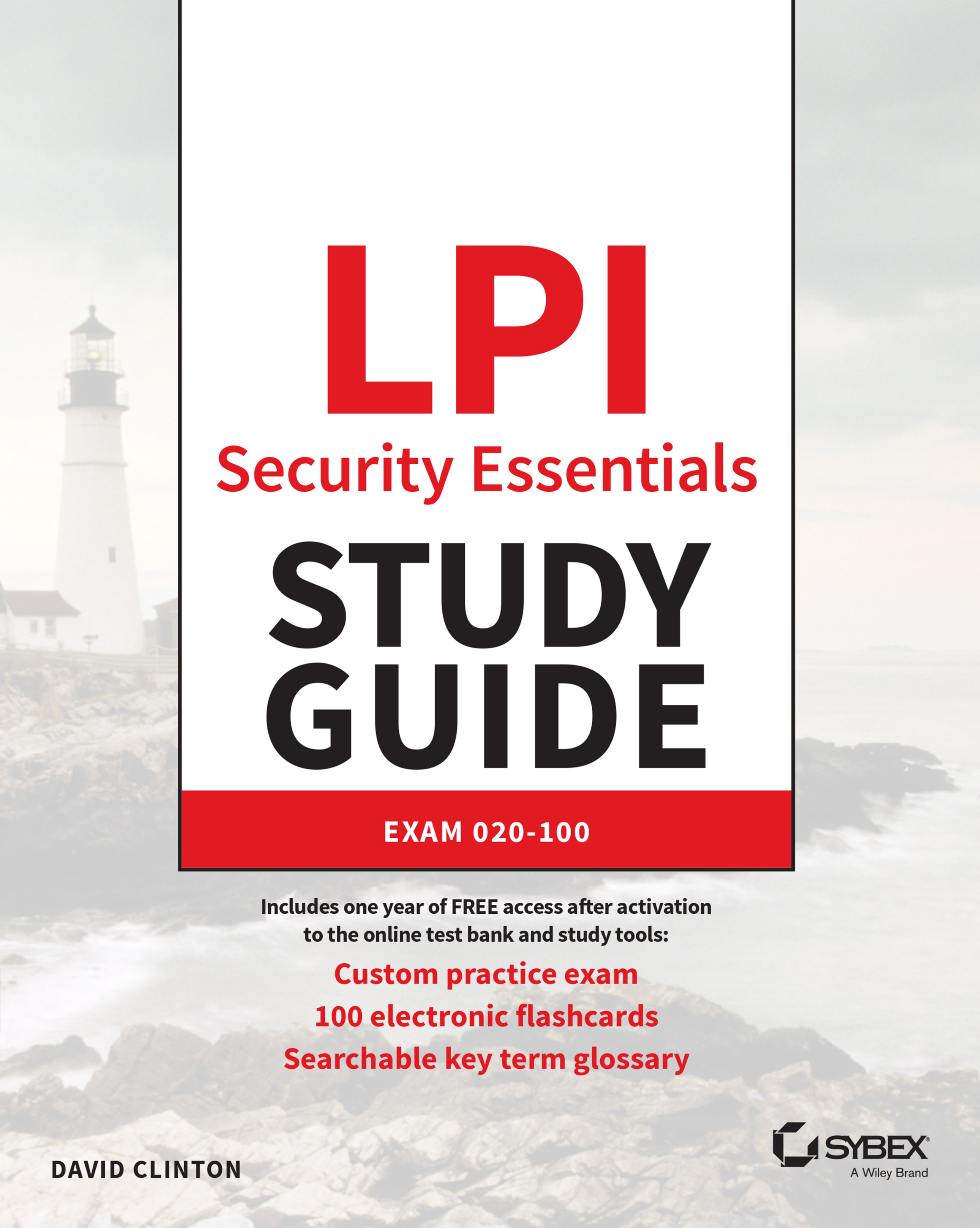

LPI

Security Essentials

STUDY GUIDE

EXAM 020-100

Includes one year of FREE access after activation
to the online test bank and study tools:

Custom practice exam
100 electronic flashcards
Searchable key term glossary

SYBEX®
A Wiley Brand

DAVID CLINTON

LPI

Security Essentials Study Guide

LPI

Security Essentials Study Guide

Exam 020-100

David Clinton

SYBEX
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-394-19653-1
ISBN: 978-1-394-19655-5 (ebk.)
ISBN: 978-1-394-19654-8 (ebk.)

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at `www.wiley.com`.

Library of Congress Control Number: 2023936823

Cover image: © Jeremy Woodhouse/Getty Images
Cover design: Wiley

Acknowledgments

I would like to thank my wife for all her help and support through the long and demanding process of writing this book. And, once again, I'm indebted to all the great people at Wiley who helped me turn a plain old manuscript into a great teaching tool.

About the Author

David Clinton is a Linux server admin who has worked with IT infrastructure in both academic and enterprise environments. He has authored and co-authored technology books—including *AWS Certified Solutions Architect Study Guide: Associate SAA-C03 Exam, Fourth Edition* (Sybex, 2022)—and created dozens of video courses teaching Amazon Web Services and Linux administration, server virtualization, and IT security.

In a previous life, David spent 20 years as a high school teacher. He currently lives in Toronto, Canada, with his wife and family and can be reached through his website: `https://bootstrap-it.com`.

Contents at a Glance

Contents

Introduction

I often say that you earn the real payoff from a well-designed certification exam by carefully working through its objectives. Sure, having a pretty certificate to hang on your wall is nice. But the skills and understanding you'll gain from hitting all the key points of a program like this Security Essentials cert will take you a whole lot further.

The moment we connect our phones, laptops, and servers to the Internet, we're all living in a very dangerous neighborhood. And there's no single "set-it-and-forget-it" solution that'll reliably keep all the looming threats away. The only way you can even hope to protect yourself and your digital resources is to understand the kinds of vulnerabilities that could affect your infrastructure and the ways smart administration can maximize both harm prevention and mitigation. But there's more. Since the IT threat landscape changes so often, you'll also need to learn how to continuously monitor your infrastructure and keep up with developments in the technology world.

Whether you're a team manager, an IT professional, a developer, a data engineer, or even just a regular technology consumer, you'll be both safer and more effective at everything you do if you can understand and apply security best practices. So I encourage you to plan to take and pass the Linux Professional Institute's Security Essentials exam. But whatever your certification goals, you should definitely plan to master the content represented by the objectives. And this book was written to get you there.

Like the certification itself, the content in this *LPI Security Essentials Study Guide* is platform neutral. That means you can ignore the *Linux* in the title. Sure, the institute's initial mandate was to enable the broader adoption of the Linux operating system—and they've done a great job at it. But the same smart and highly experienced people who drive the institute's Linux curriculum development are also outstanding security professionals. And their expertise extends to all operating systems and all platform categories. If your equipment speaks binary, it's covered here.

Each of the book's chapters includes review questions to thoroughly test your understanding of the services you've seen. The questions were designed to help you realistically gauge your understanding and readiness for the exam. Although the difficulty level will vary between questions, it's all on target and relevant to both the exam and the real digital world. Once you complete a chapter's assessment, refer to Appendix A for the correct answers and detailed explanations.

What Does This Book Cover?

This book covers topics you need to know to prepare for the Security Essentials certification exam:

Chapter 1: Using Digital Resources Responsibly In this chapter you'll learn about protecting the digital rights and privacy of people with whom you interact,—including your own employees and the users of your services.

Chapter 2: What Are Vulnerabilities and Threats? Here you'll discover the scope of the many classes of threats against your infrastructure, including digital espionage, stolen credentials, and malware.

Chapter 3: Controlling Access to Your Assets Your first line of defense against the bad guys is the outer edge of your property. So learning to manage physical and network access to your resources is a big deal.

Chapter 4: Controlling Network Connections Before you can effectively audit and secure your networks, you'll need to understand how IP/TCP networking actually works. This chapter will introduce you to both general networking administration and the basics of network security.

Chapter 5: Encrypting Your Data at Rest What can I say? Obscuring your important data stores from prying eyes is a critical component of security. Learn why, how, and where it should be done.

Chapter 6: Encrypting Your Moving Data In this chapter you'll learn about website and email encryption, along with the care and feeding of virtual private networks (VPNs).

Chapter 7: Risk Assessment You'll never know how secure your infrastructure is until it comes under attack. Now who would you prefer launches this first attack? This is something you'd rather want to do yourself through the services of vulnerability scanners and penetration testers.

Chapter 8: Configuring System Backups and Monitoring Despite all your best efforts, you're going to lose important data at some point. If you're properly backed up, then you're singing. And the sooner you find out there's bad stuff happening, the happier your song will be.

Chapter 9: Resource Isolation Design Patterns The final chapter will discuss some important security design tools, like firewalls, sandboxes, and OS access control software.

About the Exam

Here's the Linux Professional Institute's description of the certification's "minimally qualified candidate":

> "The candidate has a basic understanding of common security threats of using computers, networks, connected devices, and IT services on premises and in the cloud. The candidate understands common ways to prevent and mitigate attacks against their personal devices and data. Furthermore, the candidate is able to use encryption to secure data transferred through a network and stored on storage devices and in the cloud. The candidate is able to apply common security best practices, protect private information,

> and secure their identity. The candidate is able to securely use IT services and to take responsibility for securing their personal computing devices, applications, accounts, and online profiles."

Exam Objectives

1 021 Security Concepts

1.1 021.1 Goals, Roles and Actors (weight: 1)

1.2 021.2 Risk Assessment and Management (weight: 2)

1.3 021.3 Ethical Behavior (weight: 2)

2 022 Encryption

2.1 022.1 Cryptography and Public Key Infrastructure (weight: 3)

2.2 022.2 Web Encryption (weight: 2)

2.3 022.3 Email Encryption (weight: 2)

2.4 022.4 Data Storage Encryption (weight: 2)

3 023 Node, Device and Storage Security

3.1 023.1 Hardware Security (weight: 2)

3.2 023.2 Application Security (weight: 2)

3.3 023.3 Malware (weight: 3)

3.4 023.4 Data Availability (weight: 2)

4 024 Network and Service Security

4.1 024.1 Networks, Network Services and the Internet (weight: 4)

4.2 024.2 Network and Internet Security (weight: 3)

4.3 024.3 Network Encryption and Anonymity (weight: 3)

5 025 Identity and Privacy

5.1 025.1 Identity and Authentication (weight: 3)

5.2 025.2 Information Confidentiality and Secure Communication (weight: 2)

5.3 025.3 Privacy Protection (weight: 2)

Objective Map

The exam covers five larger domains, with each domain broken down into objectives. The following table lists each domain and its weighting in the exam, along with the chapters in the book where that domain's objectives are primarily covered.

Objective	**Weight**	**Chapter(s)**
1. Security Concepts		
1.1 Goals, Roles and Actors	1	1, 2
1.2 Risk Assessment and Management	2	4, 7, 9
1.3 Ethical Behavior	2	1, 7
2. Encryption		
2.1 Cryptography and Public Key Infrastructure	3	5, 6
2.2 Web Encryption	2	6
2.3 Email Encryption	2	6
2.4 Data Storage Encryption	2	5
3. Node, Device and Storage Security		
3.1 Hardware Security	2	2, 3
3.2 Application Security	2	3, 6
3.3 Malware	3	2, 3
3.4 Data Availability	2	8
4. Network and Service Security		
4.1 Networks, Network Services and the Internet	4	2, 4, 9
4.2 Network and Internet Security	3	2, 4
4.3 Network Encryption and Anonymity	3	1, 2, 6
5. Identity and Privacy		
5.1 Identity and Authentication	3	3, 6
5.2 Information Confidentiality and Secure Communication	2	1, 2
5.3 Privacy Protection	2	1

How to Contact the Publisher

If you believe you have found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Assessment Test

1. Which of the following digital tools is the most likely to collect—and possibly share—your private information without your knowledge?

   A. A programming integrated development environment (IDE)

   B. A USB device

   C. A web browser

   D. A command-line interface (CLI) environment

2. What is a backdoor?

   A. A network port opened to permit remote SSH access

   B. An undocumented access route to a computer system

   C. A software package management system that runs in the background

   D. The rear plate on a rack-mounted server

3. Which of these device types share information wirelessly without the need for authentication?

   A. RFID

   B. Wi-Fi

   C. Cellular networks

   D. Ethernet

4. Which of the following are components that are often protected by passwords? (Choose three.)

   A. Connecting to the Internet

   B. UEFI firmware

   C. Screen saver

   D. OS logon

5. Which of the following software tools can analyze network packets?

   A. Nmap

   B. SSH

   C. Wireshark

   D. TCP/IP

6. Which of the following is a common drawback associated with the use of asymmetric encryption?

   A. It's a new and relatively untested technology.

   B. It takes a relatively long time to process transactions.

   C. It requires the potentially risky transfer of a decryption key.

   D. It requires significant compute resources to manage.

7. What makes strong website encryption so important?
   - A. It's the best way to protect the data on your storage drives.
   - B. It's a critical tool for reducing system memory usage.
   - C. It's the best way to ensure that your website data reaches your clients intact and without being intercepted.
   - D. It's the primary defense against DNS poisoning.

8. What best describes the purpose of vulnerability scanning?
   - A. To test your infrastructure's defenses
   - B. To search for system or network misconfigurations
   - C. To discover and implement mitigation operations
   - D. To simulate an actual attack against your infrastructure

9. What process provides ongoing monitoring of your system that can alert admins when dangerous events occur?
   - A. Intrusion detection
   - B. Penetration testing
   - C. Efficiency audits
   - D. Unit testing

10. What type of service can most effectively filter packets coming into and out of a network?
    - A. Block device managers
    - B. Network firewalls
    - C. Application load balancers
    - D. Auto scalers

Answers to Assessment Test

1. C. IDEs and CLIs are not, by default, configured to connect to remote services—much less share data with them. The vast majority of USB devices don't contain self-launching scripts that are capable of manipulating data.

2. B. A backdoor is an unauthorized and undocumented way to access a computer operating system—usually left open with the goal of illegally gaining control of local data and system activities.

3. A. Wi-Fi has built-in authentication methods, and cell networks require validation (through a SIM card, for instance). Ethernet connections are not wireless.

4. B, C, D. It's not common—or even necessarily easy—to prevent passwordless access to application software (like a web browser). Screen savers, BIOS and UEFI interfaces, and OS logins all have built-in password protection (if enabled).

5. C. Nmap can identify vulnerable or hostile network devices, but it doesn't analyze packets. SSH is a tool for launching a secure remote session. TCP/IP is a set of network communication protocols.

6. D. Asymmetric encryption is not a new technology. It's unlikely that you would notice any delays in processing. There's no need to transfer private keys for asymmetric encryption.

7. C. Website encryption won't protect your local data and won't reduce memory usage. While it can help prevent DNS poisoning, it's not the primary defense.

8. B. Testing defenses or simulating attacks is closer to "penetration testing." I have no idea what "discovering and implementing mitigation operations" might mean.

9. A. Penetration testing and efficiency audits don't provide ongoing monitoring, and unit tests are for DevOps teams, not sysadmins.

10. B. Load balancers are primarily concerned with directing traffic rather than filtering it. Auto scalers are built to adjust resource availability. Block device managers deal with storage volumes, not network traffic.