code printed on the card in the sleeve in the back of your book.

Note The cardboard case in the back of this book includes a paper that lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of the Pearson Test Prep software can be used on any device that has a browser and connectivity to the Internet, including desktop machines, tablets, and smart phones. To start using your practice exams online, simply follow these steps:

1. Go to http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter the e-mail and password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.
4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the **Exams** button to launch the exam settings screen and start your exam.

The online version of the Pearson Test Prep software is supported on the following browsers:

- Chrome (Windows and Mac), version 40 and above
- Firefox (Windows and Mac), version 35 and above
- Safari (Mac), version 7
- Internet Explorer 10 and 11
- Microsoft Edge
- Opera

The online version of the Pearson Test Prep software is supported on the following devices:

- Desktop and laptop computers
- Tablets running on Android and iOS
- Smartphones with a minimum screen size of 4.7 inches

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website.

Previous users: If you have already installed the Pearson Test Prep software from another purchase, you do not need to install it again. Launch the Pearson Test Prep software from your Start menu. Click Activate Exam in the My Products or Tools tab and enter the activation key found in the sleeve in the back of your book to activate and download the free practice questions for this book.

New users: You need to install the Pearson Test Prep software on your Windows desktop. Follow the steps below to download, install, and activate your exams.

1. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
2. Once the software finishes downloading, unzip all the files on your computer.
3. Double-click the application file to start the installation, and follow the on-screen instructions to complete the registration.
4. Once the installation is complete, launch the application and select **Activate Exam** button on the My Products tab.
5. Click the **Activate a Product** button in the Activate Product Wizard.
6. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
7. Click **Next** and then the **Finish** button to download the exam data to your application.
8. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Desktop version system requirements:

- Windows 10, Windows 8.1, Windows 7, or Windows Vista (SP2)
- Microsoft NET Framework 4.5 Client
- Pentium class 1 GHz processor (or equivalent)
- 512 MB RAM
- 650 MB hard disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the "Do I Know This Already?" quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition

In addition to the free practice exams provided with your purchase, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title provides remediation for each question, directing you to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the cardboard sleeve that contains a one-time-use code as well as instructions for where to purchase the Premium Edition.

This chapter covers the following topics:

1.0 Threat Management

1.4 Explain the purpose of practices used to secure a corporate environment.

- **Penetration Testing:** Discusses the testing process and the rules of engagement.
- **Reverse Engineering:** Includes topics such as isolation and sandboxing, authenticity of hardware, and fingerprinting and decomposition of software and malware.
- **Training and Exercises:** Describes the functions of red, blue, and white teams.
- **Risk Evaluation:** Discusses the risk evaluation process both from technical and operational viewpoints.

Practices Used to Secure a Corporate Environment

Securing a corporate environment is not a one-time endeavor. It should entail a set of processes that are embedded into day-to-day operations. Some of these processes, such as penetration testing, are deigned to locate weaknesses before attackers do, while other processes, such as fingerprinting and decomposition, are important to understand because they are techniques that attackers use to thwart your best efforts at preventing the delivery of malware. This chapter discusses the process of penetration testing, the value of understanding how attackers use fingerprinting and decomposition, the importance of training and exercises, and the steps in the risk management process.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read the entire chapter. Table 4-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions." If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks."

Table 4-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Penetration Testing	1–3
Reverse Engineering	6
Training and Exercises	4, 5
Risk Evaluation	7

1. Which of the following is the first step in a pen test?
   a. Gather information about attack methods against the target system or device.
   b. Execute attacks against the target system or device to gain user and privileged access.
   c. Document information about the target system or device.
   d. Document the results of the penetration test.

2. In which type of tests is the testing team provided with limited knowledge of the network systems and device?
   a. Blind test
   b. Double-blind test
   c. Target test
   d. External test

3. Which of the following is also referred to as a closed, or black-box, test?
   a. Zero-knowledge test
   b. Partial-knowledge test
   c. Full-knowledge test
   d. Target test

4. Which of the following is not covered in the rules of engagement?
   a. Timing
   b. Scope
   c. Compensation
   d. Authorization

5. Which of the following acts as the network defense team?
   a. Blue team
   b. White team
   c. Purple team
   d. Red team

6. With which of the following can malware executable files be executed without allowing the files to interact with the local system?
   a. Sandboxing
   b. DMZ
   c. Trusted Foundry
   d. Decomposition

7. When performing qualitative risk evaluation, which of the following is considered in addition to the impact of the event?
   a. Attack vectors
   b. Likelihood
   c. Costs
   d. Frequency

Foundation Topics

Penetration Testing

A penetration test (often called a pen test) is designed to simulate an attack on a system, a network, or an application. Its value lies in its potential to discover security holes that may have gone unnoticed. It differs from a vulnerability test in that it attempts to exploit vulnerabilities rather than simply identify them. Nothing places the focus on a software bug like the exposure of critical data as a result of the bug.

In many cases, some of the valuable information that comes from these tests is the identification of single operations that, while benign on their own, create security problems when used in combination. These tests can be made more effective when utilized with a framework like Metasploit or CANVAS (discussed Chapter 14, "Using Cybersecurity Tools and Technologies").

Penetration testing should be an operation that occurs at regular intervals, and its frequency should be determined by the sensitivity of the information on the network. An example of a pen test tool is Retina. Figure 4-1 shows Retina output from scanning a single device. In this output, you can see that the tool has identified eight serious problems (indicated by the upward-pointing arrows): weak encryption in Terminal Services, six weaknesses related to Oracle, and one weakness related to a virtualization product on the machine called Oracle VirtualBox.

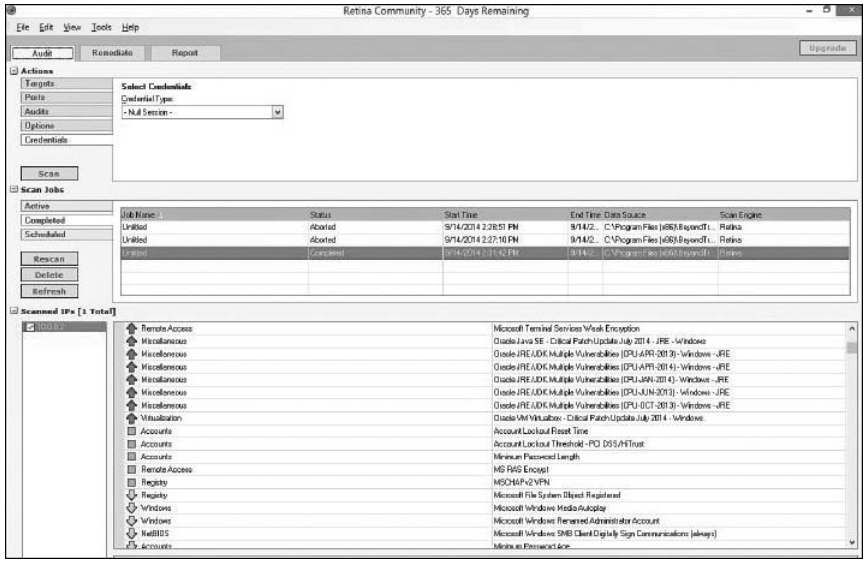

Figure 4-1 Retina Output

Key Topic

The steps in performing a penetration test are as follows:

Step 1. Planning and preparation

Step 2. Information gathering and analysis

Step 3. Vulnerability detection

Step 4. Penetration attempt

Step 5. Analysis and reporting

Step 6. Cleaning up

Both internal and external tests should be performed. Internal tests occur from within the network, whereas external tests originate outside the network, targeting the servers and devices that are publicly visible.

Strategies for penetration testing are based on the testing objectives, as defined by the organization. The strategies that you should be familiar with include the following:

Key Topic

- **Blind test:** The testing team is provided with limited knowledge of the network systems and devices, using publicly available information. The organization's security team knows that an attack is coming. This test requires more effort by the testing team, and the testing team must simulate an actual attack.
- **Double-blind test:** This test is like a blind test except the organization's security team does not know that an attack is coming. Only a few individuals at the organization know about the attack, and they do not share this information with the security team. This test usually requires equal effort for both the testing team and the organization's security team.
- **Target test:** Both the testing team and the organization's security team are given maximum information about the network and the type of test that will occur. This is the easiest test to complete but does not provide a full picture of the organization's security.

Penetration testing is also divided into categories based on the amount of information to be provided. The main categories that you should be familiar with include the following:

Key Topic

- **Zero-knowledge test:** The testing team is provided with no knowledge regarding the organization's network. The testers can use any means at their disposal to obtain information about the organization's network. This is also referred to as closed, or black-box, testing.

- **Partial-knowledge test:** The testing team is provided with public knowledge regarding the organization's network. Boundaries might be set for this type of test.
- **Full-knowledge test:** The testing team is provided with all available knowledge regarding the organization's network. This test is focused more on what attacks can be carried out.

Other penetration testing applications include Metasploit, Wireshark, CORE Impact, Nessus, Back Track, Cain & Abel, and John the Ripper. When selecting a penetration testing tool, you should first determine which systems you want to test. Then research the different tools to discover which of them can perform the tests that you want to perform for those systems. When you have a tool in mind, research the tool's methodologies for testing. In addition, the correct individual needs to be selected to carry out the test. Remember that penetration tests should include manual methods as well as automated methods because relying on only one of these two does not result in a thorough result.

Rules of Engagement

The rules of engagement define how penetration testing should occur. These issues should be settled and agreed upon before any testing begins. The following are some of the key issues to be settled:

Key Topic

- **Timing:** The timeline for the test must be established. The start and end times will be included in the scope of the project, but creating the timeline does not mean it cannot change as reality dictates; rather, it means that you have a framework to work from. This also includes the times of day the testing will occur.
- **Scope:** The scope of the test incudes the timeline and also includes a list of all devices that are included in the test, as well as a description of all testing methodologies to be used. The output of this process should be a set of documents that are provided to the tester that include the following:
  - A network diagram depicting all network segments in scope for the test
  - A data flow diagram
  - A list of services and ports exposed at the perimeter
  - Details of how authorized users access the network
  - A list of all network segments that have been isolated from the test to reduce scope

- **Authorization:** Formal authorization should be given to the tester to perform the test, with written approval by upper management. Without this, the tester could be liable for attempting to compromise the network.
- **Exploitation:** Before the test occurs, it should be determined whether exploits will be attempted if vulnerable systems are found. This is intentionally included in some cases so the incident response plan can be tested.
- **Communication:** Another of the issues in the rules of engagement is how communications are to occur between the tester and the stakeholders as the process unfolds. While regular meetings should be scheduled, there also must be a line of communication established for times when issues arise and changes may need to be made.
- **Reporting:** The type of reports to be generated is determined during the establishment of the rules of engagement. This includes the timing of reports, the format, and the specific information to be included. While postponing of reports should be allowed, it should not be allowed to become chronic, and the rules of engagement may include both incentives and penalties for the timelessness of reports.

Reverse Engineering

Reverse engineering is a term that has been around for some time. Generically, it means taking something apart to discover how it works and perhaps to replicate it. In cybersecurity, it is used to analyze both hardware and software and for various other reasons, such as to do the following:

- Discover how malware functions
- Determine whether malware is present in software
- Locate software bugs
- Locate security problems in hardware

The following sections look at the role of reverse engineering in cybersecurity analysis.

Isolation/Sandboxing

You may be wondering what the concepts of isolation and sandboxing are doing in a section on reverse engineering. How can you analyze malware without suffering the effects of the malware? The answer is to place the malware where it is safe to probe it and play with it. This is done by isolating, or sandboxing, the malware. You can

use a sandbox to run a possibly malicious program in a safe environment so that it doesn't infect the local system.

By using sandboxing tools, you can execute malware executable files without allowing the files to interact with the local system. Some sandboxing tools also allow you to analyze the characteristics of an executable. There are cases when this is not possible because malware can be specifically written to do different things if it detects that it's being executed in a sandbox.

In many cases, sandboxing tools operate by sending a file to a special server that analyzes the file and sends you a report on it. Sometimes this is a free service, but in many instances it is not. Some examples of these services include the following:

- Sandboxie
- Akana
- Binary Guard True Bare Metal
- BitBlaze Malware Analysis Service
- Comodo Automated Analysis System and Valkyrie
- Deepviz Malware Analyzer
- Detux Sandbox (Linux binaries)

Another option for studying malware is to set up a sheep dip computer. This is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware. You can take measures such as the following on a sheep dip system:

- Install port monitors to discover ports used by the malware.
- Install file monitors to discover what changes may be made to files.
- Install network monitors to identify what communications the malware may attempt.
- Install one or more antivirus programs to perform malware analysis.

Often these sheep dip systems are combined with antivirus sensor systems to which malicious traffic is reflected for analysis.

The safest way to perform reverse engineering and malware analysis is to prepare a test bed. Doing so involves the following steps:

Step 1. Install virtualization software on the host.

Step 2. Create a VM and install a guest operating system on the VM.

Step 3. Isolate the system from the network by ensuring that the NIC is set to "host" only mode.

Step 4. Disable shared folders and enable guest isolation on the VM.

Step 5. Copy the malware to the guest operating system.

Also, you need isolated network services for the VM, such as DNS. It may also be beneficial to install multiple operating systems in both patched and non-patched configurations. Finally, you can make use of virtualization snapshots and re-imaging tools to wipe and rebuild machines quickly.

Once the test bed is set up, you also need to install a number of other tools to use on the isolated VM, including the following:

- **Imaging tools:** You need these tools to take images for forensics and prosecution procedures. Examples include Safe Back Version 2.0 and DD (which is covered in Chapter 14).
- **File/data analysis tools:** You need these tools to perform static analysis of potential malware files. Examples include PE Studio and PEframe.
- **Registry/configuration tools:** You need these tools to help identify infected settings in the registry and to identify the last saved settings. Examples include Microsoft's Sysinternals Autoruns and Silent Runners.vbs.
- **Sandbox tools:** You need these tools for manual malware analysis (listed earlier in this chapter, the "Isolation/Sandboxing" section)
- **Log analyzers:** You need these tools to extract log files. Examples include AWStats and Apache Log Viewer.
- **Network capture tools:** You need these tools to understand how the malware uses the network. Examples include Wireshark and Omnipeek.

While the use of virtual machines to investigate the effects of malware is quite common, you should know that some well-written malware can break out of a VM relatively easily, making this approach problematic.

Hardware

You must be concerned with the safety and the integrity of the hardware that you purchase. The following are some of the methods used to provide this assurance:

- **Source authenticity of hardware:** When purchasing hardware to support any network or security solution, a security professional must ensure that the hardware's authenticity can be verified. Just as expensive consumer items such as

purses and watches can be counterfeited, so can network equipment. While the dangers with counterfeit consumer items are typically confined to a lack of authenticity and potentially lower quality, the dangers presented by counterfeit network gear can extend to the presence of backdoors in the software or firmware. Always purchase equipment directly from the manufacturer when possible, and when purchasing from resellers, use caution and insist on a certificate of authenticity. In any case where the price seems too good to be true, keep in mind that it may be an indication the gear is not authentic.

- **Trusted Foundry:** The Trusted Foundry program can help you exercise care in ensuring the authenticity and integrity of the components of hardware purchased from a vendor. This DoD program identifies "trusted vendors" and ensures a "trusted supply chain." A trusted supply chain begins with trusted design and continues with trusted mask, foundry, packaging/assembly, and test services. It ensures that systems have access to leading-edge integrated circuits from secure, domestic sources. At the time of this writing, 77 vendors have been certified as trusted.
- **OEM documentation:** One of the ways you can reduce the likelihood of purchasing counterfeit equipment is to insist on the inclusion of verifiable original equipment manufacturer (OEM) documentation. In many cases, this paperwork includes anti-counterfeiting features. Make sure to use the vendor website to verify all the various identifying numbers in the documentation.

Software/Malware

Software of any type can be checked for integrity to ensure that it has not been altered since its release. Checking for integrity is one of the ways you can tell when a file has been corrupted (or perhaps replaced entirely) with malware. Two main methods are used in this process:

- **Fingerprinting/hashing:** Fingerprinting, or hashing, is the process of using a hashing algorithm to reduce a large document or file to a character string that can be used to verify the integrity of the file (that is, whether the file has changed in any way). To be useful, a hash value must have been computed at a time when the software or file was known to have integrity (for example, at release time). Then at any time thereafter, the software file can be checked for integrity by calculating a new hash value and comparing it to the value from the initial calculation. If the character strings do not match, a change has been made to the software.

  Fingerprinting/hashing has been used for some time to verify the integrity of software downloads from vendors. The vendor provides the hash value and specifies the hash algorithm, and the customer recalculates the hash value after

the download. If the result matches the value from the vendor, the customer knows the software has integrity and is safe.

Anti-malware products also use this process to identify malware. The problem is that malware creators know this, and so they are constantly making small changes to malicious code to enable the code to escape detection through the use of hashes or signatures. When they make a small change, anti-malware products can no longer identify the malware, and they won't be able to until a new hash or signature is created by the anti-malware vendor. For this reason, some vendors are beginning to use "fuzzy" hashing, which looks for hash values that are similar but not exact matches.

- **Decomposition:** Decomposition is the process of breaking something down to discover how it works. When applied to software, it is the process of discovering how the software works, perhaps who created it, and, in some cases, how to prevent the software from performing malicious activity.

  When used to assess malware, decomposition can be done two ways: statically and dynamically. When static or manual analysis is used, it takes hours per file and uses tools called disassemblers. Advanced expertise is required. Time is often wasted on repetitive sample unpacking and indicator extraction tasks.

  With dynamic analysis tools, an automated static analysis engine is used to identify, de-archive, de-obfuscate, and unpack the underlying object structure. Then proactive threat indicators (PTI) are extracted from the unpacked files. A rules engine classifies the results to calculate the threat level and to route the extracted files for further analysis. Finally, the extracted files are repaired to enable further extraction or analysis with a sandbox, decompiler, or debugger. While the end result may be the same, these tools are much faster and require less skill than manual or static analysis.

Training and Exercises

Security analysts must practice responding to security events in order to react to them in the most organized and efficient manner. There are some well-established ways to approach this. This section looks at how teams of analysts, both employees and third-party contractors, can be organized and some well-established names for these teams.

Security posture is typically assessed by war game exercises in which one group attacks the network while another attempts to defend the network. These games typically have some implementation of the following teams:

Key Topic

- **Red team:** The Red team acts as the attacking force. It typically carries out penetration tests by following a well-established process of gathering

information about the network, scanning the network for vulnerabilities, and then attempting to take advantage of the vulnerabilities. The actions they can take are established ahead of time in the *rules of engagement*. Often these individuals are third-party contractors with no prior knowledge of the network. This helps them simulate attacks that are not inside jobs.

- **Blue team:** The Blue team acts as the network defense team, and the attempted attack by the Red team tests the Blue team's ability to respond to the attack. It also serves as practice for a real attack. This includes accessing log data, using a SIEM, garnering intelligence information, and performing traffic and data flow analysis.
- **White team:** The White team is a group of technicians who referee the encounter between the Red team and the Blue team. Enforcing the rules of engagement might be one of the White team's roles, along with monitoring the responses to the attack by the Blue team and making note of specific approaches employed by the Red team.

Risk Evaluation

Although penetration testing can identify vulnerabilities, it is not the recommended way to identify vulnerabilities. An organization should have a well-defined risk management process in place that includes the evaluation of risk that is present. When this process is carried out properly, *threat modeling* allows organizations to identify threats and potential attacks and implement the appropriate mitigations against these threats and attacks. These facets ensure that any security controls implemented are in balance with the operations of the organization. The three parts to this process are covered in the following sections.

Technical Impact and Likelihood

Once all assets have been identified and their value to the organization has been established, specific threats to each asset are identified. An attempt must be made to establish both the likelihood of the threat's realization and the impact to the organization if it occurs. While both quantitative and qualitative risk assessments may be performed, when a qualitative assessment is conducted, the risks are placed into the following categories:

- High
- Medium
- Low

Typically, a risk assessment matrix, such as the one in Figure 4-2, is created. Subject experts grade all risks based on their likelihood and impact. This helps prioritize the application of resources to the most critical vulnerabilities.

Key Topic

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

Figure 4-2 Risk Assessment Matrix

Technical Control Review

Technical controls are implemented with technology and include items such as firewalls, access lists, permissions on files and folders, and devices that identify and prevent threats. After it understands the threats, an organization needs to establish likelihoods and impacts, and it needs to select controls that, while addressing a threat, do not cost more than the cost of the realized threat. The review of these controls should be an ongoing process.

Operational Control Review

Operational controls are the policies, procedures, and work practices that either help prevent a threat or make the threat more likely. The review of these controls should be an ongoing process.

Exam Preparation Tasks

As mentioned in the section "Strategies for Exam Preparation" in the Introduction, you have a couple choices for exam preparation: the exercises here, Chapter 15, "Final Preparation," and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 4-2 lists these key topics and the page number on which each is found.

Key Topic

Table 4-2 Key Topics in Chapter 4

Key Topic Element	Description	Page Number
Step List	Steps in a penetration test	99
List	Strategies for pen testing	99
List	Pen test categories	99
List	Rules of engagement	100
List	Security teams	105
Figure 4-2	Risk assessment matrix	107

Define Key Terms

Define the following key terms from this chapter and check your answers against the glossary:

penetration testing, blind test, double-blind test, target test, zero-knowledge test, partial-knowledge test, full-knowledge test, rules of engagement, reverse engineering, isolation, sandboxing, sheep dip computer, imaging tools, file/data analysis tools, registry/configuration tools, sandbox tools, log analyzers, network capture tools, Trusted Foundry, fingerprinting/hashing, decomposition, Red team, Blue team, White team, risk evaluation, risk assessment matrix, technical control review, operational control review

Review Questions

1. Which of following attempts to exploit vulnerabilities?
   a. Vulnerability test
   b. Pen test
   c. Risk assessment
   d. Port scan

2. Which of the following is the third step in a pen test?
   a. Analysis and reporting
   b. Vulnerability detection
   c. Penetration attempt
   d. Cleaning up

3. In which type of test are both the testing team and the organization's security team given maximum information about the network and the type of test that will occur?
   a. Blind test
   b. Double-blind test
   c. Target test
   d. External test

4. In which of the following is the testing team provided with public knowledge regarding the organization's network?
   a. Zero-knowledge test
   b. Partial-knowledge test
   c. Full-knowledge test
   d. Target test

5. Which of the following rules of engagement includes a list of all devices that are included in the test as well as a description of all testing methodologies to be used?
   a. Timing
   b. Scope
   c. Authorization
   d. Exploitation

6. Which of the following practices places malware where it is safe to probe it and play with it?
   a. Sandboxing
   b. Compartmentalizing
   c. Boundary enforcement
   d. File locks

7. Which of the following is a system that has been isolated from other systems and is used for analyzing suspect files and messages for malware?
   a. Sheep dip computer
   b. Virtual machine
   c. Sandbox
   d. Honeypot

8. Which of the following is a good example of exercising care in ensuring the authenticity and integrity of the components of hardware purchased from a vendor?
   a. Trusted Foundry program
   b. Fingerprinting
   c. Hashing
   d. Decomposition

9. Which of the following is the process of taking a large document or file and, with the use of a hashing algorithm, reducing the file to a character string that can be used to verify the integrity of the file?
   a. Hashing
   b. Decomposing
   c. Sandboxing
   d. Reverse engineering

10. Which of the following helps prioritize the application of resources to the most critical vulnerabilities?
    a. Access control matrix
    b. Risk assessment matrix
    c. PERT chart
    d. Gantt chart

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z