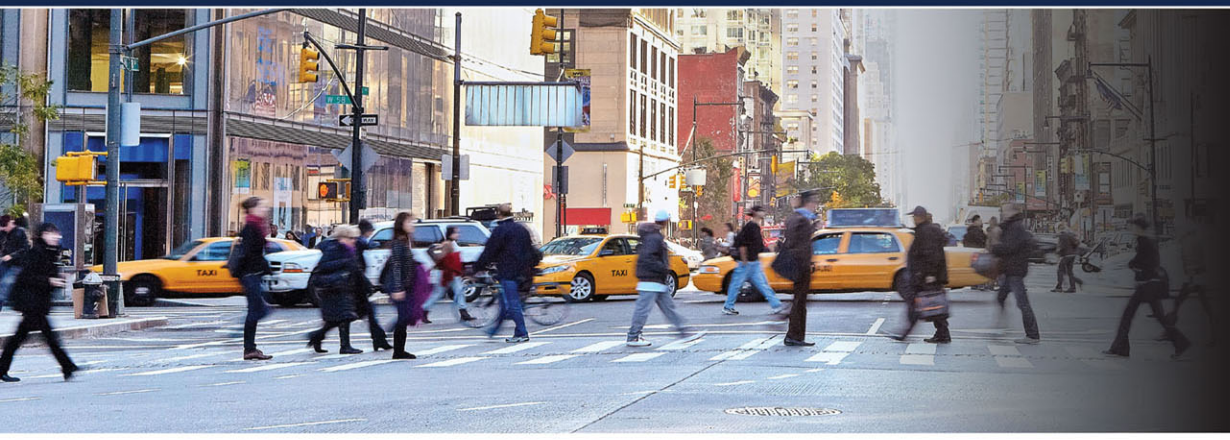
Official Cert Guide



Practice Tests

Flash Cards

Study Planner

Review Exercises

Cisco Certified Support Technician (CCST) Cybersecurity

100-160

Shane Sexton
Raymond Lacoste

ciscopress.com

FREE SAMPLE CHAPTER

Cisco Certified Support Technician (CCST) Cybersecurity 100-160 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the **print book ISBN:** 9780138203924.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

This page intentionally left blank

Cisco Certified Support Technician (CCST) Cybersecurity

100-160

Official Cert Guide

SHANE SEXTON
RAYMOND LACOSTE

Cisco Press

Cisco Certified Support Technician (CCST) Cybersecurity 100-160 Official Cert Guide

Shane Sexton and Raymond Lacoste

Published by Cisco Press

Hoboken, New Jersey

$PrintCode

Library of Congress Control Number: 2023951714

ISBN-13: 978-0-13-820392-4

ISBN-10: 0-13-820392-X

Warning and Disclaimer

This book is designed to provide information about the Cisco Certified Support Technician (CCST) Cybersecurity 100-160 exam. 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 is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. 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 discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., 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.

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

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Special Sales

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

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

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

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Alliances Manager, Cisco Press: Caroline Antonio

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Senior Project Editor: Tonya Simpson

Copy Editor: Kitty Wilson

Technical Editor: Russell Long

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Barbara Mack

Please contact us with concerns about any potential bias at www.pearson.com/report-bias.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go**

About the Authors

Shane Sexton has spent years learning and teaching all things IT. He holds CCNP Security, CND, CySA+, CCNA CyberOps, and numerous other certifications and has prepared thousands of students to take these exams. Shane earned bachelor's degrees in technology management and liberal studies (and wishes he'd taken fewer philosophy classes). He currently works as a network and system administrator at an MSP, where every day brings new learning opportunities. When he's not tackling IT emergencies, Shane practices piano, reads anything nonfiction, and expertly avoids family members with printer issues. He currently resides in Phoenix, Arizona, with three cats who have no respect for his property or the rule of law.

Raymond Lacoste has dedicated his career to developing the skills of those interested in IT. In 2001, he began to mentor hundreds of IT professionals pursuing their Cisco certification dreams. This role led to teaching Cisco courses full time. Raymond is currently a master instructor for Cisco Enterprise Routing and Switching, AWS, ITIL, and Cybersecurity at Stormwind Studios. Raymond treats all technologies as an escape room, working to uncover every mystery in the protocols he works with. Along this journey, Raymond has passed more than 120 exams, and his office wall includes certificates from Microsoft, Cisco, ISC2, ITIL, AWS, and CompTIA. If you were visualizing Raymond's office, you'd probably expect the usual network equipment, certifications, and awards. Those certainly take up space, but they aren't his pride and joy. Most impressive, at least to Raymond, is his gemstone and mineral collection; once he starts talking about it, he just can't stop. Who doesn't get excited by a wondrous barite specimen in a pyrite matrix? Raymond presently resides with his wife and two children in eastern Canada, where they experience many adventures together.

About the Technical Reviewer

The first time **Russell Long** opened a computer in the late 1980s was to install the latest and greatest technology of the time: a sound card. That interest later turned into a profession. Since then, he's held 13 different IT certifications in addition to a CCSI. All these years later, he still finds himself digging into computer technologies and doing his best to optimize them. He's on the tail end of his second decade of working in IT and working toward his second decade of instructing and teaching IT. Russell's favorite IT disciplines include networking (wireless included), security, and virtualization. He hopes to pass on the information he has learned to those looking to make a career in IT.

Dedications

Shane Sexton:

I'd like to dedicate this book to everyone who has supported and mentored me over the years. Dan Young and the entire Stormwind Studios crew have fostered a fun and supportive environment where I nerded out for a living. I also dedicate this book to my mom, who's been in my corner during life's ups and downs and has always been my cheerleader. And to Ashley, for the many times she's held me up, for learning to "adult" together, and for all the good memories we've made on the way. Thank you all!

Raymond Lacoste:

To my beloved daughter Rylie,

Your presence in my life has enriched it in countless ways, and I'm eternally thankful for the love, joy, and inspiration you bring to our entire family. You have an infectious personality that is filled with compassion, thoughtfulness, and caring that will continue to light up the lives of those fortunate enough to know you.

Rylie, this book is dedicated to you as a symbol of my hopes and dreams for your future. Your presence in my life has inspired me to reach for the stars. May this book be a source of empowerment as you continue to grow and conquer new horizons. Always remember that you are capable of achieving greatness, and my love and support will be with you every step of the way.

Love,

Daddy

Acknowledgments

Shane Sexton:

Thanks to James, Ellie, Brett, and everyone else at Cisco Press. It has been an absolute pleasure to work with you, and I appreciate your patience and help while I learned the ropes. A giant thank you to Raymond Lacoste, who mentored me as a new instructor and now as a new author. Finally, an extra-giant thanks to Russ Long, for opening this unexpected door for me, for your excellent technical review, and for being a solid friend.

Raymond Lacoste:

A huge thank you to Shane for bringing me along on this writing adventure. Combining our skills and knowledge for this book was the right decision. Shane, keep on being amazing!

Thanks to James, Ellie, Brett, Tonya, Kitty, and everyone else who made this book come to life. Without the amazing team behind the scenes, this book would be a bunch of virtual crumpled-up pieces of paper on the floor surrounding a wastepaper basket. So, THANK YOU for taking our garbage and making it useful! :)

To Russ Long, a great trusted friend who has been by my side for 10+ years on many projects. Russ, you are an amazing person. Thank you for always being there for me.

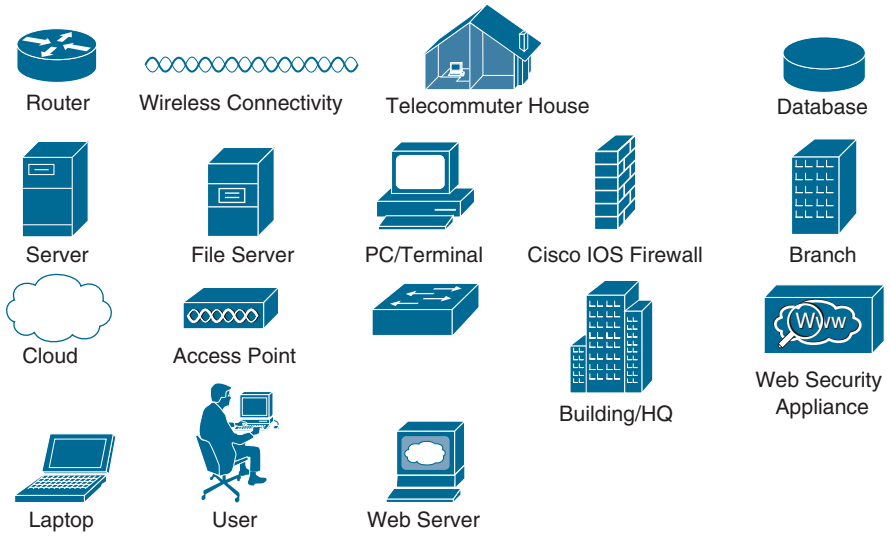
And finally, a big thank you to my family, who supported me through the ups and downs. Without you, this book would not have happened.

Contents at a Glance

Online Elements

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Congratulations! If you are reading this introduction, then you have probably decided that security is an important part of your future success and that obtaining security certifications will prove that you have a solid understanding of security related topics and concepts.

Professional certifications have been an important part of the computing industry for many years and will continue to be important for years to come. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other qualifications being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified.

So, this book was written to help anyone from up-and-coming IT professionals to veterans of the IT industry build a solid foundational understanding of cybersecurity. This book is structured specifically to prepare candidates for the CCST Cybersecurity (100-160) exam but aims to equip you with knowledge that will remain useful long after you earn the certification.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CCST Cybersecurity (100-160) exam. In fact, if the primary objective of this book were different, then the book's title would be misleading; however, the methods used in this book to help you pass the CCST Cybersecurity exam are designed to also make you much more knowledgeable about how to do your job. While this book has more than enough questions to help you prepare for the actual exam, the goal isn't to have you simply memorize as many questions and answers as you possibly can.

In this book, we help you discover the exam topics that you need to review in more depth, help you fully understand and remember those details, and help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass by memorization but helps you truly learn and understand the topics.

The knowledge the CCST Cybersecurity exam covers is vital for any cybersecurity professional. This book would do you a disservice if it didn't attempt to help you learn the material. To that end, this book helps you pass the CCST Cybersecurity exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process

Who Should Read This Book?

This book is geared toward new IT professionals and those with an interest in learning about cybersecurity; however, veteran IT professionals just getting into security or needing to obtain the certification will benefit as well. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exam.

So why should you want to pass the CCST Cybersecurity exam? Earning the certification validates your understanding of core cybersecurity concepts and techniques. Furthermore, the CCST Cybersecurity certification serves as a springboard to more advanced certifications down the road. Many of the concepts and themes we introduce here are practically universal in cybersecurity exams.

Strategies for Exam Preparation

The strategy you use to prepare for the CCST Cybersecurity exam might be slightly different from the strategies used by other readers, mainly depending on the skills, knowledge, and experience you have already obtained. For instance, if you are already familiar with security concepts and techniques, your approach will likely differ from that of a person who is brand new to cybersecurity.

Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about access management if you fully understand it already. However, many people like to make sure that they truly know a topic and thus read over material that they already know. Several book features will help you gain the confidence you need to be convinced that you know some material already and to also help you know what topics you need to study more.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

How to Access the Companion Website

To access the companion website, which gives you access to the electronic content for this book, start by establishing a login at ciscopress.com and register your book. To do so, simply go to ciscopress.com/register and enter the ISBN of the print book: 9780138203924. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page.

Simply go to your account page, click the Registered Products tab, and select Access Bonus Content to access the book's companion website.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book or bookseller eBook versions:** You can get your access code by registering the print ISBN 9780138203924 on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click Account to see details of your account, and click the digital purchases tab.

NOTE Do not lose the activation code because it is the only means with which you can access the QA content with the book.

When you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website, as shown earlier in this Introduction under the heading "How to Access the Companion Website.

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. Chapters 1 through 15 are the core chapters and can be covered in any order. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 1 through 15, cover the following topics:

- **Chapter 1, "Security Principles":** This chapter introduces core security concepts such as the CIA triad, vulnerabilities, threats, and risk. It also covers different types of attackers and common defensive measures.

- **Chapter 2, "Common Threats, Attacks, and Vulnerabilities":** This chapter discusses vulnerabilities and attacks that target hosts and networks. It also addresses the most common social engineering attacks, which target people.
- **Chapter 3, "Access Management":** This chapter covers authentication, authorization, and accounting (AAA). It describes various authentication mechanisms that can be used with AAA and concludes with an introduction to a common AAA protocol called RADIUS.
- **Chapter 4, "Cryptography":** This chapter introduces the basics of cryptography: its vocabulary, symmetric and asymmetric algorithms, and common applications of each.
- **Chapter 5, "Introduction to Networking, Addressing, and TCP/IP Protocols":** This chapter provides a crash course in networking. It introduces you to the OSI model and the TCP/IP stack. In addition, it provides you with an understanding of common TCP/IP protocols and their vulnerabilities. To wrap up, the chapter discusses network addressing and its impact on security.
- **Chapter 6, "Network Infrastructure":** This chapter discusses architectural concepts and commonly used network appliances. It introduces demilitarized zones (DMZs) and their uses and considerations for virtualized and cloud environments. It also describes common network appliances, such as proxies, honeypots, and intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).
- **Chapter 7, "Controlling Network Access":** This chapter describes how network traffic can be shielded and controlled. It begins with a description of virtual private networks (VPNs) and their use cases. Next, it explains firewalls and access control lists (ACLs). The chapter concludes with a description of network access control (NAC), which grants extensive control over the devices allowed on your networks.
- **Chapter 8, "Wireless SOHO Security":** This chapter introduces how small office/home office (SOHO) wireless devices are secured. It describes the administrative interface, wireless encryption standards, and authentication mechanisms. Other considerations, such as the SSID, MAC address filtering, and firmware updates, are also covered. The chapter concludes by describing common attacks against wireless networks.
- **Chapter 9, "Operating Systems and Tools":** This chapter introduces common operating systems, such as Windows, macOS, and Linux. For each operating system, this chapter describes integrated security features. The chapter concludes by covering common security tools used on endpoints.
- **Chapter 10, "Endpoint Policies and Standards":** This chapter discusses various management considerations for endpoint devices. It begins with an introduction to asset inventories and their importance. Then it covers ubiquitous management tasks such as program deployment and data backups. The chapter concludes by describing bring your own device (BYOD) and regulatory considerations.
- **Chapter 11, "Network and Endpoint Malware Detection and Remediation":** This chapter introduces antimalware technologies. It describes how malware signatures

work, different approaches to scanning, and Cisco's Advanced Malware Protection (AMP) technology. The chapter finishes with some best practices for malware remediation.

- **Chapter 12, "Risk and Vulnerability Management":** This chapter covers vulnerabilities and risk in more detail. It begins with a description of vulnerability management processes, tools, and techniques. Then it explains the broader topics of risk prioritization and management.
- **Chapter 13, "Threat Intelligence":** This chapter discusses threat intelligence, its sources, and its benefits. It describes intelligence sources such as vulnerability feeds, reports, and news articles. Then it covers collective and automated approaches to threat intelligence and the basics of Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII). The chapter concludes with a look at why sharing threat intelligence is beneficial.
- **Chapter 14, "Disaster Recovery and Business Continuity":** This chapter looks at how businesses plan for, survive, and recover from catastrophic events. It describes disaster recovery plans (DRPs), business impact analyses (BIAs), and business continuity plans (BCPs) and explores their similarities, differences, and relationships.
- **Chapter 15, "Incident Handling":** This chapter introduces what incidents are and discusses NIST's four phases of incident response. It also describes several attack frameworks (ways of thinking about attacks) and basic forensic concepts such as data volatility and chain of custody. The chapter ends with a discussion of how regulations impact the incident response process.

Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret; however, we do know which topics you must know to *successfully* complete this exam. Cisco publishes them as an exam blueprint for Implementing CCST Cybersecurity (100-160). Table I-1 lists each exam topic listed in the blueprint along with a reference to the book chapter that covers the topic.

Table I-1 CCST Cybersecurity (100-160) Topics and Chapter References

CCST Cybersecurity	Chapter(s) in Which Topic Is Covered
1. Essential Security Principles	
1.1. Define essential security principles	1
1.2. Explain common threats and vulnerabilities	2
1.3. Explain access management principles	3
1.4. Explain encryption methods and applications	4
2. Basic Network Security Concepts	
2.1. Describe TCP/IP protocol vulnerabilities	5
2.2. Explain how network addresses impact network security	5

CCST Cybersecurity	Chapter(s) in Which Topic Is Covered
2.3. Describe network infrastructure and technologies	6
2.4. Set up a secure wireless SoHo network	8
2.5. Implement secure access technologies	7
3. Endpoint Security Concepts	
3.1. Describe operating system security concepts	9
3.2. Demonstrate familiarity with appropriate endpoint tools that gather security assessment information	9
3.3. Verify that endpoint systems meet security policies and standards	10
3.4. Implement software and hardware updates	9
3.5. Interpret system logs	9
3.6. Demonstrate familiarity with malware removal	11
4. Vulnerability Assessment and Risk Management	
4.1. Explain vulnerability management	12
4.2. Use threat intelligence techniques to identify potential network vulnerabilities	13
4.3. Explain risk management	12
4.4. Explain the importance of disaster recovery and business continuity planning	14
5. Incident Handling	
5.1. Monitor security events and know when escalation is required	15
5.2. Explain digital forensics and attack attribution processes	15
5.3. Explain the impact of compliance frameworks on incident handling	15
5.4. Describe the elements of cybersecurity incident response	15

The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified cybersecurity professional.

It is also important to understand that this book is a "static" reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.

This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information available at Cisco.com that covers each topic in great detail. If you think you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as cybersecurity technologies continue to develop, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics

in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, hovering over Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book at http://www.ciscopress.com/title/9780138203924. It's a good idea to check the website a couple of weeks before taking your exam to be sure that you have up-to-date content.

Taking the CCST Cybersecurity Certification Exam

As with any Cisco certification exam, you should strive to be thoroughly prepared before taking the exam. There is no way to determine exactly what questions are on the exam, so the best way to prepare is to have a good working knowledge of all subjects covered on it. Schedule the exam and be sure to be rested and ready to focus when taking it.

The best place to find out the latest available Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking Your Status

You can track your certification progress by checking http://www.cisco.com/go/certifications/login. You must create an account the first time you log in to the site.

How to Prepare for an Exam

The best way to prepare for any certification exam is to use a combination of the preparation resources, labs, and practice tests. This guide has integrated some practice questions and example scenarios to help you better prepare. If possible, get some hands-on experience with Cisco Cybersecurity equipment. There is no substitute for real-world experience.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent 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.

Cisco Cybersecurity Certifications in the Real World

Cisco has one of the most recognized names on the Internet. People with a Cisco Certified Support Technician (CCST) Cybersecurity certification can bring quite a bit of

knowledge to the table because of their deep understanding of cybersecurity technologies and standards. This is why the Cisco certification carries such high respect in the marketplace. Cisco certifications demonstrate to potential employers and contract holders a certain professionalism, expertise, and dedication required to complete a difficult goal. If Cisco certifications were easy to obtain, everyone would have them.

Exam Registration

The Cisco Certified Support Technician (CCST) Cybersecurity 100-160 exam is a computer-based exam, with around 50 to 70 multiple-choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (http://www.pearsonvue.com) testing center. According to Cisco, the exam should last about 50 minutes. Be aware that when you register for the exam, you might be told to allow a certain amount of time to take the exam that is longer than the testing time indicated by the testing software when you begin. This discrepancy is because the testing center will want you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco occasionally updates exam topics without notice, Cisco Press might post additional preparatory content on the web page associated with this book at http://www.ciscopress.com/title/9780138203924. It is a good idea to check the website a couple of weeks before taking your exam, to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Cisco Press website to view any errata or supporting book files that might be available.

Figure Credits

Figures 4.1, 4.7, 9.1–9.8: Microsoft Corporation

Figures 9.9, 9.12, 9.15: Red Hat, Inc

Figure 9.10: Canonical Ltd

Figures 9. 13, 9.14, 11.2: Apple Inc

Figure 9.16: Wireshark

Figure 11.3: Sophos Ltd

Figure 12.3: Tenable, Inc

Figure 12.4: Nmap Software LLC

Figure 13.1: The National Institute of Standards and Technology

CHAPTER 3

Access Management

This chapter covers the following topics:

- **Introduction to AAA:** This section introduces you to the importance of AAA.
- **Authentication:** This section focuses on the various factors of authentication, the need for MFA, as well as passwords and password policies.
- **Authorization:** This section explores the need for authorization.
- **Accounting:** This section explores the need for accounting.
- **RADIUS:** This section examines the need for RADIUS and provides some sample use cases.

To provide confidentiality, integrity, and availability, you must be able to granularly control access to all resources and ensure that the access controls are upheld at all times. If the access controls ever break down, legitimate or non-legitimate users, applications, or services will have access to resources they should not have access to.

To provide an access management solution that maintains the appropriate levels of confidentiality, integrity, and availability, you must consider the AAA framework, which outlines the best practices you need to consider when it comes to authentication, authorization, and accounting.

This chapter introduces the AAA framework. It first focuses on authentication, MFA, and password policies. It then moves on to covering authorization, followed by accounting. It wraps up by examining a AAA service known as RADIUS.

This chapter covers information related to the following Cisco Certified Support Technician (CCST) Cybersecurity exam objective:

1.3. Explain access management principles.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Introduction to AAA	1
Authentication	2
Authorization	3
Accounting	4
RADIUS	5

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question incorrect for purposes of self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following correctly defines AAA?
   - **a.** A client/server protocol used for authentication, authorization, and accounting
   - **b.** The process of verifying that someone or something is in fact truly who they say they are
   - **c.** A framework that helps build the controls needed to access computing resources, enforce policies, and audit usage
   - **d.** A type of MFA that encourages three factors
2. Which of the following correctly defines authentication?
   - **a.** The process of adopting the least-privilege principle, the need-to-know principle, and the implicit-deny principle
   - **b.** The process of granting privileges and controlling what a user is able to do
   - **c.** The process of monitoring, recording, and auditing everything in an organization
   - **d.** The process of verifying that someone or something is in fact truly who they say they are
3. Which of the following correctly defines authorization?
   - **a.** The process of monitoring, recording, and auditing everything in an organization
   - **b.** The process of granting privileges and controlling what a user is able to do
   - **c.** The process of verifying that someone or something is in fact truly who they say they are
   - **d.** The process of collecting, consolidating, and correlating log files
4. Which of the following correctly defines accounting?
   - **a.** The process of using biometrics to allow access to a system
   - **b.** The process of verifying that someone or something is in fact truly who they say they are

c. The process of granting privileges and controlling what a user is able to do

d. The process of monitoring, recording, and auditing everything in an organization

5. What is RADIUS?

a. A client/server protocol used for accounting only

b. A client/server protocol used for authentication only

c. A client/server protocol used for authentication and authorization only

d. A client/server protocol used for authentication, authorization, and accounting

Foundation Topics

Introduction to AAA

Key Topic

AAA, which is pronounced "triple A" and stands for *authentication, authorization, and accounting*, is a framework. A framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. The AAA framework is a guide that helps you build the controls needed to access computing resources, enforce policies, and audit usage. AAA plays a very important role in security.

Authentication is about verifying the identity of those who access your systems and data. Therefore, without authentication, you can't control access to your data, and so you can't protect confidentiality, integrity, and availability (CIA). Authorization is about controlling what can be done to your systems and data. Therefore, without authorization, you can't control what can be done with your data, and so you can't protect CIA. Accounting is about recording everything that is happening to your systems and data. Therefore, without accounting, you can't keep track of the who, what, where, when, why, and how of your data, and so you can't protect CIA.

As you can see, without AAA, it is impossible to meet the CIA needs of your organization.

Authentication

Key Topic

Authentication is about proving the identity of someone or something, or verifying that someone or something is in fact truly who they say they are. Why do I say "someone or something"? Well, *someone* refers to a person, and *something* refers to anything else that needs to be authenticated. Keep in mind that systems, devices, tools, applications, and so on need to be authenticated. If you are only focused on people, you are leaving your organization vulnerable to attack.

There are a multitude of factors that people, systems, devices, applications, and tools can use to authenticate. Table 3-2 explores these factors and provides examples.

Key Topic

Table 3-2 Authentication Factors

Factor	Description	Examples
Something you know	This is authentication based on knowledge.	A username, a password, a personal identification number (PIN) you have memorized, a passphrase you have memorized, CAPTCHA test, personal verification questions

Factor	Description	Examples
Something you have	This is authentication based on possession.	A security token that can provide you with a random PIN A random PIN, passphrase, or notification from your smartphone that you can accept or reject A swipe card, tap card, or passkey
Something you are	This is authentication based on unique aspects of yourself and relies on biometrics.	Your fingerprint, your facial geometry, your retina, your palm print
Somewhere you are	This is authentication based on location.	You are allowed or denied based on your connection to the corporate Wi-Fi versus coffee shop Wi-Fi versus airport Wi-Fi versus home Wi-Fi. You are allowed or denied based on your connection in the United States versus Canada versus any other country.
Something you do	This is authentication based on habits and characteristics.	The way you walk, the way you write, the way you talk, the path you take to work, the places you eat lunch, the sports you play and when
Time	This is authentication based on the time of day and/or day of the week.	You are allowed on the Internet between 9 a.m. and 5 p.m. and are not allowed on the Internet between 5 p.m. and 9 a.m. You are allowed to connect to the VPN Monday through Friday, 7 a.m. to 9 p.m. local time

Multifactor Authentication (MFA)

Using a single factor of authentication is no longer advisable. For example, relying on a username and password (a single factor: something you know) will not protect you as it once did. Cybercriminals have developed very creative ways to figure out your username and password (such as via a convincing phishing email), and once they know them, they will be able to access anything you can access with them. The same thing is true with PINs or passphrases that you have created and memorized. Once a cybercriminal has that information, they will have access to systems and data you don't want them to have access to.

Key Topic

One of the best ways to protect yourself today is with **multifactor authentication (MFA)**. MFA involves using two or more of the factors mentioned previously, in combination, to successfully authenticate (for example, combining something you know with something you have or combining something you have with something you are or combining something you have with somewhere you are). As of this writing, MFA is becoming closer to being the norm for every application and service that exists.

Now please note that MFA does not protect you from becoming the victim of a phishing attack that is designed to steal your credentials—or any other type of attack for that matter. It does, however, help prevent the cybercriminal from gaining access to your systems

and data based only on the credentials they stole in the phishing attack. How so? Well, even though they may have stolen your username and password, they do not have the second factor that is needed to successfully authenticate to the systems and access the data. For example, let's say your first factor is a username and password. Regardless of how strong the password is, it could be stolen/captured during a phishing attack or a data breach targeting your authentication database. If you have a second factor that is required, like a one-time PIN generated by an application installed on your cell phone that is valid for only 30 seconds, the cybercriminal will not be able to access your systems and data because they do not have your cell phone and can't get the one-time PIN—and they also can't guess it or brute force it because it changes every 30 seconds.

Table 3-3 provides examples of MFA.

Key Topic

Table 3-3 Examples of MFA

Factor 1	Factor 2	Description
Your bank card	A memorized PIN	Your bank card is one factor (something you have), and the PIN is the other factor (something you know).
A swipe card	A retinal scan	The swipe card is one factor (something you have), and the retinal scan is the other factor (something you are).
A username and a password	A notification sent to your phone that asks you to click yes or no	The username/password is one factor (something you know), and your phone with the notification is the other factor (something you have).
A fingerprint scan	A PIN	The fingerprint scan is one factor (something you are), and the PIN is the other factor (something you know).
A username and a password	Your location	Your username/password is one factor (something you know), and your location is the other factor (somewhere you are).

Please be aware that true multifactor authentication requires two or more different factors, as shown in Table 3-3. So, having a username/password and a memorized PIN is not MFA as they are both something you know—and so count as only one factor. A retinal scan and a fingerprint scan are not MFA as they are also the same factor (something you are). Having your phone that generates a PIN that you enter and then an app on your phone that gives you a one-time password is not MFA as these are, again, the same factor (something you have). These are all examples of **two-step authentication** because two steps are needed for authentication, but only a single factor is being used. What I want you to realize from this is that if you implement MFA poorly, you might not be as protected as you think you are, and you would do better with other combinations. For example, what would you consider to be stronger?

Option 1. A username/password and a six-digit one-time PIN generated at the time it is needed

Or

Option 2. A USB authentication key that needs to be entered into the system and then a notification displayed on your phone that needs to be accepted or rejected

So, option 1 is an example of MFA as there are two different factors in use, and option 2 is an example of two-step authentication because the same factor is used twice. In this case, it is clear that it would be much harder for the cybercriminal to access your system with two-step authentication (the USB key and your phone) as they would need physical access to both those devices and the system they are accessing. Although option 1 is a great option and highly recommended, you can see that strength comes from the combinations and not necessarily from just different factors being used. So, for the CCST Cybersecurity exam, be clear about the difference between MFA and two-step authentication in case you have to pick them out of a lineup.

Passwords and Password Policies

The most common way to authenticate today is with a username and password. Regardless of whether they are used as the only factor or as part of MFA or as part of two-step authentication, usernames and passwords are not going away anytime soon. Therefore, it is important to ensure that passwords meet certain requirements so that they are less apt to be easily guessed or determined using brute-force techniques and then reused by cybercriminals. In addition, they should be stored securely (hashed) in a database so that if the database is compromised, the likelihood of a cybercriminal being able to use any of the passwords in the database is significantly reduced.

So, what should a password be? It should be:

- Something that is not guessable
- Something that can't be brute forced
- Something that the user can remember without having to write it down
- Something that can be used for a long period of time

We used to encourage complexity by forcing users to include lowercase letters, uppercase letters, a digit, and special characters, but users would do the minimum to meet the requirements instead of creating complex passwords. For example, the password "password" would simply become "Password1!" which is not complex at all. We wanted them to use something like "Yt56R34w" but got "Password1!" instead. So, complexity requirements really haven't worked out as they were intended to and still result in passwords being guessable, brute forced, and written down.

Now we encourage length. The longer a password is, the harder it is to guess, and the harder it is to brute force. Users can now use passphrases or sentences for their passwords, which they can remember with ease without writing them down. For example, the password "We_Love_Oranges_And_Orange_Marmalade" is not easy to guess, it is impossible to brute force,

and the user will not have to write it down. In addition, it will not have to be changed for a long time.

So, what would be a good password policy today? A good password policy would

- Encourage length (12 characters minimum with no maximum).
- Encourage the use of passphrases or sentences (something easy to remember but really long).
- Force the use of an uppercase letter, a special character, and a number and allow the rest to be all lowercase.
- Increase the number of days between password changes to a year or more.

Now a user can create a password such as "B3ing_A_CCST_Cybersecurity_Is_Awesome!" which would meet all the requirements of the password policy and more while being impossible to guess or brute forced, and the user will not have to write it down. If they don't want to use the special character _, then it would still be acceptable to use "B3ingACCSTCybersecurityIsAwesome!". You could even omit the special character ! or the number, and this would still be a very safe password.

In addition, because of the length requirement, a user could use their password for a longer period of time. Instead of forcing users to change their passwords every 30 to 90 days, you could let them change it every year or even every few years. According to the website How Secure Is My Password, at https://www.security.org/how-secure-is-my-password/, it would take a computer about 1 hundred tredecillion years to crack (brute force) the password "B3ingACCSTCybersecurityIsAwesome!". So using this password for a few years without changing it should be fine.

When it comes to storing passwords in a database, it is imperative that you use hashing and salting. Hashing is done so that the password is stored as a hash instead of plaintext. This way, if the database is ever exfiltrated, the cybercriminal will get all the hashes but will have a very difficult time converting the hashes back into the plaintext passwords. (We cover hashing in Chapter 4, "Cryptography.") Salting is a way to ensure uniqueness when storing a password as a hash and reduce the chances of a rainbow table being successful. Without salting, if two people have exactly the same plaintext password, the hash that is stored in the database will be exactly the same. However, if a salt is added (for example, four or more extra random characters) during the hashing process, then those two plaintext passwords would produce two different hashes that would be stored in the database. These extra random characters make it impossible for a cybercriminal to obtain the passwords by using a rainbow table.

Don't forget that a lengthy password does not eliminate the need for MFA. If by chance a cybercriminal tricks you into giving them your password via a phishing attack, MFA will save you, and then once you discover that you have given up your password, you can change the password and sleep better knowing that the cybercriminal did not get into your account.

Authorization

Authorization is the process of granting and controlling what an authenticated user is able to do. It is focused on permissions. When it comes to permissions, you should adopt three principles:

- The **least-privilege principle**, which is about giving users only the minimum permissions they need to accomplish their objectives
- The **need-to-know principle**, which is about only giving users access to what they absolutely need to do their jobs and perform their roles
- The **implicit-deny principle**, which means everyone is prevented from doing everything unless they are explicitly allowed

If you are careless with authorization, your users could do something they should not (by accident or on purpose), resulting in risks associated with CIA. A cybercriminal could gain control of an account with more privileges than they should have and move vertically (within a system) or laterally (between systems) and exfiltrate data, which would compromise CIA. Therefore, it is imperative that you control exactly what each user can access by establishing policies and rules and adopting the least-privilege principle (only giving users minimum permissions they need to do their job), the need-to-know principle (only giving users access to what they need to know to do their job), and the implicit-deny principle (denying by default unless explicitly allowed).

Accounting

Accounting is about keeping track of who, what, where, when, why, and how. It is the process of monitoring, recording, and auditing everything in your organization. By keeping track of who accessed what data, where and when they accessed it, why they accessed it, and how they accessed it, you will be more aware and in tune with what is happening (good or bad) in and around your organization. For a security professional, this is one of the most important A's of AAA, yet many fail to implement an appropriate level of accounting, or if they do, they are overwhelmed by it and fail to continually follow up on what needs to be done with the collected information. Accounting generates a lot of logs, and the logs will be your window into the happenings within and around your network and resources. So, having a **security information and event management (SIEM)** solution as well as a **security orchestration, automation, and response (SOAR)** tool will definitely help you stay in the loop and focused on continually monitoring and protecting your network. A SIEM solution helps you collect logs, consolidate logs, correlate logs, and get notified about abnormalities/threats in logs that are in breach of established policies. A SOAR tool helps you automate responses and reduce the amount of human intervention when an abnormality/threat has been detected.

For example, say that your SIEM solution collects logs, consolidates logs, correlates logs, and notifies you, but you have to manually react and respond. So from the moment of notification to the successful completion of the response, there may be a significant amount of time lost. With the help of a SOAR tool, you might have scripts or the help of artificial intelligence (AI) and machine learning (ML) to immediately respond to the notifications and threats without human intervention.

RADIUS

Key Topic

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol originally designed to give remote users the ability to access services via dial-up connections. (If you don't know what dial-up is, it is because you are too young. Back in my early days, we did not have always-on broadband or fiber connections to the Internet; we had to use our telephone landlines to dial in to the Internet.) RADIUS was a service used for remote authentication with dial-up network access. Because of its flexibility, over time RADIUS has evolved and been adopted and adapted for other scenarios as well. Today it is a protocol we use with AAA for authentication, authorization, and accounting purposes.

The best way to learn about RADIUS is through an example of its use. Refer to Figure 3-1 as we go through the following example.

Key Topic

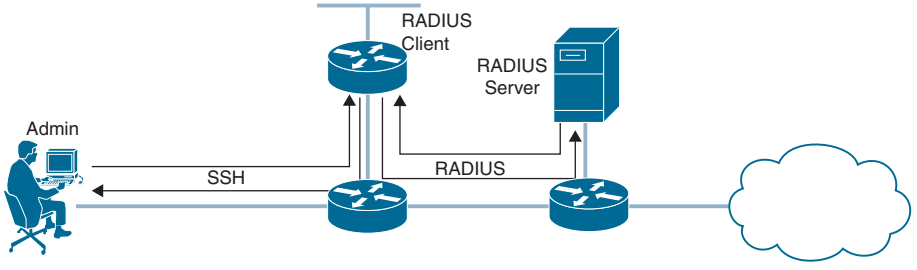


Figure 3-1 *Admin Using SSH to Manage a Router and Router Authenticating the Admin Using RADIUS*

On the right side of this figure is a RADIUS server. It is a server that contains a database of usernames and passwords, and it can communicate using the RADIUS protocol. You can implement RADIUS servers with several different options; in this example, we use Cisco Identity Services Engine (ISE). This is the server part of the client/server protocol.

In the middle of the figure is a router. This router is configured to communicate with the RADIUS server using the RADIUS protocol any time authentication needs to be performed. This is the client part of the client/server protocol.

Now focus on the left side of the figure, where you see the administrator of the router. The admin opens the SSH client and makes a connection to the router using SSH (port 22) for management purposes. They then need to provide their username and password to authenticate. When the router receives the username and password, it contacts the RADIUS server by using the RADIUS protocol so that the RADIUS server can determine if the admin is authenticated or not, based on the credentials provided. If the admin provided a username and password listed in the database, the RADIUS server tells the router to grant the admin access. If they did not provide a username and password listed in the database, the RADIUS server tells the router to deny the admin access.

With RADIUS, authentication and authorization happen at the same time. So, when the admin is being authenticated by the RADIUS server, the server can also be configured to tell the client (the router in Figure 3-1) what the user (the admin in Figure 3-1) is allowed and not allowed to do, based on a database of permissions that has been defined on the RADIUS

server. For example, in Figure 3-1, once the user authenticates, they may only be authorized to configure, verify, and troubleshoot routing protocols on the router. Or maybe they are authorized to only perform verification tasks and no configuration tasks.

As mentioned earlier, because of its flexibility, RADIUS can be used in many different scenarios. For example, Figure 3-2 shows a wireless user, a wireless access point, and the RADIUS server.

Key Topic

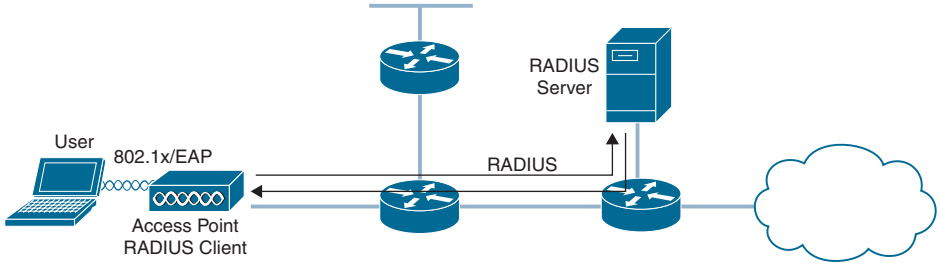


Figure 3-2 *Wireless User Authenticating to the Wireless Network Using 802.1x, EAP, and RADIUS*

For this scenario, the wireless user needs access to the network. When connecting, they provide their username and password to the wireless AP, using 802.1x and Extensible Authentication Protocol (EAP) messages. The wireless AP (RADIUS client) then sends those credentials to the RADIUS server, using the RADIUS protocol. The RADIUS server compares the username and password to those listed in the database. If the username and password are correct, the RADIUS server notifies the wireless AP that the user is authenticated and authorized, and the wireless AP can provide the user access to the network. If the username and password are not correct, the RADIUS server notifies the wireless AP that the user is not authenticated or authorized, and the wireless AP can prevent the user from accessing the network.

In addition to configuring authentication and authorization, you can also configure accounting with RADIUS. This gives you a centralized way of keeping track of who has been authenticated and who has not, when they were authenticated, and when they were not authenticated. This is important from a security standpoint as it gives you the ability to keep track of all successful and unsuccessful authentication and authorization sessions.

RADIUS uses UDP as its transport protocol. Traditionally, UDP port 1645 was used for authentication and authorization, and UDP port 1646 was used for accounting. However, today we typically see UDP port 1812 for authentication and authorization and UDP port 1813 for accounting. Why is this important? Many Cisco devices default to using 1645 and 1646 as the port numbers, but the RADIUS servers default to using 1812 and 1813 as the port numbers. So, when setting up RADIUS on many Cisco devices, you have to change the port numbers on those devices to 1812 and 1813.

If you are interested in reading more about RADIUS, you can check out RFC 2865, which covers authentication and authorization for RADIUS, and RFC 2866, which covers accounting for RADIUS.

Summary

To provide an access management solution that maintains the levels of confidentiality, integrity, and availability you need, consider the AAA framework, which includes authentication, authorization, and accounting:

- **Authentication** is about proving the identity of someone or something.
  - **Something you know** is authentication based on knowledge.
  - **Something you have** is authentication based on possession.
  - **Something you are** is authentication based on unique aspects of yourself and relies on biometrics.
  - **Somewhere you are** is authentication based on location.
  - **Something you do** is authentication based on habits and characteristics.
  - **Time** is authentication based on the time of day and/or day of the week.
  - **MFA** is about using two or more factors for authentication.
- **Authorization** is the process of granting and controlling what an authenticated user is able to do.
  - The **least-privilege principle** says to give users the minimum permissions they need to accomplish their objectives.
  - The **need-to-know principle** says to give users access only to what they absolutely need to do their jobs and perform their roles.
  - The **implicit-deny principle** says to ensure that everyone is prevented from doing everything unless explicitly allowed.
- **Accounting** is about keeping track of who, what, where, when, why, and how. It is the process of monitoring, recording, and auditing everything in an organization.
  - A **SIEM** solution helps you collect logs, consolidate logs, correlate logs, and get notified about abnormalities/threats in logs that are in breach of established policies.
  - A **SOAR** tool helps you automate responses and reduce the amount of human intervention required when an abnormality/threat has been detected.
- **Remote Authentication Dial-In User Service (RADIUS)** is a client/server protocol used with authentication, authorization, and accounting.

Exam Preparation Tasks

As mentioned in the Introduction, you can customize your strategy for exam preparation. Suggested tasks include the exercises here, Chapter 16, "Final Preparation," and the exam simulation questions on the companion website.

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 3-4 lists these key topics and the page number on which each is found.

Key Topic

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Paragraph	The AAA framework	36
Paragraph	Authentication	36
Table 3-2	Authentication Factors	36
Paragraph	MFA	37
Table 3-3	Examples of MFA	38
Section	Passwords and password policies	39
Section	Authorization	41
Section	Accounting	41
Paragraph	RADIUS	42
Figure 3-1	Admin Using SSH to Manage a Router and Router Authenticating the Admin Using RADIUS	42
Figure 3-2	Wireless User Authenticating to the Wireless Network Using 802.1x, EAP, and RADIUS	43

Define Key Terms

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

AAA; authentication; something you know; something you have; something you are; somewhere you are; something you do; multifactor authentication (MFA); two-step authentication; authorization; least-privilege principle; need-to-know principle; implicit-deny principle; accounting; security information and event management (SIEM); security orchestration, automation, and response (SOAR); Remote Access Dial-In User Service (RADIUS)

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables," found on the companion website, or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key," includes completed tables and lists you can use to check your work.

Review Questions

1. What does AAA stand for?
   - **a.** Authentication, accessibility, and availability
   - **b.** Availability, authentication, and authorization
   - **c.** Authentication, authorization, and accounting
   - **d.** Authentication, availability, and accounting
2. Which of the following are examples of MFA? (Choose two.)
   - **a.** A USB authentication key that needs to be connected to the USB port on the system and a notification displayed on your phone that needs to be accepted or rejected
   - **b.** A bank card and a memorized PIN
   - **c.** A fingerprint scan followed by a facial scan
   - **d.** A username/password and a four-digit PIN that you have memorized
   - **e.** A username/password and a notification sent to your phone that requires you to click yes or no
3. Which of the following are authorization principles? (Choose three.)
   - **a.** Enable MFA
   - **b.** Least privilege
   - **c.** Need to know
   - **d.** Implicit deny
   - **e.** Record all activity
4. Which of the following is a system that can help you collect logs, consolidate logs, correlate logs, and get notified about abnormalities and threats in logs that are in breach of established policies.
   - **a.** SIEM
   - **b.** SOAR
   - **c.** RADIUS
   - **d.** MFA
5. What port numbers are typically used with RADIUS?
   - **a.** 20 and 21
   - **b.** 22 and 23
   - **c.** 1812 and 1813
   - **d.** 3388 and 3389

This page intentionally left blank

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z