PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CC Certified in Cybersecurity

MARI GALLOWAY
AMENA JAMALI

CC Certified in Cybersecurity 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, the Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonITcertification.com/register.
2. Enter the **print book ISBN**: 9780138200381.
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

CC Certified in Cybersecurity Cert Guide

Mari Galloway
Amena Jamali

Pearson

CC Certified in Cybersecurity Cert Guide

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

ISBN-13: 978-0-13-820038-1
ISBN-10: 0-13-820038-6

Library of Congress Cataloging-in-Publication Data Is on File.

$PrintCode

Trademarks

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

Warning and Disclaimer

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

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.

GM K12, Early Career and Professional Learning
Soo Kang

Executive Editor
James Manly

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Timothy Wright

Proofreader
Barbara Mack

Technical Editor
Dominique West

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Online Elements:

Table of Contents

Online Elements:

About the Authors

Mari Galloway, a best-selling author of *Securing Our Future* and cyber professional, is the CEO and a founding board member for the Women's Society of Cyberjutsu (WSC), one of the fastest growing 501(c)3 nonprofit cybersecurity communities dedicated to bringing more women and girls to cyber. WSC provides its members with the resources and support required to enter and advance as cybersecurity professionals.

Mari began her career with Accenture, where she excelled as a network engineer. Mari is also a 2023 Presidential Lifetime Award winner and the inaugural ISC2 Diversity Award winner for 2019. With over 15 years in IT and cybersecurity, her experience spans network design, security architecture, risk assessments, vulnerability management, incident response, and policy development across government and commercial industries.

Mari holds a variety of technical and management certifications (CISSP, GIAC, CCNA, etc.) as well as a Bachelor of Business Administration in Computer Information Systems from Columbus State University and a Master of Science in Information Systems from Strayer University.

Mari is currently a resident of Las Vegas and is the CEO of a cybersecurity consulting company. She regularly contributes content to security blogs and training companies across the country as well as an adjunct professor for the University of Maryland Global Campus (UMGC). She also lends her time to various organizations as an award judge, mentor, and advisor. Outside of being a geek, Mari enjoys arts, puzzles, and Lego!

Amena Jamali is a person with multiple facets. With her rational mind, she is a cybersecurity auditor and an aspiring scholar in the field of disinformation research and cyber psychology. With her creative mind, she is an epic fantasy author with four books published so far in the *The Lord of Freedom* series and many more coming. Her pursuit of truth has been shaped by an eclectic mixture of education: a Bachelor of Arts in Politics and a Master of Science in Cybersecurity from the University of Dallas, which is located in her home state of Texas. In various forums, she speaks and writes about political philosophy, information ethics, governance, risk, compliance, and data privacy, and she is equally passionate about diversity, equity, and inclusion and about the representation of powerful women in literature. A firm believer in the supportive power of community, Amena is an active member of and leader in the Women's Society of Cyberjutsu and has in 2023 won that organization's Cyber Rising Star Award. When she is not working, writing, or theorizing, she reads, learns languages, watches superhero movies, embroiders, and bakes delicious pies.

Dedication

From Mari:

To my mom and sister, thank you for always supporting any and every decision I have made, including writing this book. To the rest of my family and friends, your support on this journey does not go unnoticed. Thank you for always believing in me and motivating me to keep dreaming big.

From Amena:

To my mother and my father, who introduced me to technology and taught me its value in building a better and more equitable world, and to the Divine for Whose praise I offer all of my creative efforts. Thank you for being with me on every journey.

Acknowledgments

Mari and Amena together offer our thanks to the women and allies of the Women's Society of Cyberjutsu. Their encouragement, amplification, and support have kept us going even on the most difficult days, and without them we would not have been able to write this book. We hope our work here will contribute to WSC's mission of empowering women to succeed in cybersecurity.

About the Technical Reviewer

Dominique West is a seasoned security leader with more than a decade of experience in the information technology industry. Specializing in digital cloud transformation, information security governance, risk, and compliance management, as well as cloud and cybersecurity strategy, Dominique has made significant contributions across various industries.

At Datadog, Dominique leads the Governance, Risk, and Compliance division, leveraging her extensive experience to align compliance initiatives with strategic business objectives. Her leadership is instrumental in maintaining and executing a robust compliance roadmap crucial to supporting Datadog's growth and revenue targets while upholding established security standards. Dominique takes pride in cultivating teams that not only excel but also embody a proactive and constructive security mindset. Her multifaceted expertise, spanning cloud security, risk management, compliance, and overall cybersecurity, drives excellence within Datadog and beyond.

Dominique holds a Bachelor of Business Administration in Computer Information Systems from Baruch College, as well as a Master of Science in Cybersecurity from the University of Dallas. Her expertise is further underscored by her CISSP certification. Beyond her professional accomplishments, Dominique is deeply committed to fostering diversity and inclusion in the cybersecurity field. She is the founder of Security in Color, a platform dedicated to providing education and career resources in cybersecurity to underrepresented groups. Additionally, Dominique serves as the NYC Chapter lead for the Women's Society of Cyberjutsu, a nonprofit organization focused on empowering women and allies in cybersecurity.

Dominique's dedication to education extends beyond her advocacy work. She has developed several courses, in partnership with LinkedIn and Pluralsight, aimed at educating users about cloud security, cybersecurity, as well as governance, risk, and compliance (GRC). Additionally, Dominique has lent her expertise as a technical editor, co-contributor for various cybersecurity professional books, and is the co-author for the Google Cloud Professional Cloud Security Engineer exam.

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Reader Services

Register your copy of *CC Certified in Cybersecurity Cert Guide* 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 9780138200381 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

Welcome to the *CC Certified in Cybersecurity Cert Guide.* Certified in Cybersecurity is a new certification by ISC2 that enables new entrants to cybersecurity to demonstrate their comprehension of essential technical concepts to employers as they begin their cybersecurity career. The Certified in Cybersecurity exam is designed to be vendor-neutral and measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. We developed this book to be a resource that you can use to study for the exam and then keep on your bookshelf for later use as a cybersecurity practitioner.

We'd like to note that covering all security concepts in depth in a single book is not feasible. However, you aren't expected to have that level of knowledge for the Certified in Cybersecurity exam, which is intended to assess a basic level of technical and governance-related security knowledge. Keep this in mind while reading through this text, and remember that the main goal of this book is to help you pass the Certified in Cybersecurity exam, not to be the master of all security. Not just yet at least!

Good luck as you prepare to take the Certified in Cybersecurity exam. As you read through this book, you will be building an impenetrable castle of knowledge (rather like security itself!), which will culminate in the know-how to pass the exam.

Goals and Methods

The number one goal of this book is to help you pass the ISC2 Certified in Cybersecurity exam. To that effect, we have filled this book and practice exams with more than 200 questions/answers and explanations. The exams are located in Pearson Test Prep practice test software in a custom test environment. These tests are geared to check your knowledge and ready you for the real exam.

The ISC2 Certified in Cybersecurity exam involves familiarity with computer security theory and hands-on know-how. To aid you in mastering and understanding the Certified in Cybersecurity objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics to be covered in the chapter.
- **Foundation Topics:** The heart of the chapter. The text explains the topics from a theory-based standpoint, as well as from a hands-on perspective. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. The chapters are broken down into two or more Foundation Topics sections each.

- **Key Topics:** The Key Topic icons indicate important sections, paragraphs, figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- **Key Terms:** Key terms are ***emphasized*** in each chapter and are listed without definitions at the end of each chapter. See whether you can define them after you have read the chapter, and then check your work against the complete key term definitions in the glossary.
- **Q&A:** These quizzes, and answers with explanations, are meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter.
- **Practice Exams:** There are 200 exams included in the Pearson Test Prep practice test software. These exams test your knowledge and skills in a realistic testing environment. Take these after you have read through the entire book. Master one, then move on to the next. Take any available bonus exams last.

Who Should Read This Book?

This book is intended for anyone who wants to enter the field of cybersecurity or to cement their knowledge of the basics. We recommend this book to a variety of readers, including those who are preparing for the Certified in Cybersecurity exam and those who want a reminder of the principles and foundations of cybersecurity.

This book is also written for those people who intend to study for additional cybersecurity certifications after passing the Certified in Cybersecurity exam. Where possible, we have elaborated on topics such that these readers would be able to transition to future studies and expand their comprehension of the subject material.

Because the Certified in Cybersecurity exam is intended for new entrants to the field who might not have IT experience, the authors recommend only that you have an elementary grasp of networking and computer operations (e.g., understand the basics of operating systems, networks, and password setup) before you begin Chapter 1. For a deeper exploration of any topic in this book, the authors recommend further study. The focus of this book is to show how the elements of cybersecurity weave together into a cohesive whole and to provide a hint of what to expect upon entrance into the field.

Certified in Cybersecurity Exam Topics

If you haven't bookmarked or reviewed the Certified in Cybersecurity exam objectives, do it now from the ISC2 website: https://www.isc2.org/certifications/cc/cc-certification-exam-outline. Use the exam objectives list to aid in your studies while you use this book.

The following two tables are excerpts from the exam objectives document. Table I-1 lists the Certified in Cybersecurity domains and each domain's percentage of the exam.

Table I-1 Certified in Cybersecurity Exam Domains

Domain	Exam Topic	% of Exam
1	Security Principles	26%
2	Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%
3	Access Controls Concepts	22%
4	Network Security	24%
5	Security Operations	18%

The Certified in Cybersecurity domains are then further broken down into individual objectives.

Table I-2 lists the Certified in Cybersecurity exam objectives and their related chapters in this book. It does not include the topics listed for each objective, but you will find those topics listed at the beginning of the corresponding chapter.

Table I-2 Certified in Cybersecurity Exam Objectives

Objective	Chapter(s)
Domain 1: Security Principles	
1.1 Understand the security concepts of information assurance	1, 8
1.2 Understand the risk management process	2
1.3 Understand security controls	2
1.4 Understand ISC2 Code of Ethics	1
1.5 Understand governance processes	2, 10

Objective	Chapter(s)
Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incidence Response Concepts	
2.1 Understand business continuity (BC)	10
2.2 Understand disaster recovery (DR)	10
2.3 Understand incident response	10
Domain 3: Access Controls Concepts	
3.1 Understand physical access controls	4
3.2 Understand logical access controls	5
Domain 4: Network Security	
4.1 Understand computer networking	6
4.2 Understand network threats and attacks	3
4.3 Understand network security infrastructure	7
Domain 5: Security Operations	
5.1 Understand data security	8, 9
5.2 Understand system hardening	9
5.3 Understand best practice security policies	8, 9
5.4 Understand security awareness training	9

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 accessing the registration code that comes with the book. You can access the code in these ways:

- You can get your access code by registering the print ISBN 9780138200381 on https://www.pearsonitcertification.com/register. Make sure to use the print book ISBN, regardless of whether you purchased an eBook or the print book. After 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.
- If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at https://www.pearsonitcertification.com, click **Account** to see details of your account, and click the **Digital Purchases** tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once 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 on the first page of the book.

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

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

Note that if you want to use the web app only at this point, just navigate to https://www.pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register for this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the Tools tab and click the Update Application button. This will ensure you are running the latest version of the software engine.

Figure Credits

Cover image: Photon photo/Shutterstock

Figure 3.1: Nicescene/Shutterstock

Figure 4.2: Serjio74/Shutterstock

Figure 4.3: Fedor Selivanov/Shutterstock

Figure 4.4: Ratchat/Shutterstock

Figure 7.1: Ohmega1982/Shutterstock

Figure 7.2b: yyang/Shutterstock

Figure 7.4: vschlichting/123RF

CHAPTER 3

Threats to Security

Understanding the various types of threats to security will aid you in understanding the need for security controls and help you implement more effective protection measures and mitigation techniques as you enter the cybersecurity field and land your first role. In this chapter, we will look at the various types of threats to security and why it's essential to understand them, common threat types and mitigations, advanced techniques used by threat actors, and ways to discover and mitigate vulnerabilities.

This chapter covers the following Certified in Cybersecurity exam objectives:

- 4.2 Understand network threats and attacks
  - 4.2a Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, on-path attack, side-channel)
  - 4.2b Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
  - 4.2c Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to decide whether you need to read this entire chapter or skip to the "Exam Preparation Tasks" section. If you doubt your selection of answers to these questions or your own assessment of your knowledge of these topics, you may want to 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 Q&A Sections." Good luck!

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

Foundation Topics Section	Questions
Threats to Security	1–3
Common Threat Categories	4, 5
Network Attacks	6–8
Detection and Mitigation Techniques	9, 10
Scanning and Penetration Testing	11, 12

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 as wrong for purposes of the 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. What is a threat in cybersecurity?
   a. A strategy to prevent data theft
   b. An event that leads to data destruction only
   c. Any circumstance or event with the potential to impact operations, assets, or individuals through unauthorized access, destruction, disclosure, or modification of information
   d. A way to reduce the time that it takes to investigate security issues

2. How can cybersecurity professionals prepare to defend against threats?
   a. By ignoring the latest news in the cybersecurity world
   b. By sharing information with peer organizations
   c. By ensuring all systems and devices have no vulnerabilities
   d. By allowing unauthorized access to information and systems

3. What is the purpose of threat intelligence?
   a. To encourage data theft and destruction
   b. To help cybersecurity professionals and executives make decisions about potential threats
   c. To slow down the investigation of security issues
   d. To keep emerging technology concerns around IoT, AI, and some aspects of the cloud a secret

4. What is ransomware?
   a. Code that runs on computer systems without the user's knowledge
   b. Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system
   c. Standalone, self-replicating malware that causes damage to systems
   d. Malicious software that encrypts your data to block access in exchange for a ransom payment

5. What is the main difference between viruses and worms?
   a. Viruses can self-replicate, while worms need a human to execute them on a system.
   b. Viruses spread through the Internet, while worms spread through LANs.
   c. Viruses are malware that slows down systems, while worms cause extensive damage to systems.
   d. Viruses need human interaction to be successful, while worms can self-replicate and spread without human interaction.

6. What is the main difference between a DDoS attack and a regular DoS attack?
   a. A DDoS attack floods a system with traffic to multiple compromised devices, while a regular DoS attack floods one system with traffic to exhaust resources.
   b. A DDoS attack targets routers, switches, and servers, while a regular DoS attack targets individual devices.
   c. A DDoS attack alters data between communicating parties, while a regular DoS attack intercepts data between communicating parties.
   d. A DDoS attack requires physical access to a system, while a DoS attack is executed remotely.

7. Where are man-in-the-middle (MITM) attacks typically executed?
   a. Secure and encrypted networks
   b. Government organizations and military networks
   c. In places with insecure Wi-Fi, such as coffee shops or hotels
   d. Internal networks within an organization

8. How do side-channel attacks exploit system vulnerabilities?
   a. By intercepting and altering data between communicating parties
   b. By flooding a system with traffic through coordinated efforts

c. By analyzing unintended information leaked by a system's physical implementation

d. By gaining physical access to a system's hardware components

9. What are the two categories of firewalls?

a. Stateful and stateless

b. Network-based and host-based

c. Proxy and packet filtering

d. Next-generation and web application

10. What is the main difference between packet filtering firewalls and web application firewalls?

a. Packet filtering firewalls inspect data packets based on payload content, while web application firewalls monitor IP information.

b. Packet filtering firewalls authenticate clients and forward requests to servers, while web application firewalls authenticate servers and forward requests to clients.

c. Packet filtering firewalls analyze surface-level data such as IP addresses and ports, while web application firewalls inspect HTTP traffic and protect against web-based attacks.

d. Packet filtering firewalls utilize machine learning and behavior analytics, while web application firewalls conduct deep packet inspection.

11. What is the purpose of vulnerability scanning in cybersecurity?

a. To exploit vulnerabilities found in an organization's environment

b. To analyze behaviors on specific endpoints and respond to issues

c. To determine what vulnerabilities an organization has, to prioritize remediation efforts, and to track progress

d. To apply patches to software to fix vulnerabilities

12. What is the difference between vulnerability scanning and pentesting?

a. Vulnerability scanning is used to exploit vulnerabilities, while pentesting analyzes behaviors on specific endpoints.

b. Vulnerability scanning doesn't exploit the vulnerabilities, while pentesting aims to find and exploit vulnerabilities.

  c. Vulnerability scanning allows teams to test incident response and detection processes, while pentesting prioritizes remediation efforts.

  d. Vulnerability scanning gives a continuous look at what is going on in an organization, while pentesting is conducted with open-source tools.

13. What is the purpose of regularly updating and patching systems in cybersecurity?

  a. To analyze behaviors on specific endpoints and respond to issues

  b. To detect and protect against threats using predictive analytics

  c. To gain unauthorized access to systems and data

  d. To apply security fixes for vulnerabilities found in the software

Foundation Topics

Threats to Security

Chapter 2, "Risk Management," quotes the NIST SP 80-37 Rev. 2 definition of a *threat*. NIST provides an alternative but similar definition of *threat* in SP 1800-15:

> *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability.*

Understanding the threats that could impact an organization enables cybersecurity professionals to develop and implement strategies to help prevent unauthorized access and harm to data. With cyber threats evolving constantly, professionals need to be aware of any new tactics and techniques attackers may use to exploit vulnerabilities in an organization's environment.

Staying updated with the latest news in the cybersecurity world enables professionals to stay one step ahead of threat actors by proactively implementing effective mitigation and protection measures before these malicious actors exploit any vulnerabilities, thereby safeguarding their systems and data.

Security breaches occur when threat actors exploit vulnerabilities and gain unauthorized access to information, systems, and devices. A breach can significantly impact organizations and individuals in a variety of ways, such as the destruction of systems, changes to data, or, even worse, data theft. Understanding how threats impact an organization helps cybersecurity professionals to better defend their environments.

Threat intelligence is meant to help cybersecurity professionals and executives make decisions about threats that may affect them. Threat intelligence companies collect, process, and analyze information about a threat actor's ***tactics, techniques, and procedures (TTPs)***. This analysis is then disseminated to customers and partners for use within their threat management programs. This data is shared via Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), government agencies such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA), security vendors such as Unit 42 and Recorded Future, and open-source intelligence tools such as MISP (which formerly stood for the Malware Information Sharing Project).

Sharing threat intelligence with peer organizations is vital to protecting the infrastructure. This information allows security teams to reduce the time it takes to investigate issues and incidents discovered in their environments. This is also an excellent way to stay abreast of emerging technology concerns regarding the Internet of Things (IoT), artificial intelligence (AI), and some aspects of the cloud. While information sharing is essential for collective security, it also presents specific challenges. For example, organizations might be reluctant to share data from a breach due to concerns about reputational damage, fearing that disclosing such incidents could tarnish their image. Additionally, there is a risk of data becoming stale and no longer relevant over time, which can hinder the effectiveness of shared threat intelligence. However, the more we share, the better prepared we are for a security breach.

Common Threat Categories

Many threats can affect an organization. In this section, we discuss various types of threats that could potentially and probably have affected an organization you have engaged with in the past. These include ***malware*** and advanced persistent threat (APT). Let's dig in!

Key Topic

Malware

NIST SP 800-83 Rev. 1 states that "*Malware*, also known as *malicious code*, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." Attackers use malware to gain unauthorized access to system files and other data. Typically, if your system is infected with malware, you will see an increase in system crashes, slow response times, and files not opening. There are a variety of different types of malware, including viruses, worms, Trojans, and ransomware.

Malware is designed specifically to disrupt, damage, or gain unauthorized access to a computer system. Malware can be downloaded on your system via email, from URLs you click, or from additional websites you visit. In each case, malware can damage your entire system, causing you to work overtime to fix the issue.

Viruses

Viruses are some of the most notorious malware variants out there. A ***virus*** is a program that runs on computer systems without the users' knowledge. If a user or system executes a compromised file, the virus can spread copies of itself throughout the network. Viruses utilize system resources to replicate and spread quickly through a network, which can impact performance and slow systems down.

NOTE Viruses need some sort of delivery method and human interaction to be successful. This is different from worms, which can self-replicate.

One of the most dangerous viruses of the Internet era was the Melissa virus, which provided free credentials to adult websites in 1999 through email and forums. This virus was spread via Microsoft macros through Word email attachments. When a user opened an email with a Word attachment, the virus would send copies of itself to the first 50 contacts in their address book, causing widespread disruption affecting more than 300 organizations that year. Melissa was able to exploit the trust associated with opening email attachments proliferating and overwhelming email servers. Microsoft permanently blocked Internet access to Office macros in 2022.

Worms

Worms are standalone, self-replicating malware that causes significant damage to an organization's environment. Worms are typically spread through the Internet or a local area network (LAN). They will use the resources on the first compromised system(s) to start reconnaissance on the rest of the network.

Worms can be spread in a variety of ways:

- *Phishing* emails that are designed to trick the recipient into clicking a link can spread worms. Typically, phishing, as a form of social engineering, plays on human behavior. A subtype is *spear phishing*, which is a more targeted phishing campaign that usually targets executives or other employees higher in the organizational hierarchy. Phishing emails are regularly used to manipulate people into divulging information.

- *Network access* via shared network drives allows worms to spread through those areas quickly.

- Worms may use *security holes and misconfigurations* to spread throughout your organization.

- *External devices* such as USB drives and CDs can contain a worm that then spreads to other systems to cause havoc. To mitigate this risk, organizations employ data loss prevention (DLP) tools to monitor device use.

The Stuxnet worm, first detected in 2010, spread via USB drives and was mostly used for cyber warfare. This worm targeted critical industrial control system (ICS) infrastructure used to control nuclear power plants. This worm was the first of its kind worldwide, thus changing how we look at security for systems that were not built with security in mind.

Trojans

In Greek mythology, the Greeks defeated the city of Troy during the Trojan War by hiding soldiers in a giant wooden horse left outside the city gates, waiting for the Trojans to bring the horse inside to celebrate their apparent victory after the Greeks had pretended to retreat. The Greek soldiers then emerged from the horse's belly and sacked the city. Aptly named for that horse, Trojans operate in the same manner. ***Trojans*** are malicious programs or software disguised as harmless, useful tools to trick users into downloading them, after which they exfiltrate data from the system on which they are installed. Additionally, Trojans are stealthy, can be executed without permission or the user's knowledge, and serve a specific purpose such as data theft, remote control, facilitating other attacks, or persistence in the system.

The Trojan named Zeus, first detected in 2007, was designed to steal personal and financial data from compromised systems. What was unique at the time was that the hackers used Zeus to rope other systems into a botnet to steal money from major corporations, causing over $70 million in damages.

Ransomware

Ransomware has been a major threat in the tech space in the past few years, affecting government agencies, healthcare systems, and school systems and causing massive financial losses to organizations. ***Ransomware*** is malicious software that encrypts your data or systems to block access in exchange for some form of payment to regain access and decrypt that information, as illustrated in Figure 3-1. Threat actors use ransomware to access high-value data such as financial and intellectual property.

Ransomware can be delivered through various means, such as phishing emails or software vulnerabilities. It's important to note that ransomware typically has three main factors: encryption capabilities, a time limit to pay the ransom, and the ability to spread across networks.

Let's discuss two notable ransomware attacks that had very different impacts on organizations. WannaCry was discovered in 2010 and affected more than 200,000 systems across the globe by spreading through phishing emails and network scanning. WannaCry was able to spread quickly due to vulnerabilities in older versions of Microsoft software. The motive behind WannaCry was financial gain. Organizations impacted by WannaCry had to pay the attackers in Bitcoin to have their data decrypted.

Figure 3-1 Ransomware (Image Credit: Nicescene/Shutterstock)

While WannaCry was for financial gain, the incident at Colonial Pipeline in 2021 caused a disruption of operations up and down the East Coast. This pipeline supplies 45% of the East Coast with fuel. This attack was attributed to the threat group DarkSide, which demanded that Colonial Pipeline Company pay 75 Bitcoin (worth approximately $5 million at the time) to access its systems again. The company paid the ransom and was able to resume operations. The Colonial Pipeline incident caused gas shortages for almost a week, leading to panic buying, price spikes in gas, and concerns for national security because the pipeline is considered critical infrastructure.

Advanced Persistent Threats

An ***advanced persistent threat (APT)*** is a highly sophisticated and targeted attack conducted by skilled threat actors, typically state-sponsored groups, looking to gain access to sensitive data or cause a disruption in operations. These threat actors utilize the malware techniques previously described to gain access to systems and wait. APTs have multiple stages of execution and can go undetected for long periods. Data exfiltration, intelligence gathering, or other malicious activities can occur during this time. Initial access for these actors typically is gained either through phishing or zero-day exploits. Network segmentation and a defense-in-depth strategy are great ways to protect against APT attacks. Additional detection and protection measures are discussed throughout this chapter.

Network Attacks

Network attacks pose a significant threat to the security of an organization's computer network. Threat actors will use various attacks that typically target systems such as routers, switches, servers, and other devices that data moves through. Let's look at three types of attacks that can impact an organization. This is not an exhaustive list of attacks.

Key Topic

Distributed Denial-of-Service Attack

A ***distributed denial-of-service (DDoS)*** attack is a malicious and coordinated effort by a threat actor to overwhelm a system's resources. This is achieved by flooding the system with a high volume of traffic. Unlike a typical denial-of-service (DoS) attack that only affects one system, a DDoS attack involves multiple systems within a computer network that are leveraged by the attacker. The main objective of a DDoS attack is to deny access to legitimate users, causing service disruptions and potentially damaging the reputation of the owner of the targeted system.

One common method employed in DDoS attacks is a *botnet*, consisting of a network of Internet-connected devices remotely controlled by the threat actor. These compromised devices enable the attacker to distribute the attack traffic across multiple sources, making mitigating and defending against the attack much more challenging. The following are common examples of DDoS attacks.

A ***synchronization (SYN) flood*** occurs when SYN requests are sent to a system but not responded to, creating half-open connections. SYN requests are the first part of the three-way handshake used to establish a connection with a system. By sending a large number of requests, resources are consumed while waiting for a response, preventing legitimate users from accessing that resource. We discuss the three-way handshake in Chapter 6, "Computer Networking Fundamentals."

A ***User Datagram Protocol (UDP) flood*** is similar to a SYN flood but uses UDP packets to flood a system and exhaust the resources. UDP is a connectionless protocol that offers faster delivery but sacrifices reliability because it doesn't require delivery confirmation. We discuss UDP in Chapter 6.

A ***Hypertext Transfer Protocol (HTTP) flood*** attacks web servers by sending HTTP Get and Post requests to the system to exhaust its resources. This application-based attack targets those systems at Layer 7 of the Open Systems Interconnection (OSI) model. We discuss the OSI model in Chapter 6.

Man-in-the-Middle Attack

A ***man-in-the-middle (MITM) attack*** occurs when a threat actor gains access to the communication channel between communicating parties and intercepts or alters the data, tricking victims into thinking they are communicating with each other. The attacker can now eavesdrop on sensitive information such as passwords, usernames, or financial data. MITM attacks are typically executed in places with insecure Wi-Fi, such as in coffee shops or hotels, and through spoofed websites. As a note, the phrase man-in-the-middle is now being replaced by "on path attack."

Side-Channel Attack

A ***side-channel attack*** exploits information leaked unintentionally by a system's physical implementation rather than a vulnerability in the software or an algorithm. By analyzing factors like power consumption or electromagnetic radiation, attackers can deduce sensitive data, such as passwords, without direct access, potentially compromising security measures. Side-channel attacks can occur in various contexts, including networks, and target specific devices or protocols. Protection against this type of attack can include limiting information in error and debugging log messages or using hardware-based security measures. For example, an attacker can intercept electromagnetic radiation emitted by a device during the process of entering a password. By analyzing variations in electromagnetic signals, such as those generated by keystrokes on a keyboard, the attacker can infer the sequence of characters being entered. This method allows the attacker to derive the password without directly accessing the device or obtaining it through traditional means.

Detection and Mitigation Techniques

While 100% prevention of cyberattacks isn't possible unless a system is isolated from Internet access, there are measures that organizations can take to help reduce the likelihood of a successful attack. One of the first documented signature-based antivirus programs, created in 1987 by Bernd Robert Fix, was used to remove the

Vienna virus. This virus infected .com files on DOS-based systems. The antivirus would then only alert on things that it had already seen. As malware and viruses evolved, antivirus software evolved. Next-generation antivirus (NGAV) protects against a group of behaviors, using predictive analytics driven by machine learning (ML) and AI to detect and protect against threats.

Endpoint detection and response (EDR) solutions emerged around 2013, creating a new category for responding to threats. EDR merged legacy AV capabilities with AI and ML. This allowed teams to analyze behaviors on specific endpoints (such as laptops or mobile phones) and respond to issues at any given time.

As the attack surface for organizations expanded and more data was being collected and processed, extended detection and response (XDR) was born. XDR gives organizations a look at threats across their entire technology ecosystem, including endpoint, network, and cloud. Organizations now have the ability to respond to threats and issues in near real time. With XDR sensors on all devices from the perimeter to the endpoint, security teams can get the full picture of what happened in one location.

In addition to implementing antivirus software, regularly updating and patching systems is critical to protecting data. The patches supplied by vendors typically include security fixes for vulnerabilities found in the software. Not applying patches leaves systems vulnerable to attacks. Threat actors can use these holes to gain unauthorized access to systems and data, take over all the systems, or launch attacks on other systems.

Key Topic

Detection Tools

There are many ways to detect and mitigate network-based attacks. One way to do this is to use an ***intrusion detection system (IDS)***. An IDS (hardware or software) monitors computer network traffic and sends alerts when it detects malicious activity or unauthorized access to systems as data enters and exits the network, in real time. An IDS analyzes network traffic, log files, and other data sources to detect suspicious activity associated with known threats. This is considered a ***network intrusion detection system IDS (NIDS)***. Whereas ***host-based intrusion detection system (HIDS)*** are directly on the host system or endpoint and monitor the traffic for that specific host vs. the entire network.

To boost security, organizations can deploy an *intrusion prevention system (IPS)* within their network traffic flow. An IPS, whether in hardware or software form, actively monitors for suspicious activity and blocks it as necessary. When a threat is detected and blocked, an alert is immediately sent to the system administration for further investigation.

These detection and prevention systems add an additional layer of protection when used along with firewalls.

Key Topic

Firewalls are network security devices that sit at the edge of a network, monitoring incoming and outgoing traffic to identify and block potential cyber threats based on predetermined security policies. Hardware or software firewalls act as a barrier between the internal network and the public Internet. The original firewalls were designed to inspect data packets as they traversed the network. Over time, firewalls improved, addressing application vulnerabilities and utilizing machine learning for advanced detection and prevention.

As illustrated in Figure 3-2, firewalls can be broken up into two categories:

- **Host-based firewall:** Firewall on the endpoint that protects that specific device
- **Network-based firewall:** Firewall on the network that protects the entire network

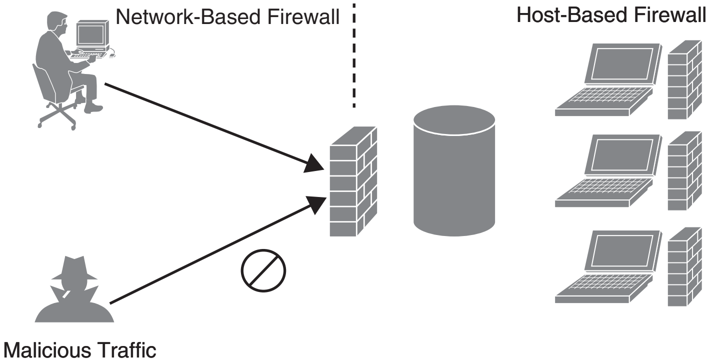

Figure 3-2 Host-Based Versus Network-Based Firewalls

Firewalls come in various types, each with distinct capabilities. Some of these types include

- Packet filtering firewalls
- Proxy, application-aware firewalls
- Web application firewalls
- Next-generation firewalls (NGFW)

Packet filtering firewalls inspect data packets as they traverse the network based on a predefined set of rules. These firewalls inspect the surface-level data, such as source and destination IP addresses and ports, to decide whether to allow or drop a packet. Any packet that fails inspection is dropped. Inspections are based on security policies and firewall rules similar to the example rule presented in Table 3-2.

Table 3-2 Sample Firewall Rule

Direction	Protocol	Source Address	Destination Address	Source Port	Destination Port	Action
Inbound	TCP	Any	22.34.145.6	Any	80	Allow
Inbound	TCP	Any	Any	Any	Any	Deny

With most firewalls, the order of the rules matters. Each rule inspects packets until one proves true. Once an action is taken, no other inspections are done on that packet. The rule outlined in Table 3-2 will allow incoming traffic to 22.34.145.6 over port 80 while denying all other traffic.

Because packet filtering firewalls inspect only surface-level data, they provide only basic levels of protection and are easier to bypass.

Packet filtering firewalls can be either of the following types:

- **Stateless:** Inspect each packet individually
- **Stateful:** Track connections and use previous data packets to make a final decision

A ***proxy, application-aware firewall*** operates at the application layer of the OSI model. These devices monitor application traffic between a client and server for malicious activity based on the content or payload of the packet in addition to the source and destination IP information.

When a client wants to establish a connection with a server, the proxy firewall first authenticates the client and then forwards the request to the server on behalf of the client. This allows the firewall to inspect and filter all traffic between the client and server, reducing the risk of malicious traffic reaching the server or client.

Web application firewalls (WAFs) are similar to proxy firewalls but are specific to protecting against web-based server attacks such as SQL (structured query language) injection and cross-site scripting (XSS). WAFs monitor and filter HTTP traffic between the web server and the Internet. They offer features such as user-defined policies, traffic logging and alerting, and rule sets that can be customized to provide the appropriate level of protection for a specific web application.

Next-generation firewalls (NGFWs) take the detection and protection game a step further and introduce machine learning (ML) and behavior analytics to allow or deny traffic. These devices conduct deep packet inspection (DPI) to determine whether the packet should be allowed or denied. NGFWs are the most popular firewall type today and provide various services and features in addition to firewall services. These services include malware scanning and filtering, network address translation (NAT) services, advanced threat intelligence, and more.

Individually, all the systems can be utilized during an investigation by reviewing the logs from each system. These logs can also be sent to a Security Incident and Event Management (SIEM) platform that enables analysts and engineers to gather data from all the sources in one location for more efficient and improved security investigations.

Key Topic

Scanning and Penetration Testing

Scanning an organization's environment helps the organization to understand what assets it has, any associated vulnerabilities, and ways to remediate and mitigate those vulnerabilities. Vulnerability scanning can be done with open-source tools such as Network Mapper (Nmap) or commercial off-the-shelf (COTS) solutions such as Rapid7 or Tenable. The purpose of these scans is to examine risks that may affect the organization continuously. It also helps the organization prioritize remediation efforts and track progress.

A vulnerability scan differs from a ***penetration test*** (often shortened to *pentest*) in that vulnerability scans are passive in nature. The scan is looking for open vulnerabilities that could lead to exploitation. With pentesting, the goal is to test an organization's technology and the safeguards currently in place by attempting to exploit vulnerabilities found during a vulnerability scan. Once a pentest is complete, the results are shared with the stakeholders for remediation or mitigation. Pentests also enable teams to test their incident response plans and make changes as needed before a threat actor enters the scene.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 13, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

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 3-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 3-3 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Section	Malware	39
Section	Distributed Denial-of-Service Attack	43
Section	Detection Tools	45
Paragraph	Firewalls and their uses	46
Section	Scanning and Penetration Testing	48

Define Key Terms

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

> tactics, techniques, and procedures (TTPs), malware; virus; worm; Trojan; ransomware; advanced persistent threat (APT); distributed denial-of-service (DDoS); synchronization (SYN) flood; User Datagram Protocol (UDP) flood; Hypertext Transfer Protocol (HTTP) flood; man-in-the-middle (MITM) attack; side-channel attack; intrusion detection system (IDS); network intrusion detection system (NIDS); host-based intrusion detection system (HIDS); intrusion prevention system (IPS); firewall; packet filtering firewall; proxy, application-aware firewall; web-application filtering firewall (WAF); next-generation firewall (NGFW); scanning; penetration test

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Why is threat intelligence sharing important in cybersecurity?
2. What are the key factors contributing to the effectiveness of ransomware as a cyber threat?
3. What is a distributed denial-of-service (DDoS) attack?
4. What device combines the power of detection and prevention and adds behavior analytics and machine learning to the mix for improved security?
5. How does a pentest differ from a vulnerability scan?

References

NIST SP 1800-15, *Securing Small-Business and Home Internet of Things (IoT) Devices*: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf

Newman, Andrew. "How Has Antivirus Software Evolved, and Where Might the Industry Be Heading?" *Forbes*, March 9, 2022: https://www.forbes.com/sites/forbestechcouncil/2022/03/09/how-has-antivirus-software-evolved-and-where-might-the-industry-be-heading/?sh=6016e8db5e0f

Holzberg, Melissa. "Hackers Got $5 Million: Colonial Pipeline Reportedly Paid a Ransom in Cryptocurrency, Contrary to Claims." *Forbes*, May 13, 2021: https://www.forbes.com/sites/melissaholzberg/2021/05/13/hackers-got-5-million-colonial-pipeline-reportedly-paid-a-ransom-in-cryptocurrency-contrary-to-claims/?sh=2b72afbb799e

Wright, Gavin, and Alexander S. Gillis. "What Is a Side-Channel Attack?" *Security*, April 6, 2021: https://www.techtarget.com/searchsecurity/definition/side-channel-attack?Offer=abt_pubpro_AI-Insider

"Top 10 Most Dangerous Malware of All Time." Dynamic Solutions Group, December 21, 2022: https://www.dsolutionsgroup.com/top-10-most-dangerous-malware-of-all-time/

This page intentionally left blank

Index