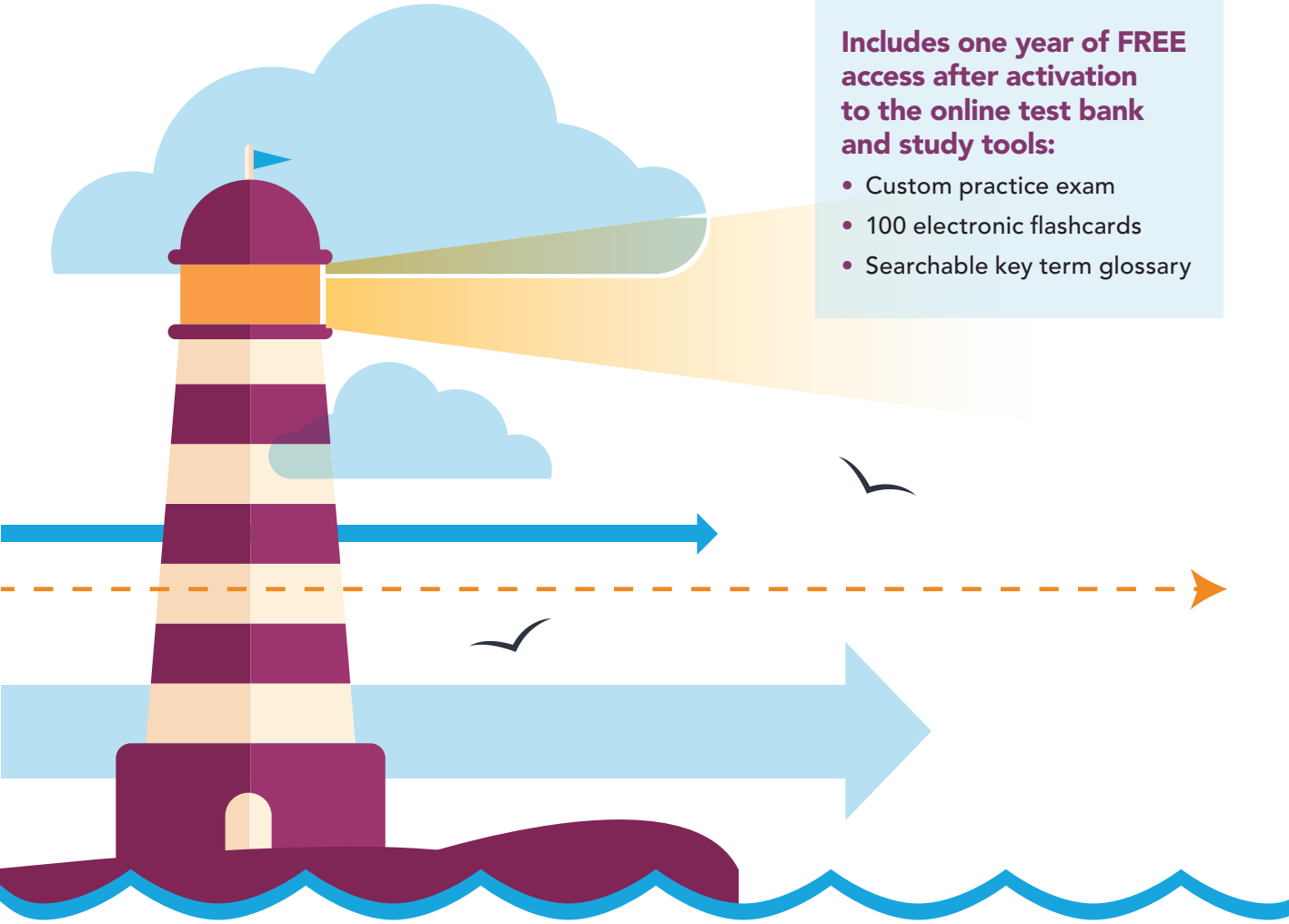


Includes one year of FREE access after activation to the online test bank and study tools:

- Custom practice exam
- 100 electronic flashcards
- Searchable key term glossary

LINUX® SECURITY FUNDAMENTALS

David Clinton

SYBEX®
A Wiley Brand

Linux®
Security Fundamentals

David Clinton

SYBEX®
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-78146-2
ISBN: 978-1-119-78157-8 (ebk)
ISBN: 978-1-119-78156-1 (ebk)

Library of Congress Control Number: 2020945159

Acknowledgments

I would like to thank my wife for all her help and support through the long and demanding process of writing these books. 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 and AWS Solutions Architect who has worked with IT infrastructure in both academic and enterprise environments. He has authored technology books—including *AWS Certified Solutions Architect Study Guide: Associate SAA-C01 Exam, Third Edition* (Sybex, 2020) and the *Ubuntu Bible* (Wiley, 2020)—and created more than 25 video courses teaching AWS and Linux administration, server virtualization, and IT security for Pluralsight.

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`.

About the Technical Editor

Ben Piper is a cloud and networking consultant who has co-authored multiple AWS study guides, including the *AWS Certified Solutions Architect Study Guide: Associate SAA-C01 Exam, Second Edition* (Sybex, 2019) and the *AWS Certified Cloud Practitioner Study Guide: CLF-C01 Exam* (Sybex, 2019). He's also created more than 20 technology training courses covering Amazon Web Services and Cisco routing and switching. You can contact Ben by visiting his website: `https://benpiper.com`.

Contents

Contents

Introduction

Right off the top, I'd like to be clear about exactly what this book is and what it's not. Linux Security Fundamentals *is* a guide to security best-practices for Linux admins. It is *not* however a comprehensive guide to deploying secure workloads in Linux environments.

So don't expect a lot of nuts and bolts demonstrations of complex administration tasks. We're not even going to cover the core basics of the Linux command line. I'll assume you've got all that already. This isn't a very *technical* book. In fact, there may be one or two chapters that don't even specifically mention Linux.

We won't talk, say, about the detailed configuration settings controlling cgroups or setting up effective and bullet-proof Nagios servers–as important as they are. For that kind of detail, you can consult Chris Negus' Linux Bible–or the Ubuntu Bible that I wrote in collaboration with Chris.

Instead, this book will quickly deliver the big-picture security knowledge that every admin should know (but often doesn't). The trick here, is that all that knowledge will delivered within a Linux context. So, for instance, along with the big-picture stuff you can expect to learn how to install the OpenVAS vulnerability scanner, construct a firewall using iptables, or build a custom Wireguard VPN. But don't expect to find that kind of technical detail in every chapter.

Why is a book like this necessary?

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 professional Linux admin, 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. And considering how Linux has come to dominate the web application, DevOps, internet of things, and mobile connectivity industries, getting security right on Linux is more critical than ever before.

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 better understand and remember the content. Although the difficulty level will vary between questions, it's all on target for the real digital world. Once you complete a chapter's assessment, refer to Appendix 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, such as firewalls, sandboxes, and OS access control software.

Interactive Online Learning Environment and Test Bank

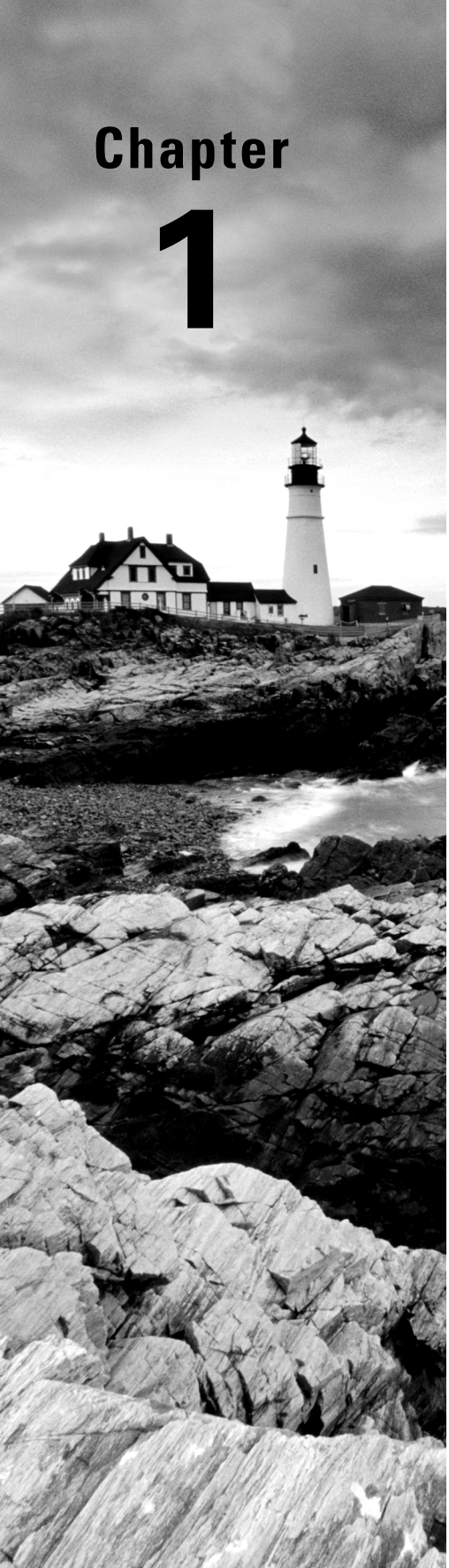
We've put together some really great online tools to help you absorb what you'll learn even better.

The online section includes the following:

Questions Many review questions are provided throughout this book and included online as part of the test bank. We've also also a practice exam online. Use these tools to test your knowledge of Linux security. The online test bank runs on multiple devices.

Flashcards The online text bank includes 100 flashcards specifically written to test your knowledge. Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning.

Go to `www.wiley.com/go/sybextestprep` to register and gain one year of FREE access after activation to this interactive online learning environment and test bank with study tools.



Chapter

1

Using Digital Resources Responsibly

"With great power comes great responsibility."

Words of wisdom. That's the message displayed for administrators when they log in for the first time to many Linux distributions. Who said those words first? Aristotle? Kant? Nope. Spider-Man's uncle. But hey, accept the truth from any source.

While we'll discuss protecting yourself from attack at length later in the book, this chapter is all about responsibilities. It's about your responsibilities both as a *consumer* of computer technologies and as an *administrator* of computer technologies. It's your job to make sure nothing you do online or with your devices causes harm to anyone's assets.

How is all this relevant to the world of information technology (IT) and, specifically, to IT security? Computers amplify your strengths. No matter how much you can remember, how fast you can calculate, or how many people's lives you can touch, it'll never come close to the scope of what you can do with a computing device and a network. So, given the power inherent in digital technologies and the depth of chaos such power can unleash, you *need* to understand how it can all go wrong before you set off to use it for good.

The rest of this chapter will explore the importance of considering how your actions can impact people's personal and property rights and privacy and how you can both ensure and assess the authenticity of online information.

I'm not a lawyer and this book doesn't pretend to offer legal advice, so we're not going to discuss some of the more esoteric places where individual rights can come into conflict with events driven by technology. Instead we'll keep it simple. People should be able to go about their business and enjoy their interactions with each other without having to worry about having physical, financial, or emotional injury imposed on them. And you should be ready to do whatever is necessary to avoid or prevent such injuries.

Protecting Personal Rights

These days, the greatest technology-based threats to an individual's personal well-being will probably exist on one or another social media platform. Facebook, Twitter, LinkedIn, and other online sites present opportunities for anyone to reach out to and communicate with millions or even billions of other users. This can make it possible to build entire businesses or social advocacy movements in ways that would have been unthinkable just a few years back. But, as we all now know, it also makes it possible to spread dangerous scams, political mischief, and social conflict.