CENGAGE

Seventh Edition

CompTIA Security+

Guide to Network Security Fundamentals

MARK CIAMPA

INFORMATION SECURITY

CompTIA Security+ SY0-601 Certification Exam Objectives

Security+ Exam Domain/Objectives	Module	Section	Bloom's Taxonomy
1.0 Threats, Attacks, and Vulnerabilities			
1.1 Compare and contrast different types of social engineering techniques. • Phishing • Smishing • Vishing • Spam • Spam over Internet messaging (SPIM) • Spear phishing • Dumpster diving • Shoulder surfing • Pharming • Tailgating • Eliciting information • Whaling • Prepending • Identity fraud • Invoice scams • Credential harvesting • Reconnaissance • Hoax • Impersonation • Watering hole attack • Typo squatting • Influence campaigns ◦ Hybrid warfare ◦ Social media • Principles (reasons for effectiveness) ◦ Authority ◦ Intimidation ◦ Consensus ◦ Scarcity ◦ Familiarity ◦ Trust ◦ Urgency	1	Vulnerabilities and Attacks	Understanding
1.2 Given a scenario, analyze potential indicators to determine the type of attack. • Malware ◦ Ransomware ◦ Trojans ◦ Worms ◦ Potentially unwanted programs (PUPs) ◦ Fileless virus ◦ Command and control ◦ Bots ◦ Cryptomalware ◦ Logic bombs ◦ Spyware ◦ Keyloggers ◦ Remote access Trojan (RAT) ◦ Rootkit ◦ Backdoor	3	Attacks Using Malware	Analyzing

Security + Exam Domain/Objectives	Module	Section	Bloom's Taxonomy
• Password attacks ◦ Spraying ◦ Dictionary ◦ Brute force ▪ Offline ▪ Online ◦ Rainbow tables ◦ Plaintext/unencrypted	12	Types of Authentication Credentials	Creating
• Physical attacks ◦ Malicious universal serial bus (USB) cable ◦ Malicious flash drive ◦ Card cloning ◦ Skimming	5	Securing Mobile Devices	Applying
• Adversarial artificial intelligence (AI) ◦ Tainted training data for machine learning (ML) ◦ Security of machine learning algorithms • Supply-chain attacks • Cloud-based vs. on-premises attacks	3	Adversarial Artificial Intelligence Attacks	Understanding
• Cryptographic attacks ◦ Birthday ◦ Collision ◦ Downgrade	6	Cryptographic Attacks and Defenses	Applying
1.3 Given a scenario, analyze potential indicators associated with application attacks. • Privilege escalation • Cross-site scripting • Injections ◦ Structured query language (SQL) ◦ Dynamic link library (DLL) ◦ Lightweight directory access protocol (LDAP) ◦ Extensible markup language (XML) • Pointer/object dereference • Directory traversal • Buffer overflows • Race conditions ◦ Time of check/time of use • Error handling • Improper input handling • Replay attack ◦ Session replays • Integer overflow • Request forgeries ◦ Server-side ◦ Client-side ◦ Cross-site • Application programming interface (API) attacks • Resource exhaustion • Memory leak • Secure sockets layer (SSL) stripping • Driver manipulation ◦ Shimming ◦ Refactoring • Pass the hash	3	Segmenting the Network Creating Network Deception Implementing Endpoint Security Hardening the Network	Understanding Applying Applying Analyzing

Seventh Edition

CompTIA Security+

Guide to Network Security Fundamentals

MARK CIAMPA, PH.D.

INFORMATION SECURITY

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

***CompTIA® Security+ Guide to Network Security Fundamentals*, Seventh Edition**
Mark Ciampa

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management: Thais Alencar

Product Team Manager: Kristin McNary

Associate Product Manager: Danielle Klahr

Product Assistant: Tom Benedetto

Director, Learning Design: Rebecca von Gillern

Senior Manager, Learning Design: Leigh Hefferon

Learning Designer: Natalie Onderdonk

Vice President, Marketing – Science, Technology, & Math: Jason Sakos

Senior Marketing Director: Michele McTighe

Marketing Manager: Cassie Cloutier

Product Specialist: Mackenzie Paine

Director, Content Creation: Juliet Steiner

Senior Manager, Content Creation: Patty Stephan

Senior Content Manager: Brooke Greenhouse

Director, Digital Production Services: Krista Kellman

Digital Delivery Lead: Jim Vaughey

Developmental Editor: Lisa Ruffalo

Production Service/Composition: SPi

Design Director: Jack Pendleton

Designer: Erin Griffin

Cover Image(s): iStockPhoto.com/phochi

Library of Congress Control Number: 2020920904

ISBN-13: 978-0-357-42437-7
Loose-leaf Edition: 978-0-357-42438-4

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Printed in the United States of America
Print Number: 01 Print Year: 2020

BRIEF CONTENTS

TABLE OF CONTENTS

MODULE 4

MODULE 5

PART 3

MODULE 6

MODULE 7

MODULE 14

MODULE 15

APPENDICES A

APPENDICES B

INTRODUCTION

The number of cyberattacks has reached epidemic proportions. According to one report, the number of new malware releases every month exceeds 20 million, and the total malware in existence is approaching 900 million variants. More than 11.5 billion records have been exposed through data breaches since 2005. In 2019, four out of every five organizations experienced at least one successful cyberattack, and more than one-third suffered six or more successful attacks.[1] It is estimated that by 2021, a business will fall victim to a ransomware attack once every 11 seconds. Cybercrime will cost the world $6 trillion annually by 2021, an increase of 100 percent in just six years, representing the greatest transfer of economic wealth in human history.[2] Compounding the problem, 85 percent of organizations are experiencing a shortfall of skilled security professionals.[3]

The need to identify and defend against these continual attacks has created an essential workforce that is now at the very core of the information technology (IT) industry. Known as information security, these professionals are focused on protecting electronic information. Various elements of information security, such as application security, infrastructure security, forensics and malware analysis, and security leadership, along with several others, make up this workforce. The demand for certified professionals in information security has never been higher.

When filling cybersecurity positions, an overwhelming majority of enterprises use the Computing Technology Industry Association (CompTIA) Security+ certification to verify security competency. Of the hundreds of security certifications currently available, Security+ is one of the most widely acclaimed security certifications. Because it is internationally recognized as validating a foundation level of security skills and knowledge, the Security+ certification has become the foundation for today's IT security professionals. The value for an IT professional who holds a CompTIA security certification is significant. On average, an employee with a CompTIA certification commands a salary between 5 and 15 percent higher than their counterparts with similar qualifications but lacking a certification.

The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam SY0-601. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls; be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.

Certification provides job applicants with more than a competitive edge over their noncertified counterparts competing for the same IT positions. Some institutions of higher education grant college credit to students who successfully pass certification exams, moving them further along in their degree programs. For those already employed, achieving a new certification increases job effectiveness, which opens doors for advancement and job security. Certification also gives individuals interested in careers in the military the ability to move into higher positions more quickly.

CompTIA® Security+ Guide to Network Security Fundamentals, Seventh Edition, is intended to equip learners with the knowledge and skills needed to be information security IT professionals. Yet it is more than an "exam prep" book. While teaching the fundamentals of cybersecurity by using the CompTIA Security+ exam objectives as its framework, the book takes a comprehensive view of security by examining in depth today's attacks against networks and endpoints and what is needed to defend against these attacks. *Security+ Guide to Network Security Fundamentals*, Seventh Edition, is a valuable tool for those who want to learn about security and enter the field of information security. It also provides the foundation that will help prepare for the CompTIA Security+ certification exam. For more information on CompTIA Security+ certification, visit the CompTIA website at *comptia.org*.

INTENDED AUDIENCE

This book is designed to meet the needs of students and professionals who want to master basic information security. A fundamental knowledge of computers and networks is all that is required to use this book. Those seeking to pass the CompTIA Security+ certification exam will find the text's approach and content especially helpful; all Security+ SY0-601 exam objectives are covered in the text (see Appendix A). *Security+ Guide to Network Security Fundamentals*, Seventh Edition, covers all aspects of network and computer security while satisfying the Security+ objectives.

The book's pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of network and computer security. In addition to the information presented in the text, each module includes Hands-On Projects that guide you through implementing practical hardware, software, network, and Internet security configurations step by step. Each module also contains case studies that place you in the role of problem solver, requiring you to apply concepts presented in the module to achieve successful solutions.

MODULE DESCRIPTIONS

The following list summarizes the topics covered in each module of this course:

Module 1, "Introduction to Security," introduces the cybersecurity fundamentals that form the basis of the Security+ certification. The module begins by defining information security and identifying attackers. It also looks at vulnerabilities in systems and the types of attacks that take advantage of the vulnerabilities.

Module 2, "Threat Management and Cybersecurity Resources," looks at threat management as it pertains to penetration testing and vulnerability scans. The module also explores cybersecurity standards, regulations, frameworks, and configuration guidelines.

Module 3, "Threats and Attacks on Endpoints," focuses on network-connected hardware devices, better known as endpoints. It begins by looking at attacks using various types of malware and then surveys application attacks. It also examines adversarial artificial intelligence attacks.

Module 4, "Endpoint and Application Development Security," describes different sources of threat intelligence information. The module also explores securing endpoint devices and creating and deploying secure applications to run on those devices.

Module 5, "Mobile, Embedded, and Specialized Device Security," looks at securing mobile devices. As users have embraced mobile devices, so too have attackers embraced them as targets. This module also explores embedded systems and the Internet of Things devices. Finally, it examines keeping specialized devices secure.

Module 6, "Basic Cryptography," explores how encryption can be used to protect data. The module covers what cryptography is and how it can be used for protection, and then examines how to protect data using three common types of encryption algorithms: hashing, symmetric encryption, and asymmetric encryption. It also covers how to use cryptography on files and disks to keep data secure.

Module 7, "Public Key Infrastructure and Cryptographic Protocols," examines how to implement cryptography and use digital certificates. It also looks at public key infrastructure and key management. This module covers cryptographic protocols to see how cryptography is used on data that is being transported and concludes with how to implement cryptography.

Module 8, "Networking Threats, Assessments, and Defenses," begins a study of network attacks and defenses. First, the module explores some of the common attacks that are launched against networks today. Then it looks at tools for assessing and defending networks. Finally, it examines physical security defenses that can be used to protect network technology devices.

Module 9, "Network Security Appliances and Technologies," examines security appliances that provide resilience to attackers—such as firewalls, proxy servers, deception instruments, and other security appliances. It also explores security technologies such as access technologies, technologies for monitoring and managing networks, and principles for designing a secure network.

Module 10, "Cloud and Virtualization Security," looks at both cloud computing and virtualization. It examines what both of these technologies are, how they function, and how they can be secured. Because cloud computing relies on secure network connections, it also discusses secure network protocols.

Module 11, "Wireless Network Security," explores the attacks on wireless devices that are common today. It also identifies vulnerabilities in wireless security and examines several secure wireless protections.

Module 12, "Authentication," defines authentication and the secure management techniques that enforce authentication. This module looks at the types of authentication credentials that can be used to verify a user's identity and the techniques and technology used to manage user accounts in a secure fashion.

Module 13, "Incident Preparation, Response, and Investigation," focuses on the plans that must be made for when a cybersecurity incident occurs. These plans cover incident preparation, incident response, and then a follow-up investigation as to how the incident occurred and how similar future events can be mitigated.

Module 14, "Cybersecurity Resilience," explores the capacity of an organization to recover quickly from difficulties and spring back into shape. This module defines business continuity and why it is important. Next, it investigates how to prevent disruptions through redundancy. Finally, it explains how business policies can help provide resilience to an organization.

Module 15, "Risk Management and Data Privacy," examines two elements of cybersecurity that are of high importance to both enterprises and users. The first involves risk and the strategies for mitigating risks. It also explores data privacy and the issues that surround it.

Appendix A, "CompTIA SY0-601 Certification Examination Objectives," provides a complete listing of the latest CompTIA Security+ certification exam objectives and shows the modules and headings in the modules that cover material associated with each objective, as well as the Bloom's Taxonomy level of that coverage.

Appendix B, "Two Rights & a Wrong: Answers," contains the answers to the "Two Rights and a Wrong" assessment questions.

FEATURES

The course's pedagogical features are designed to provide a truly interactive learning experience and prepare you to face the challenges of cybersecurity. To aid you in fully understanding computer and network security, this course includes many features designed to enhance your learning experience.

- **Maps to CompTIA Objectives.** The material in this text covers all the CompTIA Security+ SY0-601 exam objectives.
- **Module Objectives.** Each module lists the concepts to be mastered within that module. This list serves as a quick reference to the module's contents and as a useful study aid.
- **Front-Page Cybersecurity.** This section opens each module and provides an explanation and analysis of some of the latest attacks and defenses related to topics that are covered in the module. The sections establish a real-world context for understanding cybersecurity.
- **Illustrations, Tables, and Bulleted Lists.** Numerous full-color diagrams illustrating abstract ideas and screenshots of cybersecurity tools help learners better visualize the concepts of cybersecurity. In addition, the many tables and bulleted lists provide details and comparisons of both practical and theoretical information that can be easily reviewed and referenced in the future.
- **Module Summaries.** Each module reading concludes with a summary of the concepts introduced in that module. These summaries revisit the ideas covered in each module.
- **Key Terms.** All of the terms in each module that were introduced with bold text are gathered in a Key Terms list, providing additional review and highlighting key concepts. Key Term definitions are included in the Glossary at the end of the text.
- **Review Questions.** The end-of-module assessment begins with a set of review questions that reinforce the ideas introduced in each module. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts and provide valuable practice for taking CompTIA's Security+ exam.
- **Hands-On Projects.** Projects at the end of each module give you the opportunity to apply in practice what you have just learned. These projects include detailed step-by-step instructions to walk you through endpoint security configuration settings and demonstrate actual security defenses using websites or software downloaded from the Internet. In addition, instructions are provided regarding how to perform these projects in a protected sandbox or virtual machine environment so that the underlying computer is not impacted.

- **Case Projects.** Although it is important to understand the theory behind cybersecurity technology, nothing beats real-world experience. To this end, each module includes several case projects aimed at providing practical implementation experience as well as practice in applying critical thinking skills to reinforce the concepts learned throughout the module.

New to this Edition

- Maps fully to the latest CompTIA Security+ exam SY0-601
- Completely revised and updated with expanded coverage on attacks and defenses
- New module units: Security Fundamentals, Endpoint Security, Cryptography, Network Security, and Enterprise Security
- All new "Front-Page Cybersecurity" opener in each module
- Two Rights & a Wrong self-assessments that give you opportunities to quickly assess your understanding of the topics
- All new virtual machine labs that help you refine the hands-on skills needed to master today's cybersecurity toolset
- New and updated Hands-On Projects cover some of the latest security software
- All new introductions to the Hands-On Projects provide time estimates, Security+ objective mappings, and project descriptions
- New cybersecurity consultant and assurance service scenarios in which you serve as an intern and gain practical experience regarding what you might encounter on the job
- New Information Security Community Site activities allow you to interact with other learners and security professionals from around the world through a regularly updated blog, discussion boards, and other features
- All SY0-601 exam topics fully defined
- Linking of each exam subdomain to Bloom's Taxonomy (see Appendix A)

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The following icons and elements are used in this textbook:

NOTE 1

Note elements draw your attention to additional helpful material related to the subject being described.

CAUTION The Caution icons warn you about potential mistakes or problems and explain how to avoid them.

TWO RIGHTS & A WRONG

The "Two Rights & a Wrong" elements let you quickly assess your understanding of the topics. The answers to these assessments appear in Appendix B.

VM LAB The VM Lab icons alert you to live, virtual machine labs that reinforce the material in each module.

CERTIFICATION

Certification icons indicate CompTIA Security+ objectives covered under major module headings.

INSTRUCTOR MATERIALS

Everything you need for your course is in one place. This collection of book-specific lecture and class tools is available online. Please visit *login.cengage.com* and log in to access instructor-specific resources on the Instructor Resources, which includes the Guide to Teaching Online; Instructor Manual; Solutions to the textbook, lab manual, and live, virtual machine labs; Test Bank files; PowerPoint Presentations; Syllabus; and Student Downloads.

- **Guide to Teaching Online.** The Guide to Teaching Online includes two main parts. Part 1 offers general technological and pedagogical considerations and resources, and Part 2 provides discipline-specific suggestions for teaching when you can't be in the same room with students.
- **Electronic Instructor Manual.** The Instructor Manual that accompanies this textbook includes the following items: additional instructional material to assist in class preparation—including suggestions for lecture topics, additional projects, and class discussion topics.
- **Solutions Manuals.** The instructor resources include solutions to all end-of-module material, including review questions and case projects. The Lab Manual Solutions include answers to the review questions found in the lab manual modules. The Live, Virtual Machine Labs Solutions include examples of correct screenshots and answers to the inline questions found within the labs.
- **Test Banks with Cengage Testing Powered by Cognero.** This flexible, online system allows you to do the following:
  - Author, edit, and manage test bank content from multiple Cengage solutions.
  - Create multiple test versions in an instant.
  - Deliver tests from your LMS, your classroom, or wherever you want.
- **PowerPoint Presentations.** This book comes with a set of Microsoft PowerPoint slides for each module. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for module review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced.
- **Syllabus.** The sample syllabus provides an example of a template for setting up a 14-week course.
- **Student Downloads.** The student downloads include Accessible Launch Text for MindTap Lab Simulations and Accessible Launch Text for MindTap Live Virtual Machine Labs.

Total Solutions for Security

To access additional course materials, please visit *www.cengage.com*. At the *cengage.com* home page, search for the ISBN of your title (from the back cover of your book) using the search box at the top of the page. This will take you to the product page where these resources can be found.

MindTap

MindTap for *Security+ Guide to Network Security Fundamentals*, Seventh Edition, is a personalized, fully online digital learning platform of content, assignments, and services that engages students and encourages them to think critically while allowing you to easily set your course through simple customization options.

MindTap is designed to help students master the skills they need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and certification test prep. Students are guided through assignments that help them master basic knowledge and understanding before moving on to more challenging problems.

All MindTap activities and assignments are tied to defined learning objectives. Readings support course objectives, while Security for Life activities encourage learners to read articles, listen to podcasts, or watch videos to stay current with what is happening in the field of IT and cybersecurity. You can use these activities to help build student interest in the field of information security as well as lifelong learning habits.

Reflection activities encourage self-reflection and open sharing among students to help improve their retention and understanding of the material. Visualize Videos help explain and illustrate difficult information technology concepts.

Lab simulations provide students with an opportunity for hands-on experience and problem-solving practice with automatic feedback. The live, virtual machine labs provide hands-on practice and give students an opportunity to troubleshoot, explore, and try different real-life solutions in a secure, private sandbox environment.

Test Prep questions in the ATP app allow students to quiz themselves on specific exam domains, and the pre- and post-course assessments measure exactly how much they have learned. CNOW quizzes provide test questions in the style of the Security+ certification exam and help you measure how well learners mastered the material after completing each MindTap module.

MindTap is designed around learning objectives and provides the analytics and reporting to easily see where the class stands in terms of progress, engagement, and completion rates.

Students can access eBook content in the MindTap Reader—which offers highlighting, note taking, search, and audio, as well as mobile access. Learn more at *www.cengage.com/mindtap/*.

Instant Access Code: (ISBN: 9780357424407)

Printed Access Code: (ISBN: 9780357424414)

Lab Manual

Hands-on learning is necessary to master the security skills needed for both CompTIA's Security+ Exam and for a career in network security. Included only in the MindTap, *Security+ Guide to Network Security Fundamentals Lab Manual*, 7th Edition, contains hands-on exercises that use fundamental networking security concepts as they are applied in the real world. Each module offers review questions to reinforce your mastery of network security topics and to sharpen your critical thinking and problem-solving skills.

Bloom's Taxonomy

Bloom's Taxonomy is an industry-standard classification system used to help identify the level of ability that learners need to demonstrate proficiency. It is often used to classify educational learning objectives into different levels of complexity. Bloom's Taxonomy reflects the "cognitive process dimension." This represents a continuum of increasing cognitive complexity, from remember (lowest level) to create (highest level).

There are six categories in Bloom's Taxonomy as seen in Figure A.

In all instances, the level of coverage the domains in *Security+ Guide to Network Security Fundamentals*, Seventh Edition, meets or exceeds the Bloom's Taxonomy level indicated by CompTIA for that objective. See Appendix A for more detail.

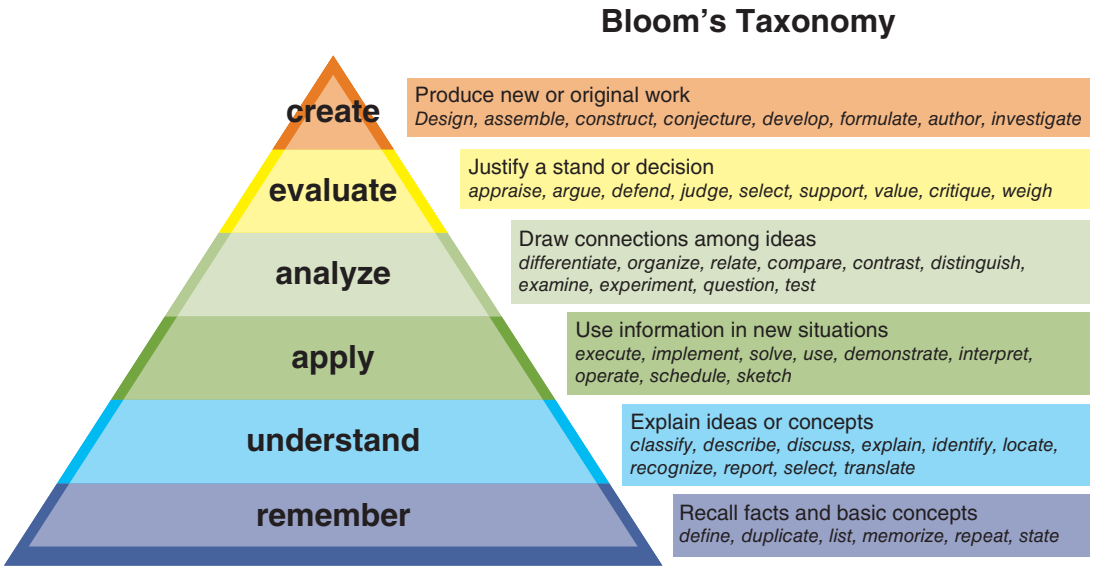


FIGURE A Bloom's Taxonomy

Information Security Community Site

Stay secure with the Information Security Community Site. Connect with students, professors, and professionals from around the world, and stay on top of this ever-changing field. Visit *http://community.cengage.com/Infosec2/* to

- **Ask** authors, professors, and students the questions that are on your mind in the Discussion Forums.
- **See** up-to-date news, videos, and articles.
- **Read** regular blogs from author Mark Ciampa.
- **Listen** to podcasts on the latest Information Security topics.
- **Review** textbook updates and errata.

Each module's Case Projects include information on a current security topic and specific projects ask the learner to post reactions and comments to the Information Security Community Site. This allows users from around the world to interact and learn from other users as well as security professionals and researchers.

WHAT'S NEW WITH COMPTIA SECURITY+ CERTIFICATION

The CompTIA Security+ SY0-601 exam was updated in November 2020. Several significant changes have been made to the exam objectives. The exam objectives have been significantly expanded to reflect current security issues and knowledge requirements more accurately. These exam objectives place importance on knowing "how to" rather than just knowing or recognizing security concepts.

The following are the domains covered on the new Security+ exam:

Domain	% of Examination
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%
Total	100%

About the Author

Dr. Mark Ciampa is Professor of Information Systems in the Gordon Ford College of Business at Western Kentucky University in Bowling Green, Kentucky. Previously, he was Associate Professor and Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee, for 20 years. Mark has worked in the IT industry as a computer consultant for businesses, government agencies, and educational institutions. He has published more than 25 articles in peer-reviewed journals and is also the author of more than 25 technology textbooks, including *CompTIA Guide to CySA+*, *CWNA Guide to Wireless LANs 3e, Guide to Wireless Communications, Security Awareness: Applying Practical Security In Your World 5e,* and *Networking BASICS*. Dr. Ciampa holds a PhD in technology management with a specialization in digital communication systems from Indiana State University, and he has certifications in security and health care.

Acknowledgments

A large team of dedicated professionals all contributed to this project, and I am honored to be part of such an outstanding group of professionals. First, thanks go to Cengage Product Managers Amy Savino and Danielle Klahr for providing me the opportunity to work on this project and for providing their continual support. Thanks also to Senior Content

Manager Brooke Greenhouse for answering all my questions, to Learning Designer Natalie Onderdonk for her valuable input, and to Danielle Shaw for her technical reviews. I would like to give special recognition to developmental editor Lisa Ruffolo. Although this was our first major project together, it was like we had worked together for many years because she knew exactly what I needed. Lisa provided numerous helpful suggestions, made excellent comments, and expertly managed all the pieces that this fast-moving project required. I also appreciated the significant contributions of the reviewers for this edition: Joyce Thompson, Professor of Computer Science and GIS at Lehigh Carbon Community College, and Jeffrey Koch, Professor of Computer Science at Tarrant County College. To everyone on the team I extend my sincere thanks.

Finally, I want to thank my wonderful wife, Susan. Her patience, support, and love were, as always, there from the first page to the last. I could not have done it without her.

Dedication

To Braden, Mia, Abby, Gabe, Cora, Will, and Rowan.

TO THE USER

This book should be read in sequence, from beginning to end. Each module builds on those that precede it to provide a solid understanding of networking security fundamentals. The book may also be used to prepare for CompTIA's Security+ certification exam. Appendix A pinpoints the modules and sections in which specific Security+ exam objectives are covered.

Hardware and Software Requirements

Following are the hardware and software requirements needed to perform the end-of-module Hands-On Projects.

- Microsoft Windows 10
- An Internet connection and web browser
- Microsoft Office

Free Downloadable Software Requirements

Free, downloadable software is required for the Hands-On Projects in the following modules.

Module 1:

- Microsoft Safety Scanner
- Oracle VirtualBox

Module 3:

- Refog Keylogger
- EICAR AntiVirus Test File

Module 4:

- ConfigureDefender

Module 5:

- Prey
- BlueStacksNorton Security (Android app)

Module 6:

- OpenPuff Steganography
- HashCalc
- Jetico BestCrypt

Module 7:

- Adobe Reader

Module 9:

- GlassWire

Module 10:

- VMware vCenter Converter

Module 11:

- NirSoft WifiInfoView
- Vistumbler

Module 12:

- BioID Facial Recognition Authenticator
- KeePass

Module 13:

- Directory Snoop

Module 14:

- UNetbootin
- Linux Mint

Module 15:

- Browzar

References

1. "2020 Cyberthreat defense report," *Cyberedge Group*, accessed Apr. 20, 2020, https://cyber-edge.com/cdr/.
2. Morgan, Steve, "2019 official annual cybercrime report," *Cybersecurity Ventures*, accessed Apr. 20, 2020, www .herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.
3. "2020 Cyberthreat defense report," *Cyberedge Group*, accessed Apr. 20, 2020, https://cyber-edge.com/cdr/.

SECURITY FUNDAMENTALS

Relentless is perhaps the best way to describe today's cyberattacks. These attacks, directed against devices ranging from huge cloud computing servers to tiny Internet of Things (IoT) sensors, are designed to steal or manipulate the sensitive data stored in them. The modules in Part 1 introduce security and outline the causes of these attacks. The modules also discuss how to perform security evaluations to identify the weaknesses that need to be addressed to repel attacks.

PART 1

MODULE 1

INTRODUCTION TO SECURITY

After completing this module, you should be able to do the following:

1. Define information security and explain why it is important
2. Identify threat actors and their attributes
3. Describe the different types of vulnerabilities and attacks
4. Explain the impact of attacks

Front-Page Cybersecurity

Threat actors have a long history of using current events to take advantage of distracted and unsuspecting users. For example, whenever a natural disaster such as a hurricane or flood occurs, unscrupulous attackers send out email messages with tempting subject lines such as "Contribute to Disaster Relief Here" or "These Flood Pictures Are Unbelievable!" These messages are, of course, intended to trick a user to open an email attachment that contains malware or click a hyperlink that redirects them to a malicious website.

The 2020 pandemic caused by the coronavirus disease (COVID-19) was no exception. Threat actors used this tragic worldwide event as cover for their attacks. A variety of campaigns distributed malware, stole user credentials, and scammed victims out of their money.

Many email scams offered to sell hard-to-find face masks or even medication to cure COVID-19 infections. Some scams asked for investments in fake companies that claimed to be developing vaccines, while other email scams asked for donations to fictitious charities, such as the World Health Community. (This organization does not exist, but the name is similar enough to the World Health Organization to cause confusion.)

Some malicious emails were designed to infect a victim's computer with malware. Email subject lines such as a "Breaking Coronavirus News Update" or "You Must Do This Right Now!" were common and caused anxious victims to open an attachment that infected their computer. Often emails that pretended to come from the Centers of Disease Control and Prevention (CDC) claimed to contain a list of new COVID-19 cases in the vicinity and included the instructions, "You are instructed to immediately read this list of cases to avoid potential hazards." Unfortunately, opening the attachment installed malware on the computer and stole user passwords.[1]

In one particularly egregious email attack, the threat actors claimed to have access to personal information about the email recipient, including where they lived. The attackers threatened to visit the user to infect them and their family with COVID-19 unless a ransom was paid online. Over a span of two days, this attack was detected more than 1,000 times.

Perhaps the award for the most innovative attack goes to the AI Corona Antivirus website. This site advertised "Corona Antivirus—World's best protection." Downloading and installing its digital "AI Corona Antivirus" would protect the computer

from digital malware infections and keep the user from being infected by the biological COVID-19. In case someone might be skeptical that downloading and installing computer antivirus software would protect them from COVID-19, the website claimed proof that their product actually worked: "Our scientists from Harvard University have been working on a special AI development to combat the virus using a Windows app. Your PC actively protects you against the coronaviruses while the app is running."

However, downloading the AI Corona Antivirus software on a computer did not protect the user from the biological COVID-19—though it took several other actions. It turned the computer into a launching pad to attack other computers. It also took screenshots of what was displayed on the monitor, stole web browser cookies and saved passwords, installed a program to capture keystrokes, and even took any Bitcoin wallets saved on the computer.[2]

How many cyberattacks have you heard about over the past month? The past week? Even today? The number of attacks has reached astronomical proportions. According to one report, the number of new malware releases every month exceeds 20 million, and the total malware in existence is approaching 900 million instances.[3] In 2019, four out of every five organizations experienced at least one successful cyberattack, and more than one-third suffered six or more successful attacks.[4] It is estimated that by 2021, a business will fall victim to a ransomware attack once every 11 seconds. Cybercrime will cost the world $6 trillion annually by 2021, an increase of 100 percent in just six years, representing the greatest transfer of economic wealth in human history.[5] Compounding the problem, 85 percent of organizations are experiencing a shortfall of skilled security professionals.[6] The dismal numbers go on and on.

The need to identify and defend against these constant attacks has created an essential workforce that is now at the core of the information technology (IT) industry. Known as *information security,* personnel in this field are focused on protecting electronic information. Various elements of information security—such as *application security, infrastructure security, forensics and malware analysis,* and *security leadership*, along with several others—make up this workforce.

The information security workforce is usually divided into two broad categories. Information security *managerial personnel* administer and manage plans, policies, and people, while information security *technical personnel* are concerned with designing, configuring, installing, and maintaining technical security equipment. Within these two broad categories are four generally recognized types security positions:

- *Chief information security officer (CISO)*. This person reports directly to the chief information officer (CIO). (Large enterprises may have more layers of management between this person and the CIO.) The CISO is responsible for assessing, managing, and implementing security.
- *Security manager*. The security manager reports to the CISO and supervises technicians, administrators, and security staff. Typically, a security manager works on tasks identified by the CISO and resolves issues identified by technicians. This position requires an understanding of configuration and operation but not necessarily technical mastery.
- *Security administrator*. The security administrator has both technical knowledge and managerial skills. A security administrator manages daily operations of security technology and may analyze and design security solutions within a specific entity as well as identifying users' needs.
- *Security technician*. This position is generally entry level for a person who has the necessary technical skills. Technicians provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems.

NOTE 1

The job outlook for security professionals is exceptionally strong. According to the U.S. Bureau of Labor Statistics (BLS) "Occupational Outlook Handbook," the job outlook for information security analysts through 2024 is expected to grow by 18 percent, much faster than the average job growth rate.[8] One report states that by the end of the decade, demand for security professionals worldwide will rise to 6 million, with a projected shortfall of 1.5 million unfilled positions.[9]

As noted earlier, organizations have a desperate need for trained security personnel. The number of unfilled cybersecurity positions has increased by 50 percent since 2015.[7] By some estimates, 3.5 million positions will open by 2021.

When filling cybersecurity positions, an overwhelming majority of enterprises use the Computing Technology Industry Association (CompTIA) Security+ certification to verify security competency. Of the hundreds of security certifications currently available, Security+ is one of the most widely acclaimed security certifications.

Because it is internationally recognized as validating a foundation level of security skills and knowledge, the Security+ certification has become the foundation for today's IT security professionals.

NOTE 2

The value for an IT professional who holds a CompTIA security certification is significant. On average, an employee with a CompTIA certification commands a salary from 5 to 15 times higher than their counterparts with similar qualifications but lacking a certification.[10]

The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam, SY0-601. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls, be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.

NOTE 3

The CompTIA Security+ certification meets the ISO 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill multiple levels of the DoD 8140 directive, which is an expansion of and replacement for the earlier DoD 8570 directive. This directive outlines which cybersecurity certifications are approved to validate the skills for certain job roles.

This module introduces the security fundamentals that form the basis of the Security+ certification. It begins by defining information security and then examines the attackers and how they function. It also covers vulnerabilities, categories of attacks, and the impacts of attacks.

WHAT IS INFORMATION SECURITY?

The first step in a study of information security is to define exactly what it is. This involves examining the definition of security and how it relates to information security.

Understanding Security

What is *security*? The word comes from Latin, meaning *free from care.* Sometimes security is defined as *the state of being free from danger*, which is the *goal* of security. It is also defined as the *measures taken to ensure safety*, which is the *process* of security. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal. In this light, security can be defined as *the necessary steps to protect from harm*.

The relationship between *security* and *convenience* is *inversely proportional* (the symbol α), as illustrated in Figure 1-1: as security is increased, convenience is decreased. That is, the more secure something is, the less convenient it may become to use. Consider a house in which the homeowner installs an automated alarm system. The alarm requires a resident to enter a code on a keypad within 30 seconds of entering the house. Although the alarm system makes the house more secure, it is less convenient to race to the keypad than to casually walk into the house.

NOTE 4

Security is often described as *sacrificing convenience for safety.*

Defining Information Security

Several terms describe security in an IT environment: *computer security, IT security, cybersecurity,* and *information assurance*, to name just a few. Whereas each has its share of proponents and slight variations of meanings, the term *information security* may be the most appropriate because it is the broadest: protecting information from harm. Information security is often used to describe the tasks of securing digital information, whether it is manipulated by a microprocessor (such as on a personal computer), preserved on a storage device (such as a hard drive or USB flash drive), or transmitted over a network (such as a local area network or the Internet).

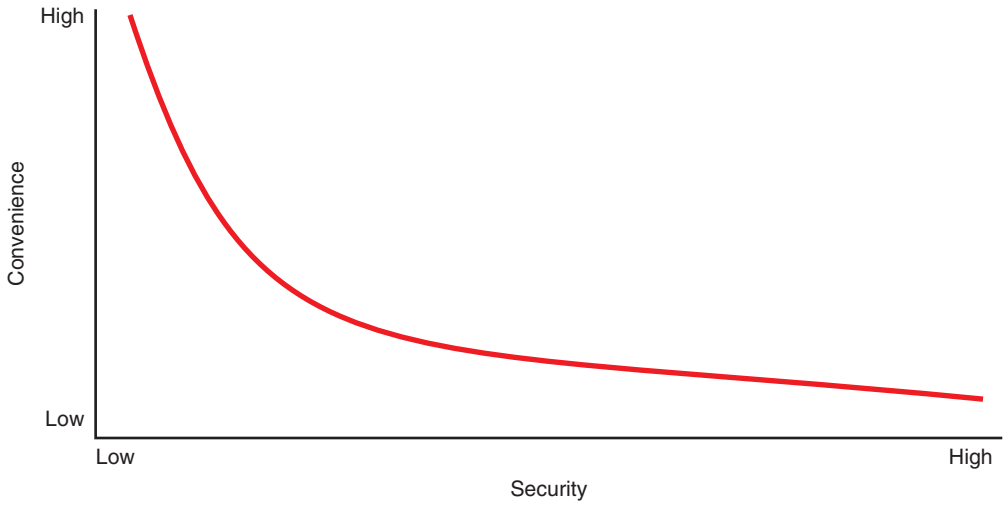


Figure 1-1 Relationship of security to convenience

CAUTION

Information security should not be viewed as a war to win or lose. Just as crimes such as burglary can never be completely eradicated, neither can attacks against technology devices. The goal is not achieving complete victory but instead maintaining equilibrium: as attackers take advantage of a weakness in a defense, defenders must respond with an improved defense. Information security is an endless cycle between attacker and defender.

Information security cannot completely prevent successful attacks or guarantee that a system is totally secure, just as the security measures taken for a house can never guarantee complete safety from a burglar. The goal of information security is to ensure that protective measures are properly implemented to ward off attacks, prevent the total collapse of the system when a successful attack does occur, and recover as quickly as possible. Thus, information security is first *protection*.

Second, information security is intended to protect *information* that provides value to people and enterprises. Known as the *CIA Triad*, three protections must be extended over information:

1. *Confidentiality.* Only approved individuals should be able to access sensitive information. For example, the credit card number used to make an online purchase must be kept secure and unavailable to unapproved entities. *Confidentiality* ensures that only authorized parties can view the information. Providing confidentiality can involve several security tools, ranging from software to encrypt the credit card number stored on the web server to door locks to prevent access to those servers.
2. *Integrity. Integrity* ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of an online purchase, an attacker who could change the amount of a purchase from $10,000.00 to $1.00 would violate the integrity of the information.
3. *Availability.* Information has value if the authorized parties who are assured of its integrity can access the information. *Availability* ensures that data is accessible to only authorized users and not to unapproved individuals. For example, the total number of items ordered as the result of an online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer, but the information should not be available to a competitor.

Because information is stored on computer hardware, manipulated by software, and transmitted by communications, each of these areas must be protected. The third objective of information security is to protect the integrity, confidentiality, and availability of information *on the devices that store, manipulate, and transmit the information.*

Protection is achieved through a process that combines three entities. As shown in Figure 1-2, information and hardware, software, and communications are protected in three layers: *products*, *people*, and *policies and procedures*. The procedures enable people to understand how to use products to protect information.

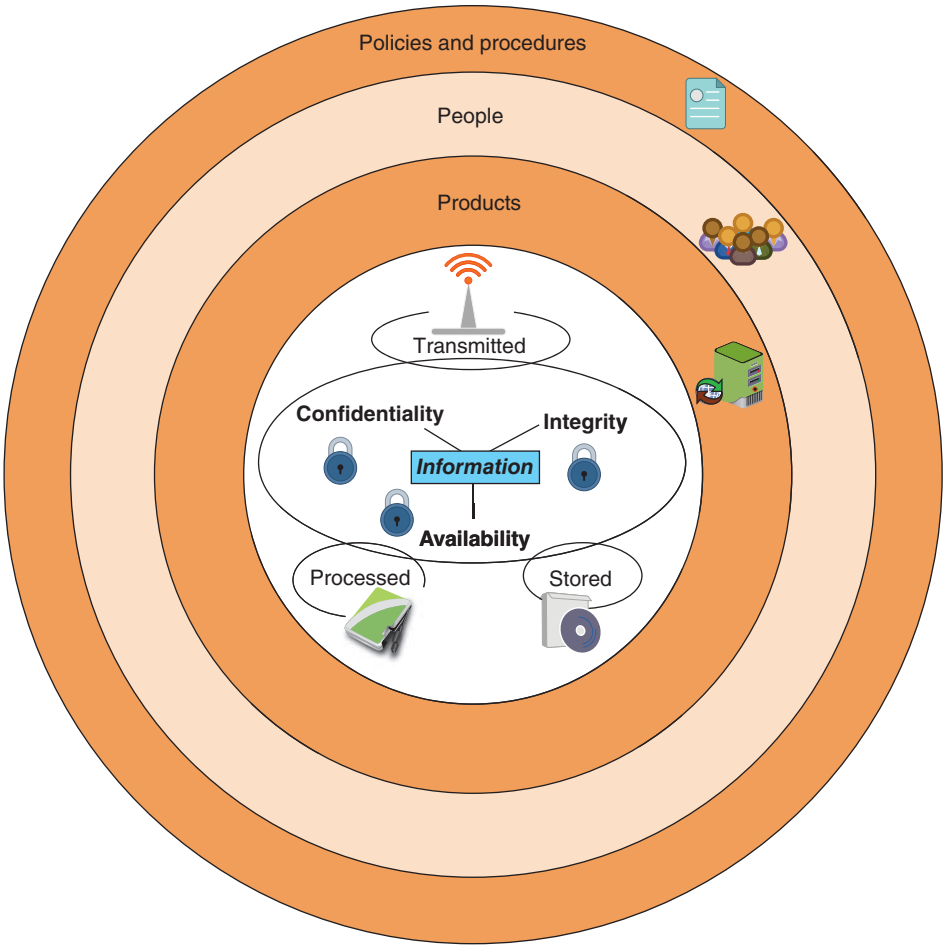


Figure 1-2 Information security layers

Thus, information security may be defined as *that which protects the integrity, confidentiality, and availability of information through products, people, and procedures on the devices that store, manipulate, and transmit the information.*

TWO RIGHTS & A WRONG

1. A security manager works on tasks identified by the CISO and resolves issues identified by technicians.
2. Since 2015, the number of unfilled cybersecurity positions has increased by 10 percent.
3. The relationship between security and convenience is inversely proportional: as security is increased, convenience is decreased.

See Appendix B for the answer.

WHO ARE THE THREAT ACTORS?

CERTIFICATION

1.5 Explain different threat actors, vectors, and intelligence sources.

In cybersecurity, a **threat actor** (also called a *malicious actor*) is an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users. The generic term *attacker* is also commonly used.

The very first cyberattacks were mainly for the threat actors to show off their technology skills (*fame*). However, that soon gave way to threat actors with the focused goal of financial gain (*fortune*). Financial cybercrime is often divided into three categories based on its targets:

- *Individual users*. The first category focuses on individuals as the victims. The threat actors steal and use stolen data, credit card numbers, online financial account information, or Social Security numbers to profit from their victims or send millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography.
- *Enterprises*. The second category focuses on enterprises and business organizations. Threat actors attempt to steal research on a new product so that they can sell it to an unscrupulous foreign supplier who then builds an imitation model of the product to sell worldwide. This deprives the legitimate business of profits after investing hundreds of millions of dollars in product development, and because these foreign suppliers are in a different country, they are beyond the reach of domestic enforcement agencies and courts.
- *Governments*. Governments are also the targets of threat actors. If the latest information on a new missile defense system can be stolen, it can be sold—at a high price—to that government's enemies. In addition, government information is often stolen and published to embarrass the government in front of its citizens and force it to stop what is considered a nefarious action.

The **attributes**, or characteristic features, of the groups of threat actors can vary widely. Some groups have a high level of power and complexity (called **level of capability/sophistication**) with a massive network of resources, while others are "lone wolves" with minimal skills and no resources. In addition, some groups have deep **resources and funding** while others have none. Whereas some groups of threat actors may work within the enterprise (**internal**), others are strictly outside the organization (**external**). Finally, the **intent/motivation**—that is, the reason for the attacks—of the threat actors also varies widely.

In the past, the term **hacker** referred to a person who used advanced computer skills to attack computers. Because that title often carried a negative connotation, it was qualified in an attempt to distinguish between different types of the attackers. The types of hackers are summarized in Table 1-1.

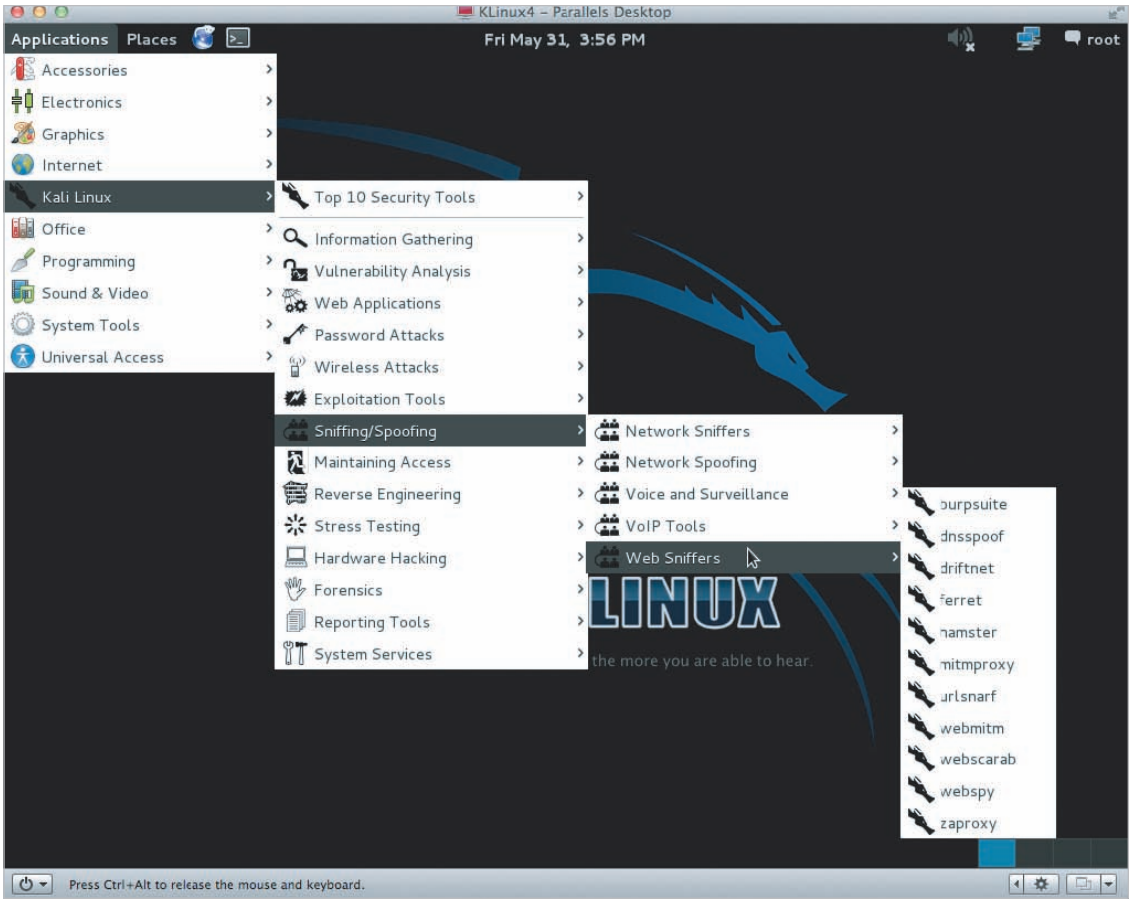
Table 1-1 Types of hackers

Hacker Type	Description
Black hat hackers	Threat actors who violate computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive).
White hat hackers	Also known as *ethical attackers*, they attempt to probe a system (with an organization's permission) for weaknesses and then privately provide that information back to the organization.
Gray hat hackers	Attackers who attempt to break into a computer system without the organization's permission (an illegal activity) but not for their own advantage; instead, they publicly disclose the attack in order to shame the organization into taking action.

However, these broad categories of hackers no longer accurately reflect the differences between attackers. Today threat actors are classified in more distinct categories, such as script kiddies, hacktivists, state actors, insiders, and others.

Script Kiddies

Script kiddies are individuals who want to perform attacks, yet lack the technical knowledge to carry them out. Script kiddies instead do their work by downloading freely available automated attack software (*scripts*) and use it to perform malicious acts. Figure 1-3 illustrates a widely available software package that launches a sophisticated attack when a user simply makes selections from a menu. Due to their lack of knowledge, script kiddies are not always successful in penetrating defenses, but when they are, they may end up causing damage to systems and data instead of stealing the data.



Source: Kali Linux

Figure 1-3 Menu of attack tools

Hacktivists

Individuals that are strongly motivated by ideology (for the sake of their principles or beliefs) are **hacktivists** (a combination of the words *hack* and *activism*). Most hacktivists do not explicitly call themselves "hacktivists," but the term is commonly used by security researchers and journalists to distinguish them from other types of threat actors.

In the past, the types of attacks by hacktivists often involved breaking into a website and changing its contents as a means of making a political statement. (One hacktivist group changed the website of the U.S. Department of Justice to read *Department of Injustice*.) Other attacks were retaliatory: hacktivists have disabled a bank's website because the bank stopped accepting online payments deposited into accounts belonging to groups supported by the hacktivists. Today many hacktivists work through disinformation campaigns by spreading fake news and supporting conspiracy theories.

NOTE 5

Hacktivists were particularly active during the coronavirus disease (COVID-19) pandemic of 2020. One large group of what were considered far-right neo-Nazi hacktivists embarked on a months-long disinformation campaign designed to weaponize the pandemic by questioning scientific evidence and research. In another instance, thousands of breached email addresses and passwords from U.S. and global health organizations—including the U.S. National Institutes of Health, CDC, and the World Health Organization—were distributed on Twitter by these groups to harass and distract the health organizations.

State Actors

Instead of using an army to march across the battlefield to strike an adversary, governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. These attackers are known as **state actors**. Their foes may be foreign governments or even citizens of their own nation that the government considers