



Red Hat and IT Security

With Red Hat Ansible, Red Hat
OpenShift, and Red Hat
Security Auditing

—
Rithik Chatterjee

Apress®

Red Hat and IT Security

**With Red Hat Ansible, Red Hat
OpenShift, and Red Hat
Security Auditing**

Rithik Chatterjee

Apress®

Red Hat and IT Security

Rithik Chatterjee
Pune, Maharashtra, India

ISBN-13 (pbk): 978-1-4842-6433-1
<https://doi.org/10.1007/978-1-4842-6434-8>

ISBN-13 (electronic): 978-1-4842-6434-8

Copyright © 2021 by Rithik Chatterjee

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Divya Modi
Development Editor: Matthew Moodie
Coordinating Editor: Divya Modi

Cover designed by eStudioCalamar

Cover image designed by Pixabay

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, Suite 4600, New York, NY 10004-1562, USA. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-6433-1. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

*This book is dedicated to my parents: Rita and Ashish;
thank you for always supporting and encouraging me
to pursue my ambitions.*

Table of Contents

About the Author	xiii
About the Technical Reviewer	xv
Acknowledgments	xvii
Introduction	xix
Chapter 1: Introduction to IT Security	1
Basics of Networking	1
Firewalls	2
Virtual Private Network.....	2
Virtual Private Cloud	2
DHCP.....	3
Domain Name System	3
TCP	4
UDP	4
Simple Network Management Protocol.....	5
SSH.....	6
HTTP	6
SSL/TLS	7
Network Address Translation.....	7
Port Forwarding.....	8
IT Infrastructure Elements	8
Switching vs. Routing.....	8
Domain Controller.....	9

TABLE OF CONTENTS

Database Server	9
Application Server	10
Load Balancing Server	10
Linux System Administration Essential Concepts	10
Directory Services	11
LDAP	11
File Systems in Linux.....	13
Block Storage	15
Security Basics in Linux.....	15
Access Control Lists (ACLs)	15
SELinux.....	16
Firewall Daemon (Firewalld).....	18
Standardizing Security in Network and System Administration	20
Confidentiality.....	20
Integrity	20
Availability	21
Chapter 2: Red Hat Hybrid Cloud Infrastructure	23
Basics of Cloud Infrastructure.....	23
What Is Cloud Computing?	23
Cloud Computing Services	26
Cloud Bursting	30
Security in Cloud Infrastructure.....	31
Introduction to Hybrid Cloud Architecture	32
Operating Hybrid Clouds.....	34
Cloud First	37
Migration	38
Flexibility	40
Tiered Hybrid Strategy.....	40

Benefits of Tiered Hybrid Implementation	41
Analytical Hybrid Infrastructure.....	42
Hybrid Edge Cloud Computing.....	42
Modern Hybrid Cloud Architecture	43
Security in Hybrid Clouds	44
Red Hat Cloud Suite	45
Red Hat CloudForms.....	46
Red Hat Virtualization	48
Red Hat OpenStack Platform	48
Red Hat OpenShift Container Platform	48
Advantages of CloudSuite.....	49
Orchestration with Red Hat OpenShift	50
OpenShift Container Platform (Red Hat OCP).....	51
Compatibility with Hybrid Cloud	51
OpenShift Security.....	52
Distinctive Features.....	53
Kubernetes	54
OCP Life Cycle	60
OCP Installation	61
Installation Procedure.....	62
Chapter 3: Security in DevOps and Automation.....	65
Categories of DevOps.....	65
Automation	66
Continuous Integration (CI).....	66
Continuous Testing (CT)	66
Agile Development.....	67
Enterprise Systems Management (ESM).....	67

TABLE OF CONTENTS

Continuous Delivery vs. Continuous Deployment.....	68
Continuous Delivery (CD).....	68
Continuous Deployment (CD).....	68
Continuous Monitoring.....	69
Benefits of DevOps.....	70
Scalability.....	70
Speed.....	70
Innovation.....	71
Agility.....	71
Qualitative Growth.....	72
Reliability.....	72
Cost-Effective.....	72
Evolution of DevSecOps.....	72
DevSecOps in Environment and Data Security.....	77
DevSecOps in CI/CD Pipeline.....	78
Infrastructure as Code and Security as Code.....	80
Infrastructure as Code (IaC).....	80
Security as Code (SaC).....	85
Automation with Red Hat Ansible Automation Platform.....	88
Ansible Components.....	90
Using Ansible.....	91
Building an Inventory.....	94
Default Groups.....	95
Ansible Playbook.....	99
DevSecOps in OpenShift.....	102
Red Hat Consulting.....	104

Chapter 4: Red Hat Hyperconverged Infrastructure.....	105
Obsolescence of Legacy Infrastructure.....	105
What Is Hyperconverged Infrastructure?	106
HCI Architecture	109
Databases.....	111
Analytics and Logging	112
Data Security	112
Data Storage.....	113
Edge Computing	113
Desktop as a Service (DaaS)	114
Programming.....	114
General Uses	114
Red Hat Hyperconverged Infrastructure for Virtualization	115
Core Operations.....	117
Key Features.....	119
Red Hat Virtualization.....	119
Elements of Red Hat Virtualization	121
Security in Red Hat Virtualization	124
Configuration of sVirt.....	125
Flexibility with Red Hat Gluster Storage.....	126
Red Hat Hyperconverged Infrastructure for Cloud.....	135
Cloud Computing with Red Hat OpenStack Platform (RHOSP)	137
Scalability with Red Hat Ceph Storage.....	143
Hyperconverged Infrastructure Security Best Practices	146
Secure Individual Components.....	146
Security Centralization	147
Accessibility	148
Security Policies Implementation	148

TABLE OF CONTENTS

Chapter 5: Red Hat Smart Management and Red Hat Insights149

Red Hat Satellite Architecture 150

Core System Elements 154

 Organizations..... 155

 Locations 155

 Life-Cycle Environments..... 156

 Provisioning..... 156

 Kickstart 157

 PXE Booting 157

Infrastructure Controlling with Red Hat Smart Management..... 160

Predictive Analytics Using Red Hat Insights..... 162

 Advisor Service..... 164

 Vulnerability Service..... 167

 Security Rules 168

 Compliance Service..... 169

 System Comparison / Drift Analysis 171

 System Baselines 173

 Reference Point 173

 System Facts..... 174

 Insights Policies..... 174

 Webhooks 175

 System Patching Using Ansible Playbooks..... 175

Chapter 6: Red Hat Security Auditing177

IT System Auditing 177

General Controls vs. Application Controls 179

Risk Analysis 182

System Security 184

Control Objectives and Environment.....	184
Finding	185
Best Practices for Red Hat System Audit	186
RHEL Audit Use Cases	187
Audit Configuration.....	190
Evaluate Vulnerabilities and Verify Compliance.....	193
Conclusion	197
Chapter 7: Case Studies.....	199
Case Study 1: Anonymous.....	199
Context	199
Policies and Controls That Could Have Helped	201
Case Study 2: Sony Pictures Entertainment (2014).....	205
Context	205
Policies and Controls That Could Have Helped	207
Case Study 3: Capital One (2019).....	214
Context	214
Policies and Controls That Could Have Helped	217
Additional Case Studies	220
Bangladesh Bank Cyber Heist (2016)	220
Facebook–Cambridge Analytica Data Scandal (2018).....	221
Twitter Hack (2020)	221
References.....	223
Index.....	225