



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<sup>®</sup> SECURITY FUNDAMENTALS

David Clinton

 **SYBEX**<sup>®</sup>  
A Wiley Brand



# Linux<sup>®</sup>

## Security Fundamentals



David Clinton

 **SYBEX<sup>®</sup>**  
A Wiley Brand

Copyright © 2021 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-78146-2

ISBN: 978-1-119-78157-8 (ebk)

ISBN: 978-1-119-78156-1 (ebk)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2020945159

**TRADEMARKS:** Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. Linux is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

# 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

<i>Introduction</i>		<i>xiii</i>
<b>Chapter 1</b>	Using Digital Resources Responsibly	1
<b>Chapter 2</b>	What Are Vulnerabilities and Threats?	15
<b>Chapter 3</b>	Controlling Access to Your Assets	33
<b>Chapter 4</b>	Controlling Network Connections	59
<b>Chapter 5</b>	Encrypting Your Data at Rest	81
<b>Chapter 6</b>	Encrypting Your Moving Data	93
<b>Chapter 7</b>	Risk Assessment	109
<b>Chapter 8</b>	Configuring System Backups and Monitoring	125
<b>Chapter 9</b>	Resource Isolation Design Patterns	143
<b>Appendix</b>	Answers to Review Questions	155
<i>Index</i>		<i>167</i>



# Contents

*Introduction*

*xiii*

<b>Chapter 1</b>	<b>Using Digital Resources Responsibly</b>	<b>1</b>
	Protecting Personal Rights	2
	Protecting Digital Privacy	4
	What Is Personal Data?	4
	Where Might My Personal Data Be Hanging Out?	4
	What Are My Responsibilities as a Site Administrator?	6
	Can Escaped Genies Be Forced Back into Their Bottles?	6
	What Can I Do as a User?	7
	Establishing Authenticity	7
	Think About the Source	8
	Be Aware of Common Threat Categories	8
	Summary	9
	Back to the Basics	10
	Review Questions	11
<b>Chapter 2</b>	<b>What Are Vulnerabilities and Threats?</b>	<b>15</b>
	The Basics: What Are We Trying to Accomplish Here?	16
	What Are Vulnerabilities and Threats?	17
	What Can Be Exploited?	17
	Who's Doing the Exploiting?	18
	Why Do They Attack?	19
	Common Vulnerabilities	20
	Software Vulnerabilities	20
	Hardware Vulnerabilities	21
	Bioware Vulnerabilities	21
	Digital Espionage	21
	USB Devices	21
	Backdoors	22
	Wireless Entry Points	22
	Stolen Credentials	23
	Data Breaches	23
	Identity Theft (Besides Breaches)	24
	Malware	24
	Network-Based Attacks	25
	Man-in-the-Middle Attacks	25
	Denial-of-Service and Distributed Denial-of-Service Attacks	26
	Network Routing Attacks	26

	Summary	26
	Back to the Basics	27
	Review Questions	28
<b>Chapter 3</b>	<b>Controlling Access to Your Assets</b>	<b>33</b>
	Controlling Physical Access	34
	Understanding Your Devices	34
	Protecting Your Devices	36
	Managing Authentication Through Effective Password Use	38
	Managing Authorization Through Permissions	44
	Controlling Network Access	45
	Firewalls	45
	Virus and Malware Protection	48
	Educating Your Users	49
	Controlling Software Sources	50
	PC Software Repositories	51
	Mobile Package Management	51
	Summary	52
	Back to the Basics	52
	Review Questions	54
<b>Chapter 4</b>	<b>Controlling Network Connections</b>	<b>59</b>
	Understanding Network Architecture	60
	The Transmission Control Protocol	60
	The Internet Protocol	61
	Understanding the Domain Name System	64
	Auditing Networks	65
	Network Auditing Tools	66
	Automating Audits	70
	Securing Networks	71
	Patch Your Software	71
	Physically Secure Your Infrastructure	73
	Secure Your Network Behavior	73
	Other Stuff	74
	Summary	74
	Back to the Basics	75
	Review Questions	76
<b>Chapter 5</b>	<b>Encrypting Your Data at Rest</b>	<b>81</b>
	What Is Encryption?	82
	Encryption Usage Patterns	85
	What Should You Encrypt?	85
	Understanding Hashing vs. Encryption	86
	What Are Blockchains?	86

	Encryption Technologies	87
	Summary	89
	Back to the Basics	89
	Review Questions	90
<b>Chapter 6</b>	<b>Encrypting Your Moving Data</b>	<b>93</b>
	Website Encryption	94
	Why You Should Use Encryption	95
	How Website Encryption Works	96
	Generating Certificates	98
	Email Encryption	99
	GNU Privacy Guard	100
	Does Gmail Encrypt Your Emails?	100
	Working with VPN Connections and Software Repositories	100
	Securing Your Actions Using VPNs	101
	Securing Transfers from Software Repositories	104
	Summary	105
	Back to the Basics	105
	Review Questions	106
<b>Chapter 7</b>	<b>Risk Assessment</b>	<b>109</b>
	Conducting Open Source Intelligence Gathering	111
	Accessing Public Vulnerability Databases	112
	Vulnerability Data Frameworks	112
	Vulnerability Data Formats	113
	Vulnerability Data Metrics	114
	Vulnerability Data Management Tools	114
	Conducting Vulnerability Scans	115
	Conducting Penetration Tests	117
	Attack Vectors	118
	Tooling Frameworks	118
	Follow-Up	119
	Summary	119
	Back to the Basics	120
	Review Questions	121
<b>Chapter 8</b>	<b>Configuring System Backups and Monitoring</b>	<b>125</b>
	Why You Need to Get Backups Right the First Time	127
	Appreciating the Risks	128
	Spreading Your Backups Across Multiple Sites	129
	Testing Your Backups	130
	Meeting Regulatory Compliance	131

	Backup Types	132
	Incremental Backups	132
	Differential Backups	133
	Backup Life Cycles	133
	Multitier Backups	133
	Multisite Storage Solutions	134
	Disaster Recovery Planning	134
	Configuring Monitoring and Alerts	135
	Working with System Logs	135
	Intrusion Detection	136
	Summary	137
	Back to the Basics	138
	Review Questions	139
<b>Chapter 9</b>	<b>Resource Isolation Design Patterns</b>	<b>143</b>
	Configuring Network Firewalling	145
	Balancing Public and Private Networks	145
	Building Isolated Development Environments	147
	Working with Sandbox Environments	148
	Use Cases for Sandboxes	148
	Sandbox Designs	149
	Controlling Local System Access	150
	Configuring Mandatory Access Controls	150
	Setting Usage Quotas	151
	Summary	152
	Back to the Basics	152
	Review Questions	153
<b>Appendix</b>	<b>Answers to Review Questions</b>	<b>155</b>
	Chapter 1: Using Digital Resources Responsibly	156
	Chapter 2: What are Vulnerabilities and Threats?	157
	Chapter 3: Controlling Access to Your Assets	158
	Chapter 4: Controlling Network Connections	160
	Chapter 5: Encrypting Your Data at Rest	161
	Chapter 6: Encrypting Your Moving Data	162
	Chapter 7: Risk Assessment	163
	Chapter 8: Configuring System Backups and Monitoring	165
	Chapter 9: Resource Isolation Design Patterns	166
	<i>Index</i>	167

# 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 be 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](http://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.