EXAM CRAM

CCNP® and CCIE® Security Core

SCOR 350-701


Cram Sheet


Flash Cards


Practice Tests

JOSEPH MLODZIANOWSKI
EDUARDO MENDONCA
NICHOLAS KELLY

FREE SAMPLE CHAPTER |

CCNP and CCIE Security Core SCOR 350-701 Exam Cram

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.pearsonitcertification.com/register**.
2. Enter the print book's ISBN: **9780137282517**.
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 in to 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

EXAM CRAM

CCNP and CCIE Security Core SCOR 350-701 Exam Cram

Joseph Mlodzianowski
Eduardo Mendonca
Nicholas Kelly

Pearson IT Certification
Hoboken, New Jersey

CCNP and CCIE Security Core SCOR 350-701 Exam Cram

Joseph Mlodzianowski, Eduardo Mendonca, Nicholas Kelly

Published by:
Pearson IT Certification

$PrintCode

Library of Congress Control Number: 2023923358

ISBN-13: 978-0-13-728251-7

ISBN-10: 0-13-728251-6

Warning and Disclaimer

This book is designed to provide information about the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) 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, Pearson / Pearson IT Certification 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.

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

Trademark Acknowledgments

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.

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 Pearson IT Certification, 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 www.pearsonitcertification.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

GM K12, Early Career and Professional Learning: Soo Kang

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Senior Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editor: Akhil Behl

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Donna E. Mulder

About the Authors

Joseph Mlodzianowski is a CCIE, CISSP, information security aficionado, and adventurer; he started multiple events and villages at RSA Conference, DEF CON, and Black Hat, among others, including founding the Red Team Village. He has been in the information technology security field for more than 25 years working in cybersecurity, infrastructure, networking, systems, design, offense, and defense. Joseph is currently a cybersecurity architect for Cisco Managed and Intelligence Services. He spent more than 12 years at the Department of Defense as an operator, principal cyber engineer, and SME designing and deploying complex technologies in support of missions around the world. He has consulted, investigated, and provided support for multiple federal agencies during the past 15 years. Joseph continues to contribute to content, reviews, and editing in the certification testing and curriculum process. Joseph spent almost 15 years in the energy sector, supporting refineries, pipelines, and chemical plants, specializing in ICS/SCADA industrial control networks, and building data centers. Joseph holds a broad range of certifications, including the Cisco CCIE, CNE, CSNA, CNSS-4012, CISSP, ITILv4, MCSE, NSA IAM and IEM, OIAC1180, FEMA IS-00317, Aruba ACMA, First Responder, Hazmat Certified, Member of Bexar County Sheriff's Office CERT, and Certified Hacking Investigator. He also is a founding contributor to the CyManII (Cybersecurity Manufacturing Innovation Institute) Supply Chain. He is a member of Messaging Malware Mobile Anti-Abuse Working Group (M3aawg) and founder of the Texas Cyber Summit, a nonprofit. He believes in giving back to the community and supporting nonprofits. More information on Joseph and his training classes can be found at CyberLearningPath.org.

Eduardo (Eddie) Mendonca is a 23-year Cisco veteran whose current role is cybersecurity technical solutions architect in the Cisco security channel team. Before joining the security channel team, Eddie served as a technical leader on the Cisco Identity Services Engine (ISE) infrastructure development team. Eddie authored several infrastructure features in ISE, including the installation framework, upgrade and patching framework, OS layer IPv6 support, NIC Bonding, Secure Boot, and RootPatch kit. Eddie holds various technical certifications, including CISSP and Cisco DevNet. He also holds U.S. Patent US8250630: Detecting Unauthorized Computer Access. Eddie holds a bachelor's degree in computer science from Fresno State University and is based out of Clovis, California.

Nicholas Kelly has worked for more than 25 years in the cybersecurity industry. He has worked in the private sector, in diplomatic security for the U.S. Department of State, and in volunteer capacity. He currently leads a team of Security Architects at Cisco, whose mission is to provide technical enablement to partners and customers. He is the author of the Leon "Catwalk" Caliber cyberpunk noir series of novels and comics and hosts several podcasts. Nick works alongside the Innocent Lives Foundation, a non-profit, non-vigilante organization that identifies child predators and helps to bring them to justice. He resides in Virginia with his wife, son, and rotating roster of rescued fur babies.

About the Technical Reviewer

Akhil Behl, CCIE Emeritus No. 19564, is a passionate IT executive with a key focus on cloud and security. He has 18+ years of experience in the IT industry working across several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specializations include cloud, security, infrastructure, data center, and business communication technologies. Currently he leads business development for cloud for a global systems integrator.

Akhil has written multiple titles on security and business communication technologies. He has contributed as technical editor for more than a dozen books on security, networking, and information technology. He has published four books with Pearson Education/Cisco Press.

He has published several research papers in national and international journals, including *IEEE Xplore*, and has presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passions and a part of his life.

He holds CCIE Emeritus (Collaboration and Security), Azure Solutions Architect Expert, Google Professional Cloud Architect, Azure AI Certified Associate, Azure Data Fundamentals, CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and master's degree in business administration.

Dedications

Joseph: I would like to dedicate this book to my wife and daughter who have supported me throughout my career.

Eddie: I'd like to dedicate this book to my supportive family—namely my wife Andrea and children Lucas and Simon. Thank you Mendonca family for supporting my career and all of the extracurriculars that come along with it.

Nick: This book is dedicated to my blushing bride of 25 years, and my son, both of whom have challenged me to always explore the fascinating, uncharted waters.

Acknowledgments

Joseph: I would like to thank James Manly, Ellie Bru, and Denise Lincoln from Pearson for their dedication and support to the authoring process; Nick and Eddie from Cisco for their collaboration on this book; and the Cisco leadership team and the CXPM team for all their support.

Eddie: I would like to thank all of the individuals that supported my career move from software development to presales engineering. Without this move, I would have never been involved with this book project. Thank you Aaron Torres, Bill Oehlrich, and Austin Smith for taking a chance on this ISE developer with zero sales experience and allowing me to join the Cisco security channel engineering team. I'd also like to thank my leaders at Cisco who have always been supportive of projects like this. Thank you Tim Myers and Alison Stahl for your continued support and your unwavering commitment to a strong work/life balance.

Nick: I would sincerely like to thank the folks who have taught me leadership and accountability over the years. This starts with my current boss, Tim Myers, who somehow always finds the balance in letting me voice unconventional opinions. Ken Daniels shares a brain with me and keeps me grounded when situations get untidy. My team inspires me and challenges me to grow greater and never settle.

Many thanks to the leaders I have had the privilege of serving over the years who taught me responsibility, organization, and, most importantly, work/

life balance: Amber Johanson, Kevin Lemmon, Tim Balog, Tim Wiley, Dan Ramaswami, and anyone I may have missed.

Finally, thanks to the crew who helped me cut my teeth on life as a firewall jockey. I wouldn't be here if you didn't help me take the first steps: Darrin Slater, Joe Simmons, James "D.B. Cooper" Kelly, Brian Howe, Grilla, Kris Domich, and any of the other really smart folks I've left off this list.

Contents at a Glance

Reader Services

Register your copy of *CCNP and CCIE Security Core SCOR 350-701 Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780137282517 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.

Contents

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

The Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam is the required "core" exam for the CCNP Security and CCIE Security certifications. If you pass the SCOR 350-701 exam, you also obtain the Cisco Certified Specialist—Security Core Certification. This exam covers core security technologies, including cybersecurity fundamentals, network security, cloud security, identity management, secure network access, endpoint protection and detection, and visibility and enforcement.

The exam Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) is a 120-minute exam.

You can review the exam blueprint from Cisco's website at https://learningnetwork.cisco.com/s/scor-exam-topics.

This Introduction covers how the *Exam Cram* series can help you prepare for the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam. This Introduction discusses the basics of the Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam. Included are sections covering preparation, how to take an exam, a description of this book's contents, how this book is organized, and, finally, author contact information. Each chapter in this book contains practice questions. There are also two full-length Practice Exams at the end of the book. Practice Exams in this book should help you accurately assess the level of expertise you need in order to pass the test. Answers and explanations are included for all test questions. It is best to obtain a level of understanding equivalent to a consistent pass rate of at least 90 percent on the Review Questions and Practice Exams in this book before you take the real exam.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the SCOR 350-701 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 CCNP and CCIE Security Core SCOR exam are designed to also make you much more knowledgeable about how to do your job. While this book and the accompanying companion website together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass by memorization but instead helps you truly learn and understand the topics. This book would do you a disservice if it didn't attempt to help you learn the material. To that end, the book will help you pass the CCNP and CCIE Security Core SCOR 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 via test questions on the companion website

How to Prepare for the Exam

This text follows the official exam objectives closely to help ensure your success. The official objectives from Pearson IT Certification can be found here:

https://www.pearsonitcertification.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.html

As you examine the numerous Exam Topics now covered on the CCNP and CCIE Security Core SCOR exam, resist the urge to panic! This book you are holding will provide you with the knowledge (and confidence) you need to succeed in this new CCNP and CCIE Security Core SCOR exam. You just need to make sure you read it and follow the guidance it provides throughout your CCNP and CCIE Security Core SCOR journey.

Chapter Format and Conventions

Every *Exam Cram* chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- **Opening topics list:** This defines the CCNP and CCIE Security Core SCOR 350-701 objective(s) to be covered in the chapter.
- **Topical coverage:** The heart of the chapter, this explains the topics from a hands-on and a theory-based standpoint. This includes in-depth

descriptions, tables, and figures geared to build your knowledge so that you can pass the exams.

- **CramQuiz questions:** At the end of each topic is a quiz. The quizzes, and ensuing explanations, are meant to help you gauge your knowledge of the subjects you have just studied. If the answers to the questions don't come readily to you, consider reviewing individual topics or the entire chapter. In addition to being in the chapters, the CramQuiz questions can be found within the book's companion web page at www.pearsonit-certification.com.
- **Exam Alerts, Sidebars, and Notes:** These are interspersed throughout the book. Watch out for them!

> **Exam Alert**
>
> This is what an Exam Alert looks like. An alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more questions on the exam.

Additional Elements

Beyond the chapters, there are a few more elements that would be helpful in your journey for preparation for the CCNP and CCIE Security Core SCOR 350-701 exam:

- **Practice Exams:** Practice Exams are available as part of the custom practice test engine at the companion web page for this book. They are designed to prepare you for the multiple-choice questions that you will find on the real CCNP and CCIE Security Core SCOR 350-701 exam.
- **Cram Sheet:** The Cram Sheet is located on the companion website of the book. This is designed to jam some of the most important facts you need to know for each exam into one small sheet, allowing for easy memorization. It is also in PDF format on the companion web page.

Practice Questions

This book is filled with practice questions to get you ready. Enjoy the following:

- **CramSaver questions before each and every section**: These difficult, open-ended questions ensure that you really know the material. Some readers use these questions to "test out of" reading a particular section.
- **CramQuizzes ending each section**: These quizzes provide a chance to demonstrate your knowledge after completing a section.

- **Review Questions ending each chapter**: These questions give you a final pass through the material covered in the chapter.
- **Two full Practice Exams**: The Answer Keys for the Practice Exams include explanations and tips for approaching each Practice Exam question.

In addition, the book includes two additional full practice tests in the Pearson Test Prep software available to you either online or as an offline Windows application. If you are interested in more practice exams than are provided with this book, check out the Pearson IT Certification Premium Edition eBook and Practice Test product. In addition to providing you with three eBook files (EPUB, PDF, and Kindle), this product provides you with two additional exams' worth of questions. The Premium Edition version also offers you a link to the specific section in the book that presents an overview of the topic covered in the question, allowing you to easily refresh your knowledge.

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 and bookseller eBook versions**: You can get your access code by registering the print ISBN (9780137282517) on pearsonitcertification.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 Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click Account to see details of your account, and click the digital purchases tab.

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

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

- **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 pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register 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 does not provide the detailed score reports that the other two modes do, 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. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four 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, and 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 while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software. Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click 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 click the Tools tab and click the Update Application button. This ensures that you are running the latest version of the software engine.

Who Should Read This Book?

This book is not designed to be a general networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the CCNP and CCIE Security Core SCOR exam. 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 CCNP and CCIE Security Core SCOR exam? Because it's one of the milestones toward getting the CCNP certification—no small feat in itself. What would getting the CCNP mean to you? A raise, a promotion, recognition? How about to enhance your resume? To demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. To please your reseller-employer, who needs more certified employees for a higher discount from Cisco. Or one of many other reasons.

Strategies for Exam Preparation

The strategy you use for CCNP and CCIE Security Core might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended a live training, purchased the Complete Video Course, or read the Official Cert Guide, then you might take a different approach than someone who learned Cisco Security principles via on-the-job training. Chapter 1 is all about the Cisco CCNP and CCIE Security Core Certification, which includes a strategy that should closely match your background.

Regardless of the strategy you use or the background you have, the 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 core network, cloud, application, user, and endpoint security fundamentals. 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 that you need to be convinced that you know some material already, and to also help you know what topics you need to study more.

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. Chapter 1 provides an overview of the CCNP and CCIE certifications, and offers some strategies for how to prepare for the exams. Chapters 1 through 6 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 6, cover the following topics:

- **Chapter 1, "Security Concepts"**—This chapter discusses fundamental concepts of common threats against on-premises and cloud

environments, workloads moving to the cloud, and the impact to the security threat model. This chapter also covers data breaches, insecure APIs, DoS/DDoS, compromised credentials, cryptography components, and various VPN types.

- **Chapter 2, "Network Security"**—This chapter discusses network security concepts, including how to compare and describe deployment models, architecture in network security solutions that provides intrusion prevention and firewall capabilities, and the components, capabilities, and benefits of using NetFlow. Other topics include Layer 2 security, VLANs, port security, DHCP snooping, Storm Control, private VLANs, and defenses against attacks on MAR, ARP, STP, and DHCP rogue attacks. Finally, it discusses implementing segmentation, access control policies, Application Visibility and Control, URL filtering, malware protection, and intrusion policies.
- **Chapter 3, "Securing the Cloud"**—This chapter discusses how to identify security solutions for public, private, and hybrid cloud environments. You'll learn about community clouds, cloud services models such as SaaS, PaaS, and IaaS, and how NIST 800-145 plays a role in the space. We will compare and contrast cloud responsibilities, patch management, and security assessments in the cloud.
- **Chapter 4, "Content Security"**—This chapter focuses on content security concepts, such as the function of a web proxy, the various methods in which traffic is directed through a web proxy, and how a web proxy controls Internet access. You will also learn components and capabilities of the Cisco Secure Web Appliance, Cisco Secure Web Appliance, and Cisco Secure Email Gateway.
- **Chapter 5, "Endpoint Protection and Detection"**—This chapter discusses the importance of managing and protecting assets, including endpoints and mobile devices. Included are details on endpoint protection, endpoint detection and response, mobile device management, antivirus and anti-malware, Outbreak Control techniques, multifactor authentication, posture assessments, and patching.
- **Chapter 6, "Secure Network Access, Visibility, and Enforcement"**—This chapter focuses on identity management concepts. You will learn fundamental concepts of identity management, such as authentication, authorization, and accounting (AAA), port-based network access control, as well as protocols used in identity management such as RADIUS and TACACS+.

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 CCIE Security Core SCOR 350-701. Table I-1 lists each exam topic listed in the blueprint, along with a reference to the book chapter that covers the topic. These are the same topics you should be proficient in when working with Cisco CCNP and CCIE Security Core technologies in the real world.

> **Note**
>
> At the time this book is being published, the SCOR exam is based on the Cisco CCIE Security Core SCOR 350-701 v1.1 exam.

TABLE I-1 **CCIE Security Core SCOR 350-701 Topics and Chapter References**

CCIE Security Core SCOR 350-701 Exam Topic	Chapter(s) in Which Topic Is Covered
1.0 Security Concepts	**1**
1.1 Explain common threats against on-premises, hybrid, and cloud environments	1
1.1.a On-premises: viruses, Trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware	1
1.1.b Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials	1
1.2 Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, OWASP top ten, missing encryption ciphers, buffer overflow, path traversal, cross-site scripting/forgery	1
1.3 Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key, and certificate-based authorization	1
1.4 Compare site-to-site and remote access VPN deployment types and components such as virtual tunnel interfaces, standards-based IPsec, DMVPN, FlexVPN, and Cisco Secure Client including high availability considerations	1
1.5 Describe security intelligence authoring, sharing, and consumption	1

CCIE Security Core SCOR 350-701 Exam Topic	Chapter(s) in Which Topic Is Covered
1.6 Describe the controls used to protect against phishing and social engineering attacks	1
1.7 Explain northbound and southbound APIs in the SDN architecture	1
1.8 Explain Cisco DNA Center APIs for network provisioning, optimization, monitoring, and troubleshooting	1
1.9 Interpret basic Python scripts used to call Cisco Security appliances APIs	1
2.0 Network Security	**2**
2.1 Compare network security solutions that provide intrusion prevention and firewall capabilities	2
2.2 Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities	2
2.3 Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records	2
2.4 Configure and verify network infrastructure security methods	2
2.4.a Layer 2 methods (network segmentation using VLANs; Layer 2 and port security; DHCP snooping; dynamic ARP inspection; Storm Control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks)	2
2.4.b Device hardening of network infrastructure security devices (control plane, data plane, and management plane)	2
2.5 Implement segmentation, access control policies, AVC, URL filtering, malware protection, and intrusion policies	2
2.6 Implement management options for network security solutions (single vs. multidevice manager, in-band vs. out-of-band, cloud vs. on-premises)	2
2.7 Configure AAA for device and network access such as TACACS+ and RADIUS	2
2.8 Configure secure network management of perimeter security and infrastructure devices such as SNMPv3, NETCONF, RESTCONF, APIs, secure syslog, and NTP with authentication	2

CCIE Security Core SCOR 350-701 Exam Topic	Chapter(s) in Which Topic Is Covered
2.9 Configure and verify site-to-site and remote access VPN	2
2.9.a Site-to-site VPN using Cisco routers and IOS	2
2.9.b Remote access VPN using Cisco AnyConnect Secure Mobility client	2
2.9.c Debug commands to view IPsec tunnel establishment and troubleshooting	2
3.0 Securing the Cloud	**3**
3.1 Identify security solutions for cloud environments	3
3.1.a Public, private, hybrid, and community clouds	3
3.1.b Cloud service models: SaaS, PaaS, IaaS (NIST 800-145)	3
3.2 Compare security responsibility for the different cloud service models	3
3.2.a Patch management in the cloud	3
3.2.b Security assessment in the cloud	3
3.3 Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and secure software development)	3
3.4 Implement application and data security in cloud environments	3
3.5 Identify security capabilities, deployment models, and policy management to secure the cloud	3
3.6 Configure cloud logging and monitoring methodologies	3
3.7 Describe application and workload security concepts	3
4.0 Content Security	**4**
4.1 Implement traffic redirection and capture methods for web proxy	4
4.2 Describe web proxy identity and authentication including transparent user identification	4
4.3 Compare the components, capabilities, and benefits of on-premises, hybrid, and cloud-based email and web solutions (Cisco Secure Email Gateway, Cisco Secure Email Cloud Gateway, and Cisco Secure Web Appliance)	4

CCIE Security Core SCOR 350-701 Exam Topic	Chapter(s) in Which Topic Is Covered
4.4 Configure and verify web and email security deployment methods to protect on-premises, hybrid, and remote users	4
4.5 Configure and verify email security features such as SPAM filtering, anti-malware filtering, DLP, blocklisting, and email encryption	4
4.6 Configure and verify Cisco Umbrella Secure Internet Gateway and web security features such as blocklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption	4
4.7 Describe the components, capabilities, and benefits of Cisco Umbrella	4
4.8 Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)	4
5.0 Endpoint Protection and Detection	**5**
5.1 Compare endpoint protection platforms (EPPs) and endpoint detection and response (EDR) solutions	5
5.2 Configure endpoint anti-malware protection using Cisco Secure Endpoint	5
5.3 Configure and verify outbreak control and quarantines to limit infection	5
5.4 Describe justifications for endpoint-based security	5
5.5 Describe the value of endpoint device management and asset inventory systems such as MDM	5
5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy	5
5.7 Describe endpoint posture assessment solutions to ensure endpoint security	5
5.8 Explain the importance of an endpoint patching strategy	5
6.0 Secure Network Access, Visibility, and Enforcement	**6**
6.1 Validating WLAN configuration settings at the infrastructure side	6
6.2 Validating AP infrastructure settings	6
6.3 Validate client settings	6
6.4 Employ appropriate controller tools to assist troubleshooting	6

CCIE Security Core SCOR 350-701 Exam Topic	Chapter(s) in Which Topic Is Covered
6.5 Identify appropriate third-party tools to assist troubleshooting	6
6.6 Describe the benefits of network telemetry	6
6.7 Describe the components, capabilities, and benefits of these security products and solutions	6
6.7.a Cisco Secure Network Analytics	6
6.7.b Cisco Secure Cloud Analytics	6
6.7.c Cisco pxGrid	6
6.7.d Cisco Umbrella Investigate	6
6.7.e Cisco Cognitive Intelligence	6
6.7.f Cisco Encrypted Traffic Analytics	6
6.7.g Cisco Secure Client Network Visibility Module (NVM)	6

Each version of the exam can have topics that emphasize different functions or features, and some topics can be rather broad and generalized. 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 wireless networking 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 that you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as security 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, Pearson IT Certification might post additional preparatory content on the web page associated with this book at http://www.pearsonitcertification.com/title/978013728251. 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 CCIE Security Core SCOR 350-701 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 the exam. Schedule yourself for the exam and be sure to be rested and ready to focus when taking the exam.

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. There is no substitute for real-world experience; it is much easier to understand the designs, configurations, and concepts when you can actually work within a live security environment.

Cisco.com provides a wealth of information about network, applications, cloud, user, and endpoint security fundamentals.

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 CramSaver 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 CCIE Security Core SCOR 350-701 Certification in the Real World

Cisco has one of the most recognized names on the Internet. Those who have earned the Cisco CCIE Security Core SCOR 350-701 certification can bring quite a bit of knowledge to the table because of their deep understanding of security technologies and how to secure the network, cloud, users, endpoints, and applications. 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 CCNP and CCIE Security Core SCOR 350-701 exam is a computer-based exam, with around 100 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 120 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, Pearson IT Certification might post additional preparatory content on the web page associated with this book at http://www.pearsonitcertification.com/title/9780137282517. 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 Pearson IT Certification website to view any errata or supporting book files that may be available.

Contacting the Authors

Thank you for selecting our book. This book provides you the tools to pass the SCOR 350-701 exam. Feedback is appreciated. You can contact us via the below links:

- Linkedin:/in/mlodzianowski
- Linkedin:/in/eddie-mendonca
- Linkedin:/in/nicholaskelly

Figure Credits

Figure 1-4 - Python Software Foundation

Figure 1-5 - Roger Perkin

Figure 2-6 - Wireshark Foundation

Figure 3-2 - Spiceworks Inc

Figures 3-5, 4-4 - Microsoft Corporation

This page intentionally left blank

CHAPTER 1

Security Concepts

This chapter covers the following SCOR 350-701 exam objectives:

- Security Concepts

This chapter prepares you for exam questions related to security concepts of the SCOR 350-701 exam. You will learn fundamental concepts of common threats against on-premises and cloud environments, and with many workloads moving to the cloud, this shifts and impacts your security threat model.

This chapter also covers data breaches, insecure APIs, denial of service (DoS) and distributed denial of service (DDoS), and compromised credentials. We will also discuss the functions of the cryptography components and get into various virtual private network (VPN) types.

Essential Terms and Components

- On-premises threats
- Threats against cloud environments
- Threats posed by malware, viruses, and Trojans
- Phishing and social engineering
- Active attacks such as SQL injection and man-in-the-middle (MitM)
- Cryptography components
- Intelligence sharing
- Insecure APIs

CramSaver

If you can correctly answer these CramSaver questions, you can save time by skimming the ExamAlerts in each section and then completing the CramQuiz at the end of each section. If you are in doubt whether you fully understand this topic, read everything in this chapter!

1. A threat is any potential issue that affects an asset. What is one of the costliest assets?
   - **a.** Proprietary data
   - **b.** Physical buildings
   - **c.** Specialized equipment
   - **d.** Transportation vehicles
   - **e.** Data centers
2. What is a vulnerability?
   - **a.** A special security feature in a software package
   - **b.** A cryptographic package that encrypts files
   - **c.** A weakness in software, hardware, or firmware
   - **d.** A PKI certificate that expired 30 days before its usage
3. What is an exploit?
   - **a.** A section of code that enables passwords
   - **b.** Code that resets user passwords, usernames, groups, and access to files
   - **c.** A section of code, script, or tool that can take advantage of a vulnerability, allowing the attacker to gain privilege access
   - **d.** Code that allows a user to access documents in a group they are a member of
4. Viruses are code that's mobilized to exploit a weakness in a system. How can a virus infect a system?
   - **a.** When Windows SCCM updates endpoint devices with patches
   - **b.** Downloading an infected file that is then executed and replicates itself in other files
   - **c.** Launching an executable that supports a virtual video on social media
   - **d.** Launching a drawing program that allows you to draw a virus in 3D
5. Where might you observe a cross-site scripting (XXS) attack taking place?
   - **a.** While a programmer is coding a script for use in cross-site access
   - **b.** Anywhere a malicious user is allowed to post unregulated code to a trusted website
   - **c.** In Active Directory, where an administrator can set a password for a user
   - **d.** During a CSV download from an application that collects SQL data

Explain Common Threats Against On-Premises and Cloud Environments

For over three decades, data assets remained tied to the corporate headquarters and data centers. With the advent of cloud computing, co-location, managed hosting, and Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), the threats to these systems haven't been eliminated or reduced. They have simply shifted, and new types of threats have even been created. Two threats that are often overlooked are the availability of technical resources and the expertise to support these systems. When we are unable to staff well-trained persons capable of identifying, mitigating, responding to, and recovering from attacks, we are at higher risk of threats being missed and attackers impacting operations.

Common Threats Against On-Premises Assets

Common on-premises threats include viruses, Trojans, DoS/DDoS attacks, phishing, rootkits, MitM attacks, SQL injection, cross-site scripting, and malware.

When defending on-premises assets from threats, we must first have a good accounting of what those threats consist of, which can range from software, firmware, hardware, and systems to the operating system (OS) versions, patches, and each of their exposures to threats. The three most common assets for any company are:

- First and foremost, employees are the number-one asset. Without them, there is no innovation, product, or sales.
- Second is data, which contains company proprietary information. Understand that data drives business operations.
- Third is the systems themselves, their ability to provide service, and their availability (that they are online and ready to use when needed).

Table 1-1 provides an overview of these three assets and some of their threats and mitigations.

TABLE 1-1 **Assets and Threats**

Assets	Threats	Mitigations
Employees	Phishing, malware, virus, ransomware	Security awareness and training programs
Data, trade secrets	Ransomware, corruption, deletion, exfiltration	Offline/offsite backups, data leak prevention (DLP)
Systems, compute	Malware, OS and firmware attacks, DDoS	Updates, patches

Let's take a closer look at the first asset—people. Protecting employees from cyber criminals and potential workplace hazards, such as a hacker gaining control of a power generation plant or water supply, is necessary. While employees can be a company's greatest asset, they can also be its weakest link.

Employees can be social-engineered, phished, have their endpoints infected with a virus, or they can download ransomware, malware, or other Trojans that could comprise employee personal data as well as spread and affect the corporate networks. Securing the employees should be one of a company's top priorities. Employee awareness programs, monthly awareness newsletters, quarterly training, and biannual training and certification programs can help reduce the negative impacts. Some companies hire phishing companies to try and trick users and then warn them they could have been compromised. Employees can also be insider threats. An employee who is angry or not happy with their position or pay could sabotage or sell intellectual property.

Another highly valuable item is the companies' data. Data often holds the company's customers, products, research, and trade secrets. Attackers could be looking to steal the data to resell it, corrupt the data to harm the business, or encrypt it with cryptography for ransomware and hold the organization hostage. Data is what drives business decisions and provides the organizations with a potential advantage over their competition.

Answers

1. a. The most valuable asset of any company is its proprietary data. This is what differentiates a company from its competitors.
2. c. A vulnerability is a weakness in a system or device that could be exploited.
3. c. A program designed to take advantage of weakness in code. Exploits can be single-purposed or part of a framework tool.
4. b. Viruses involve human intervention to spread and replicate themselves.
5. b. Poorly developed web applications can lead to cross-site scripting attacks.

Finally, the systems themselves that serve up the data can be a target. Hackers can attack the operating system, modify firmware, set up man-in-the-middle attacks, perform code or SQL injections, and code errors causing scripting vulnerabilities. Once an attacker has access to the underlying host (operating system or apps), they can impact performance, steal data, redirect data flow, and make the system unavailable for usage. The various types of attackers are summarized in Table 1-2 along with their capabilities.

TABLE 1-2 **Attacker Types and Capabilities and Motivations**

Hacker Type	Capabilities/Motivations
Black hat	Motivated by money, revenge, or notoriety and wants to sabotage and do harm to systems.
White hat	Generally, the good person who finds vulnerabilities.
Gray hat	An explorer, may do iffy type activity, or may have done borderline bad things. Typically is engaged in the discovery of "what if."
State sponsored	Government-sanctioned hackers or hackers hired to attack other governments.
Hacktivist	Hacking and leaking data as a noble cause.
Cyber terrorist	Causes maximum harm to an organization; usually tied to publicity.
Suicide hacker	Knows they will get caught, wants to cause damage, and understands there is a consequence.
Script kiddie	No real skills, likes to point and click, uses tools and scripts of others.
Physical attacker	Has physical access to systems and wants to cause damage.

The most advanced attackers are nation-state actors and organized crime. With unlimited budgets and resources, they tend to be formidable adversaries. Generally defending against attackers requires understanding their motivation. Table 1-2 lists the most common types. This context will best position you to stop them when you encounter them in the wild. Nation-states usually target governments, utilities, and businesses, with the intent to disrupt capabilities, steal trade secrets, and extort money.

Another on-premises threat is keyloggers, which can be software or hardware based and can be used on any device, such as a PC, server, tablet, or phone. Keyloggers are used to monitor all keystrokes and send them off the system via a covert channel. This way, attackers can obtain your passwords and much more.

Before we get into malware, viruses, Trojans, and vulnerabilities, let's review some terms:

- **Threat:** Any potential danger to an asset, such as theft, fire, water, natural disaster, an attacker, and so on.

- **Vulnerability:** A weakness in a system, system design, or its implementation. Can be in hardware and software. No software or hardware is immune to vulnerabilities.
- **Exploit:** A script or tool that can take advantage of a vulnerability. An exploit leads to access.

Threats come in many shapes, sizes, and delivery methods. Someone can steal your compute device, such as your laptop or phone, or just the data on your systems. Your data center can be exposed to a fire, flood, or a natural disaster. Vulnerabilities can be defined as a weakness in hardware, firmware, or software, and they can be the result of a misconfiguration or a system design flaw. To identify vulnerabilities, a program was developed by MITRE, called the Common Vulnerabilities and Exposure, or CVE. The format of each vulnerability is the "year" and the "ID" assigned, such as CVE-2023-1234. This allows everyone to be on the same page. As defined previously, an exploit is a script, code, or a tool, much like a recipe, designed to take advantage of a weakness in firmware, OS, software package, or system. Exploits generally lead to privilege escalation, loss of integrity, or denial of service. A collection of exploits built into a tool is called an attack framework. Examples include Metasploit, Cobalt Strike, and Immunity Canvas. Professionals use these tools to help find weaknesses and then help an organization defend against those weaknesses, whereas attackers use them to carry out automated, widespread, multiple attacks with a single click. In Table 1-3, we examine the types of attacks and their effects.

TABLE 1-3 **Types of Attacks**

Malware	Virus	A malicious computer program that, when executed, inserts its own code into computer programs and replicates itself. A virus is designed to spread.
	Trojan	A malicious computer program posing as a useful program that, when executed, creates backdoors for hackers to access the system(s).
	Ransomware	Malicious script or code that allows an attacker to execute unauthorized actions on a victim's system and lock them out of the data by encrypting it. Hackers demand ransom for decrypting the data.

Denial of service (DoS)	Direct	Generates packets sent to the victim or target system to overload the target system and deny legitimate users' access to the system.
	Reflected	Spoofing an unwilling system to originate the DoS attack.
	Amplification attack	Spoofing attack where the response is larger than the query, such as the DNS query response is larger than the initial query.
	Botnet DDoS	Many (zombie) systems make up a botnet under the control of the attacker who requests all of them to initiate traffic to the target.
Phishing	An email attack	Emails purporting to be from a reputable company in order to induce an individual to expose their data or system to an attacker.
Rootkit	System, low-level attack	Infects at a low level in order to manipulate information reported on the system to stay hidden.
Man-in-the-middle attack (also known as an on-path attack)	Attacker sits between the victim and the destination	MitM Attacks on-path attacks are hard to detect and give the attacker ability to inject data into the stream.
SQL injection	SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed.	SQL injection process works by prematurely terminating a text string and appending a new command.
Cross-site scripting (XSS)	Malicious JavaScript is executed in the user's browser, recording all the user's interactions with the site.	Cross-site scripting occurs when attackers or malicious users can manipulate a website or web application to return malicious JavaScript to users.

Viruses and worms are scripts or program code mobilized to exploit a weakness in a system. Since the dawn of PC computers in the mid-1980s, there have been viruses, and in 1988 the infamous Morris Worm infiltrated the Internet. A virus requires human interaction such as opening an email attachment, accessing a file, or clicking an executable. The unique characteristic of a virus is that it requires people to interact with a file or program to start the infection. All viruses contain search, infection, and payload routines. The search routine will locate new storage space, files, RAM, and available hard disk space. Then the

infection routine will multiply the virus by attaching itself to any vulnerable items found. Finally, a payload, which is designed to do harm, such as altering, encrypting, or deleting files or exfiltrating data, is executed. Modern viruses steal or exfiltrate files and data or delete files to cause issues. More recently, ransomware variants encrypt files and hold the data ransom until the company pays for the key to decrypt. Virus propagation is done by infecting files, the computer's master boot record (MBR), and macros, and it's accomplished across the network by scanning for vulnerable systems to spread to. More advanced viruses have anti-detection stealth capabilities so they may run in a virtual machine, disable antivirus software, or hide messages from the operating system indicating that there is malware.

Malware is a catch-all term that describes any malicious software that is designed to act badly. Examples include viruses, Trojans, spyware, adware, and ransomware. Malware writers obfuscate their programs to avoid detection by security controls as long as possible. There are many different infection and payload techniques. Profiling and search routines look to find new files to infect and to determine if the system is "infection worthy" by checking available RAM and disk space. A second component of the malware/virus is the infection routine that looks to copy itself to other files and systems. Payload can mean different things. It can just be the routine set to erase the entire disk, it can generate pop-ups to get the user to click them, or it can use the address book in the user's email application to propagate the malware to their contacts.

Trojans are typically programs that appear to do one thing but instead do something quite different—typically a malicious act. Some "Trojaned" PDF and Word documents will drop files to the target's hard disk and set up a method to auto-load other programs. A remote access Trojan (RAT) is one such program and is used to gain full control of a system. Click-fraud Trojans are feed lists of sites to visit to help the fraudster make money by causing infected computers to visit specific sites with ads. There are data-hiding Trojans that will hide themselves and user data from view. E-banking Trojans intercept and use the victim's bank information for financial gain. DoS, FTP, and proxy Trojans allow attackers to use the victim's computer to attack other systems.

Spyware monitors the system's usage, such as the websites you browse, files you work on, calls you make, text messages you send, photos you take, programs you run, and games you play. Consider it surveillance. This information is sent to various third parties such as criminals, marketing companies, nation-states, law enforcement, and others. This information can then be used to market directly to you, cause pop-ups and hijack and redirect your browser to specific sites, or to steal your data and photos. Reporters have seen this done to them by nation-states that use the collected data to intimidate and silence opposition.

Distribution of viruses and malware is done via a wrapper (also known as a binder or packager) used to avoid detection by antivirus software. It combines two or more executables into a single packaged program and makes it more difficult to discern its intent. For example, you could download a game from an untrustworthy website, the game or its packer would be the Trojan, and when its executed, it launches a second program (a virus), which starts to perform its nefarious actions. Packers (which can be custom or off the shelf) such as winrar, winzip, and tar are used to compress and obfuscate the code, making it harder for antivirus software to read. The idea is to prevent viewing of the true intent of the code until it is placed in memory.

Crypters are specifically designed packers with the sole purpose of encrypting and obscuring the malware code to avoid detection. More advanced crypters use advanced algorithms such as AES and Blowfish. Crypters are becoming a more common way to avoid detection by antivirus and intrusion detection systems (IDSs).

Droppers are single-purposed software designed to install malware on the victim's system. They utilize a host of complex antidetection techniques to avoid discovery and evade security controls.

Rootkits utilize advanced persistent threat (APT) methods to infect the system, and they typically hide at a very low level on a device, such as the boot sector or drivers. Rootkits remain quiet in the background. This allows them to intercept and change the operating system processes so that they can stay hidden and exfiltrate data unseen. After a rootkit infects a device, you cannot trust any information that the device reports about itself, and a complete rebuild is generally required. A rootkit can display all the information on the system and exclude anything associated with itself so that the system looks normal.

Man-in-the-middle attacks can use many different techniques. We will discuss a few here. The first method is IP spoofing, where every device on a network has an IP address and MAC address. By spoofing an IP address, an attacker can redirect traffic to their device first and then forward it out, where you wouldn't even be aware of the interception. This is typically done via ARP poisoning. Here are some other techniques use for MitM attacks:

- ARP spoofing is where the attacker floods the network with ARP *mis*information, pointing all devices to itself.
- Session hijacking (or cookie theft) happens when the attacker sits between a system and a web resource and collects cookies and tokens and then replays them on certain websites so they look like the original connection. This allows the attacker to gain access to your email, banking website, and more.

- DNS spoofing or DNS cache poisoning is where the attacker corrupts the Domain Name System's resolver cache function, thus diverting the user to the attacker's website.
- Wi-Fi eavesdropping is where the attacker creates a twin network, and because of its proximity and signal strength, the victim connects to the attacker's fake network, allowing the attacker to intercept all traffic, messages, passwords, and more.
- SSL stripping involves the attacker downgrading the communication between the client and the server to an unencrypted format to be able to intercept cleartext traffic. The user may notice the lock icon in the address bar has changed to "untrusted." There is a tool called SSLstrip, created by Moxie Marlinspike, that tests if an implementation is vulnerable to this attack. It allows for interception of web server traffic, and when an HTTPS URL is encountered, SSLstrip replaces it with an HTTP link and keeps a mapping of the change.

In Table 1-4, we examine the attack methods, activity types, and results of the attack.

TABLE 1-4 **MitM Attack Methods**

Attack Method	Attack Activity	Attack Results
IP spoofing	Spoofing the IP and MAC addresses	ARP spoofing allows an attacker to broadcast the default route to redirect traffic to itself.
DNS spoofing	Poisoning the DNS	Corrupts the Domain Name System data and introduces incorrect results.
Wi-Fi eavesdropping	Creating a fake access point	Attacker creates a twin network that the victim connects to, allowing for the interception of all traffic.
SSL stripping/ hijacking	Downgrading the connection from HTTPS to HTTP	Attacker intercepts HTTPS traffic and strips the "S," resulting in an HTTP connection.
Browser cookie theft	Hijacking a session	The attacker collects the cookies ("tokens") the user is sending over the network and then replays them to trick the receiving end.

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are designed to disrupt, disable, and deny service to legitimate users of a system or program. They do this by flooding a network or system with requests or crafted network traffic. The most common method is an ICMP (ping) attack,

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