

[DOC] Selinux By Example Using Security Enhanced Linux David Caplan

Right here, we have countless ebook **selinux by example using security enhanced linux david caplan** and collections to check out. We additionally manage to pay for variant types and next type of the books to browse. The enjoyable book, fiction, history, novel, scientific research, as skillfully as various new sorts of books are readily friendly here.

As this selinux by example using security enhanced linux david caplan, it ends occurring instinctive one of the favored books selinux by example using security enhanced linux david caplan collections that we have. This is why you remain in the best website to look the amazing books to have.

SELinux by Example-Frank Mayer 2006-07-27 SELinux: Bring World-Class Security to Any Linux Environment! SELinux offers Linux/UNIX integrators, administrators, and developers a state-of-the-art platform for building and maintaining highly secure solutions. Now that SELinux is included in the Linux 2.6 kernel—and delivered by default in Fedora Core, Red Hat Enterprise Linux, and other major distributions—it's easier than ever to take advantage of its benefits. SELinux by Example is the first complete, hands-on guide to using SELinux in production environments. Authored by three leading SELinux researchers and developers, it illuminates every facet of working with SELinux, from its architecture and security object model to its policy language. The book thoroughly explains SELinux sample policies— including the powerful new Reference Policy—showing how to quickly adapt them to your unique environment. It also contains a comprehensive SELinux policy language reference and covers exciting new features in Fedora Core 5 and the upcoming Red Hat Enterprise Linux version 5. • Thoroughly understand SELinux's access control and security mechanisms • Use SELinux to construct secure systems from the ground up • Gain fine-grained control over kernel resources • Write policy statements for type enforcement, roles, users, and constraints • Use optional multilevel security to enforce information classification and manage users with diverse clearances • Create conditional policies that can be changed on-the-fly • Define, manage, and maintain SELinux security policies • Develop and write new SELinux security policy modules • Leverage emerging SELinux technologies to gain even greater flexibility • Effectively administer any SELinux system

SELinux by Example-Frank Mayer 2007 SELinux: Bring World-Class Security to Any Linux Environment! SELinux offers Linux/UNIX integrators, administrators, and developers a state-of-the-art platform for building and maintaining highly secure solutions. Now that SELinux is included in the Linux 2.6 kernel—and delivered by default in Fedora Core, Red Hat Enterprise Linux, and other major distributions—it's easier than ever to take advantage of its benefits. SELinux by Example is the first complete, hands-on guide to using SELinux in production environments. Authored by three leading SELinux researchers and developers, it illuminates every facet of working with SELinux, from its architecture and security object model to its policy language. The book thoroughly explains SELinux sample policies— including the powerful new Reference Policy—showing how to quickly adapt them to your unique environment. It also contains a comprehensive SELinux policy language reference and covers exciting new features in Fedora Core 5 and the upcoming Red Hat Enterprise Linux version 5. • Thoroughly understand SELinux's access control and security mechanisms • Use SELinux to construct secure systems from the ground up • Gain fine-grained control over kernel resources • Write policy statements for type enforcement, roles, users, and constraints • Use optional multilevel security to enforce information classification and manage users with diverse clearances • Create conditional policies that can be changed on-the-fly • Define, manage, and maintain SELinux security policies • Develop and write new SELinux security policy modules • Leverage emerging SELinux technologies to gain even greater flexibility • Effectively administer any SELinux system

SELinux-Bill McCarty 2005 Offers a readable, practical introduction and step-by-step procedural manual for the installation, configuration, and use of SELinux, a kernel module and set of Linux programs developed by the National Security Agency to help protect computers running on Linux. Original. (All

users)

SELinux System Administration-Sven Vermeulen 2013-09-24 A step-by-step guide to learn how to set up security on Linux servers by taking SELinux policies into your own hands. Linux administrators will enjoy the various SELinux features that this book covers and the approach used to guide the admin into understanding how SELinux works. The book assumes that you have basic knowledge in Linux administration, especially Linux permission and user management.

SELinux Cookbook-Sven Vermeulen 2014-09-23 If you are a Linux system administrator or a Linux-based service administrator and want to fine-tune SELinux to implement a supported, mature, and proven access control system, then this book is for you. Basic experience with SELinux enabled distributions is expected.

Security Strategies in Linux Platforms and Applications-Michael Jang 2015-10-13 "The Second Edition of Security Strategies in Linux Platforms and Applications opens with a discussion of risks, threats, and vulnerabilities. Part 2 discusses how to take advantage of the layers of security and the modules associated with AppArmor and SELinux. Part 3 looks at the use of open source and proprietary tools when building a layered security strategy"--

Exploring SE for Android-William Confer 2015-02-24 This book is intended for developers and engineers with some familiarity of operating system concepts as implemented by Linux. A basic background in C code would be helpful. Their positions range from hobbyists wanting to secure their Android powered creations to OEM engineers building handsets to engineers of emerging areas where Android is seeing growth.

E-Technologies: Embracing the Internet of Things-Esma Aïmeur 2017-06-09 This book constitutes the refereed proceedings of the 7th International Conference on E-Technologies, MCETECH 2017, held in Ottawa, ON, Canada, in May 2017. This year's conference drew special attention to the ever-increasing role of the Internet of Things (IoT); and the contributions span a variety of application domains such as e-Commerce, e-Health, e-Learning, and e-Justice, comprising research from models and architectures, methodology proposals, prototype implementations, and empirical validation of theoretical models. The 19 papers presented were carefully reviewed and selected from 48 submissions. They were organized in topical sections named: pervasive computing and smart applications; security, privacy and trust; process modeling and adaptation; data analytics and machine learning; and e-health and e-commerce.

Securing Docker-Scott Gallagher 2016-03-30 Learn how to secure your Docker environment and keep your environments secure irrespective of the threats out there
About This Book Gain confidence in using Docker for containerization without compromising on security This book covers different techniques to help you develop your container security skills It is loaded with practical examples and real-world scenarios to secure your container-based applications
Who This Book Is For This book is for developers who wish to use Docker as their testing platform as well as security professionals who are interested in securing Docker containers. You must be familiar with the basics of Docker.
What You Will Learn Find out how to secure your Docker hosts and nodes Secure your Docker components Explore different security measures/methods for Linux kernels Install and run the Docker Bench security application Monitor and report security issues Familiarize yourself with third-party tools such as Traffic Authorization, Summon, sVirt, and SELinux to secure your Docker environment
In Detail With the rising integration and adoption of Docker containers, there is a growing need to ensure their security. The purpose of this book is to provide techniques and enhance your skills to secure Docker containers easily and efficiently. The book starts by sharing the techniques to configure Docker components securely and explore the different security measures/methods one can use to secure the kernel. Furthermore, we will cover the best practices to report Docker security findings and will show you how you can safely report any security findings you come across. Toward the end, we list the internal and third-party tools that can help you immunize your Docker environment. By the end of this book, you will have a complete understanding of Docker security so you are able to protect your container-based applications.
Style and approach This book is your one-stop solution to resolve all your Docker security concerns. It will familiarize you with techniques to safeguard your applications that run on Docker containers.

Verification and Evaluation of Computer and Communication Systems-Belgacem Ben Hedia

Android Security Internals-Nikolay Elenkov 2014-10-14 There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In Android Security Internals, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions,

cryptographic providers, and device administration. You'll learn: -How Android permissions are declared, used, and enforced -How Android manages application packages and employs code signing to verify their authenticity -How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks -About Android's credential storage system and APIs, which let applications store cryptographic keys securely -About the online account management framework and how Google accounts integrate with Android -About the implementation of verified boot, disk encryption, lockscreen, and other device security features -How Android's bootloader and recovery OS are used to perform full system updates, and how to obtain root access With its unprecedented level of depth and detail, Android Security Internals is a must-have for any security-minded Android developer.

Linux Observability with BPF-David Calavera 2019-11-14 Build your expertise in the BPF virtual machine in the Linux kernel with this practical guide for systems engineers. You'll not only dive into the BPF program lifecycle but also learn to write applications that observe and modify the kernel's behavior; inject code to monitor, trace, and securely observe events in the kernel; and more. Authors David Calavera and Lorenzo Fontana help you harness the power of BPF to make any computing system more observable.

Familiarize yourself with the essential concepts you'll use on a day-to-day basis and augment your knowledge about performance optimization, networking, and security. Then see how it all comes together with code examples in C, Go, and Python. Write applications that use BPF to observe and modify the Linux kernel's behavior on demand Inject code to monitor, trace, and observe events in the kernel in a secure way—no need to recompile the kernel or reboot the system Explore code examples in C, Go, and Python Gain a more thorough understanding of the BPF program lifecycle

On the Move to Meaningful Internet Systems: OTM 2009-Robert Meersman 2009-10-26 This two-volume set LNCS 5870/5871 constitutes the refereed proceedings of the four confederated international conferences on Cooperative Information Systems (CoopIS 2009), Distributed Objects and Applications (DOA 2009), Information Security (IS 2009), and Ontologies, Databases and Applications of Semantics (ODBASE 2009), held as OTM 2009 in Vilamoura, Portugal, in November 2009. The 83 revised full papers presented together with 4 keynote talks were carefully reviewed and selected from a total of 234 submissions. Corresponding to the four OTM 2009 main conferences CoopIS, DOA, IS, and ODBASE the papers are organized in topical sections on workflow; process models; ontology challenges; network complexity; modeling cooperation; information complexity; infrastructure; information; aspect-oriented approaches for distributed middleware; distributed algorithms and communication protocols; distributed infrastructures for cluster and Grid computing; object-based, component-based, resource-oriented, event-oriented, and service-oriented middleware; peer-to-peer and centralized infrastructures; performance analysis of distributed computing systems; reliability, fault tolerance, quality of service, and real time support; self* properties in distributed middleware; software engineering for distributed middleware systems; security and privacy in a connected world; ubiquitous and pervasive computing; information systems security; privacy and authentication; security policies and verification; managing ontologies; using ontologies; event processing; dealing with heterogeneity; building knowledge bases; and XML and XML schema.

Practical Linux Topics-Chris Binnie 2015-12-30 Teaches you how to improve your hands-on knowledge of Linux using challenging, real-world scenarios. Each chapter explores a topic that has been chosen specifically to demonstrate how to enhance your base Linux system, and resolve important issues. This book enables sysadmins, DevOps engineers, developers, and other technical professionals to make full use of Linux's rocksteady foundation. Explore specific topics in networking, email, filesystems, encryption, system monitoring, security, servers, and more-- including systemd and GPG. Understand salient security concerns and how to mitigate them. Applicable to almost all Linux flavors--Debian, Red Hat, Ubuntu, Linux Mint, CentOS--Practical Linux Topics can be used to reference other Unix-type systems with little modification. Improve your practical know-how and background knowledge on servers and workstations alike, increase your ability to troubleshoot and ultimately solve the daily challenges encountered by all professional Linux users. Empower your Linux skills by adding Power Linux Topics to your library today. What You'll Learn Solve a variety of challenges faced by sysadmins and DevOps engineers Understand the security implications of the actions you take Study the history behind some of the packages that you are using for a greater in-depth understanding Become a professional at troubleshooting Extend your knowledge by learning about multiple OSs and third-party packages Who This Book Is For Having mastered the basics of running Linux systems this book takes you one step further to help you master the elements of Linux which you may have struggled with in the past. You have progressed past the basic stages of using Linux and want to delve into the more complex aspects. Practical Linux instantly offers

answers to problematic scenarios and provides invaluable information for future reference. It is an invaluable addition to any Linux library.

Operating System Security-Trent Jaeger 2008 "Operating systems provide the fundamental mechanisms for securing computer processing. Since the 1960s, operating systems designers have explored how to build "secure" operating systems - operating systems whose mechanisms protect the system against a motivated adversary. Recently, the importance of ensuring such security has become a mainstream issue for all operating systems. In this book, we examine past research that outlines the requirements for a secure operating system and research that implements example systems that aim for such requirements. For system designs that aimed to satisfy these requirements, we see that the complexity of software systems often results in implementation challenges that we are still exploring to this day. However, if a system design does not aim for achieving the secure operating system requirements, then its security features fail to protect the system in a myriad of ways. We also study systems that have been retro-fit with secure operating system features after an initial deployment. In all cases, the conflict between function on one hand and security on the other leads to difficult choices and the potential for unwise compromises. From this book, we hope that systems designers and implementers will learn the requirements for operating systems that effectively enforce security and will better understand how to manage the balance between function and security."--BOOK JACKET.

Linux in Action-David Clinton 2018 Linux in Action is a task-based tutorial that will give you the skills and deep understanding you need to administer a Linux-based system. This hands-on book guides you through 12 real-world projects so you can practice as you learn. Each chapter ends with a review of best practices, new terms, and exercises.

Red Hat Enterprise Linux Administration Unleashed-Tammy Fox 2007-04-20 This comprehensive guide can help you administer Red Hat Enterprise Linux 5 effectively in any production environment, no matter how complex or challenging. Long-time Red Hat insider Tammy Fox brings together today's best practices for the entire system lifecycle, from planning and deployment through maintenance and troubleshooting. Fox shows how to maximize your efficiency and effectiveness by automating day-to-day maintenance through scripting, deploying security updates via Red Hat Network, implementing central identity management services, and providing shared data with NFS and Samba. Red Hat Enterprise Linux 5 Administration Unleashed contains extensive coverage of network and web services, from the Apache HTTP server and Sendmail email services to remote login with OpenSSH. Fox also describes Red Hat's most valuable tools for monitoring and optimization and presents thorough coverage of security—including a detailed introduction to Security-Enhanced Linux (SELinux).

Hands-on Guide to the Red Hat Exams-Damian Tommasino 2011-04-12 Master every topic on Red Hat's new RHCSA™ and RHCE® exams. Assess your knowledge and focus your learning. Get the practical workplace knowledge you need! Start-to-finish RHCSA™ and RHCE® preparation from leading Linux system administrator, IT trainer, and certification expert Damian Tommasino! Master every RHCSA™ and RHCE® topic! Red Hat Enterprise Linux 6 local and network installation System services, runlevels, and bootup Disks, partitions, and file systems, including LUKS encryption Networking Package management User administration Logging, monitoring, and automation Kernel updates and tuning Security, including SELinux, firewalls, and policies Remote access, including SSH Apache, Squid, DNS, DHCP, NTP, and email NFS and Samba Client and network troubleshooting KVM virtualization Test your knowledge, build your confidence, and succeed! 22 hands-on RHCSA™ and RHCE® Labs, each with multiple real-world tasks Downloadable troubleshooting scripts Practical tutorials and real-world tips Exam tips Red Hat Enterprise Linux 6 Command Quick Reference Exclusive Red Hat exam prep advice and task lists Two full length lab-based practice exams Damian Tommasino (RHCE, RHCSA, MCSA, CCNA, CCENT, MCP, Security+, Network+, A+) is a Linux system administrator at TradeCard and CEO of Modular Learning Inc., an online IT training company. He blogs on Red Hat, Linux, and security at Security Nut (<http://secnut.blogspot.com>), and actively contributes to the popular IT exam certification forums at techexams.net.

Practical Linux Security Cookbook-Tajinder Kalsi 2016-04-29 Secure your Linux machines and keep them secured with the help of exciting recipes About This Book This book provides code-intensive discussions with detailed recipes that help you understand better and learn faster. More than 50 hands-on recipes to create and administer a secure Linux system locally as well as on a network Enhance file system security and local and remote user authentication by using various security tools and different versions of Linux for different tasks Who This Book Is For Practical Linux Security Cookbook is intended for all those Linux users who already have knowledge of Linux File systems and administration. You should be familiar with

basic Linux commands. Understanding Information security and its risks to a Linux system is also helpful in understanding the recipes more easily. However, even if you are unfamiliar with Information security, you will be able to easily follow and understand the recipes discussed. Since Linux Security Cookbook follows a practical approach, following the steps is very easy. What You Will Learn Learn about various vulnerabilities and exploits in relation to Linux systems Configure and build a secure kernel and test it Learn about file permissions and security and how to securely modify files Explore various ways to authenticate local users while monitoring their activities. Authenticate users remotely and securely copy files on remote systems Review various network security methods including firewalls using iptables and TCP Wrapper Explore various security tools including Port Sentry, Squid Proxy, Shorewall, and many more Understand Bash vulnerability/security and patch management In Detail With the growing popularity of Linux, more and more administrators have started moving to the system to create networks or servers for any task. This also makes Linux the first choice for any attacker now. Due to the lack of information about security-related attacks, administrators now face issues in dealing with these attackers as quickly as possible. Learning about the different types of Linux security will help create a more secure Linux system. Whether you are new to Linux administration or experienced, this book will provide you with the skills to make systems more secure. With lots of step-by-step recipes, the book starts by introducing you to various threats to Linux systems. You then get to walk through customizing the Linux kernel and securing local files. Next you will move on to manage user authentication locally and remotely and also mitigate network attacks. Finally, you will learn to patch bash vulnerability and monitor system logs for security. With several screenshots in each example, the book will supply a great learning experience and help you create more secure Linux systems. Style and approach An easy-to-follow cookbook with step-by-step practical recipes covering the various Linux security administration tasks. Each recipe has screenshots, wherever needed, to make understanding more easy.

LPIC-2 Linux Professional Institute Certification Study Guide-Roderick W. Smith 2011-05-09 The first book to cover the LPIC-2 certification Linux allows developers to update source code freely, making it an excellent, low-cost, secure alternative to alternate, more expensive operating systems. It is for this reason that the demand for IT professionals to have an LPI certification is so strong. This study guide provides unparalleled coverage of the LPIC-2 objectives for exams 201 and 202. Clear and concise coverage examines all Linux administration topics while practical, real-world examples enhance your learning process. On the CD, you'll find the Sybex Test Engine, electronic flashcards, and a glossary containing the most important terms you need to understand.. Prepares you for exams 201 and 202 of the Linux Professional Institute Certification Offers clear, concise coverage on exam topics such as the Linux kernel, system startup, networking configuration, system maintenance, domain name server, file sharing, and more Addresses additional key topics for the exams including network client management, e-mail services, system security, and troubleshooting This must-have study guide serves as an invaluable roadmap to attaining LPI certification.

Red Hat Enterprise Linux Server Cookbook-William Leemans 2015-12-23 Over 60 recipes to help you build, configure, and orchestrate RHEL 7 Server to make your everyday administration experience seamless About This Book Create fully unattended installations and deploy configurations without breaking a sweat Discover and kick-start the newest RHEL 7 configuration and management tools through an easy-to-follow, practical approach for a lazy system management Be guided by an experienced RHEL expert who is a certified Linux engineer with a passion for open source and open standards Who This Book Is For Red Hat Enterprise Linux Server Cookbook is for RHEL 7 system administrators and DevOps in need of a practical reference guide to troubleshoot common issues and quickly perform tasks. What You Will Learn Set up and configure RHEL 7 Server Use NetworkManager to configure all aspects of your network Manage virtual environments using libvirt Set up software repositories Secure and monitor your RHEL environment Configure SELinux, and create and apply its policies Create kickstart scripts to automatically deploy RHEL 7 systems Use Orchestration and configuration management tools to manage your environment In Detail Dominating the server market, the Red Hat Enterprise Linux operating system gives you the support you need to modernize your infrastructure and boost your organization's efficiency. Combining both stability and flexibility, RHEL helps you meet the challenges of today and adapt to the demands of tomorrow. This practical Cookbook guide will help you get to grips with RHEL 7 Server and automating its installation. Designed to provide targeted assistance through hands-on recipe guidance, it will introduce you to everything you need to know about KVM guests and deploying multiple standardized RHEL systems effortlessly. Get practical reference advice that will make complex networks setups look like child's play, and dive into in-depth coverage of configuring a RHEL system. Also including full recipe

coverage of how to set up, configuring, and troubleshoot SELinux, you'll also discover how secure your operating system, as well as how to monitor it. Style and approach This practical guide is packed full of hands-on recipes that provide quick solutions to the problems faced when building your RHEL 7 system from scratch using orchestration tools. Each topic is explained sequentially in the process of setting up a system and binding everything together.

Mastering Linux Security and Hardening-Donald Tevault 2018-01-11 A comprehensive guide to mastering the art of preventing your Linux system from getting compromised. Key Features Leverage this guide to confidently deliver a system that reduces the risk of being hacked Perform a number of advanced Linux security techniques such as network service detection, user authentication, controlling special permissions, encrypting file systems, and much more Master the art of securing a Linux environment with this end-to-end practical guide Book Description This book has extensive coverage of techniques that will help prevent attackers from breaching your system, by building a much more secure Linux environment. You will learn various security techniques such as SSH hardening, network service detection, setting up firewalls, encrypting file systems, protecting user accounts, authentication processes, and so on. Moving forward, you will also develop hands-on skills with advanced Linux permissions, access control, special modes, and more. Lastly, this book will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this book, you will be confident in delivering a system that will be much harder to compromise. What you will learn Use various techniques to prevent intruders from accessing sensitive data Prevent intruders from planting malware, and detect whether malware has been planted Prevent insiders from accessing data that they aren't authorized to access Do quick checks to see whether a computer is running network services that it doesn't need to run Learn security techniques that are common to all Linux distros, and some that are distro-specific Who this book is for If you are a systems administrator or a network engineer interested in making your Linux environment more secure, then this book is for you. Security consultants wanting to enhance their Linux security skills will also benefit from this book. Prior knowledge of Linux is mandatory.

Demystifying Internet of Things Security-Sunil Cheruvu 2019-08-13 Break down the misconceptions of the Internet of Things by examining the different security building blocks available in Intel Architecture (IA) based IoT platforms. This open access book reviews the threat pyramid, secure boot, chain of trust, and the SW stack leading up to defense-in-depth. The IoT presents unique challenges in implementing security and Intel has both CPU and Isolated Security Engine capabilities to simplify it. This book explores the challenges to secure these devices to make them immune to different threats originating from within and outside the network. The requirements and robustness rules to protect the assets vary greatly and there is no single blanket solution approach to implement security. Demystifying Internet of Things Security provides clarity to industry professionals and provides an overview of different security solutions What You'll Learn Secure devices, immunizing them against different threats originating from inside and outside the network Gather an overview of the different security building blocks available in Intel Architecture (IA) based IoT platforms Understand the threat pyramid, secure boot, chain of trust, and the software stack leading up to defense-in-depth Who This Book Is For Strategists, developers, architects, and managers in the embedded and Internet of Things (IoT) space trying to understand and implement the security in the IoT devices/platforms.

Moodle Security-Darko Miletić 2011-02-10 Learn how to install and configure Moodle in the most secure way possible.

Security for Linux on System z-Lydia Parziale 2013-01-10 No IT server platform is 100% secure and useful at the same time. If your server is installed in a secure vault, three floors underground in a double-locked room, not connected to any network and switched off, one would say it was reasonably secure, but it would be a stretch to call it useful. This IBM® Redbooks® publication is about switching on the power to your Linux® on System z® server, connecting it to the data and to the network, and letting users have access to this formidable resource space in a secure, controlled, and auditable fashion to make sure the System z server and Linux are useful to your business. As the quotation illustrates, the book is also about ensuring that, before you start designing a security solution, you understand what the solution has to achieve. The base for a secure system is tightly related to the way the architecture and virtualization has been implemented on IBM System z. Since its inception 45 years ago, the architecture has been continuously developed to meet the increasing demands for a more secure and stable platform. This book is intended for system engineers and security administrators who want to customize a Linux on System z environment to meet strict security, audit, and control regulations. For additional information, there is a tech note that describes the best practices for securing your network. It can be found at:

<http://www.redbooks.ibm.com/abstracts/tips0981.html?Open>

Apache Security-Ivan Ristic 2005 "The complete guide to securing your Apache web server"--Cover.

Fedora 13 Security-Enhanced Linux User Guide-Fedora Documentation Project 2010-07 The Fedora 13 SELinux user guide is for people with minimal or no experience with SELinux. ... This guide provides an introduction to fundamental concepts and practical applications of SELinux. After reading this guide you should have an intermediate understanding of SELinux--P. 8.

The Linux Programming Interface-Michael Kerrisk 2010-10-01 The Linux Programming Interface (TLPI) is the definitive guide to the Linux and UNIX programming interface—the interface employed by nearly every application that runs on a Linux or UNIX system. In this authoritative work, Linux programming expert Michael Kerrisk provides detailed descriptions of the system calls and library functions that you need in order to master the craft of system programming, and accompanies his explanations with clear, complete example programs. You'll find descriptions of over 500 system calls and library functions, and more than 200 example programs, 88 tables, and 115 diagrams. You'll learn how to: -Read and write files efficiently -Use signals, clocks, and timers -Create processes and execute programs -Write secure programs -Write multithreaded programs using POSIX threads -Build and use shared libraries -Perform interprocess communication using pipes, message queues, shared memory, and semaphores -Write network applications with the sockets API While The Linux Programming Interface covers a wealth of Linux-specific features, including epoll, inotify, and the /proc file system, its emphasis on UNIX standards (POSIX.1-2001/SUSv3 and POSIX.1-2008/SUSv4) makes it equally valuable to programmers working on other UNIX platforms. The Linux Programming Interface is the most comprehensive single-volume work on the Linux and UNIX programming interface, and a book that's destined to become a new classic.

Red Hat RHCSA 8 Cert Guide-Sander van Vugt 2019-11-04 This is the eBook version of the print title.

Learn, prepare, and practice for Red Hat RHCSA 8 (EX200) exam success with this Cert Guide from Pearson IT Certification, a leader in IT Certification learning. Master Red Hat RHCSA 8 EX200 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam-preparation tasks Practice with four unique practice tests Learn from two full hours of video training from the author's Red Hat Certified System Administrator (RHCSA) Complete Video Course, 3rd Edition. Red Hat RHCSA 8 Cert Guide is a best-of-breed exam study guide. Leading Linux consultant, author, and instructor Sander van Vugt shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time, including Basic system management: Installation, tools, file management, text files, RHEL8 connections, user/group management, permissions, and network configuration Operating running systems: Managing software, processes, storage, and advanced storage; working with systemd; scheduling tasks; and configuring logging Advanced system administration: Managing the kernel and boot procedures, essential troubleshooting, bash shell scripting Managing network services: Configuring SSH, firewalls, and time services; managing Apache HTTP services and SE Linux; and accessing network storage

Security and Privacy in Communication Networks-Bhavani Thuraisingham 2016-01-23 This volume constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Security and Privacy in Communication Networks, SecureComm 2015, held in Dallas, TX, USA, in October 2015. The 29 regular and 10 poster papers presented were carefully reviewed and selected from 107 submissions. It also presents 9 papers accepted of the workshop on Applications and Techniques in Cyber Security, ATCS 2015. The papers are grouped in the following topics: mobile, system, and software security; cloud security; privacy and side channels; Web and network security; crypto, protocol, and model.

Learning Docker-Pethuru Raj 2015-06-29 Docker is a next-generation platform for simplifying application containerization life-cycle. Docker allows you to create a robust and resilient environment in which you can generate portable, composable, scalable, and stable application containers. This book is a step-by-step guide that will walk you through the various features of Docker from Docker software installation to the impenetrable security of containers. The book starts off by elucidating the installation procedure for

Docker and a few troubleshooting techniques. You will be introduced to the process of downloading Docker images and running them as containers. You'll learn how to run containers as a service (CaaS) and also discover how to share data among containers. Later on, you'll explore how to establish the link between containers and orchestrate containers using Docker Compose. You will also come across relevant details about application testing inside a container. You will discover how to debug a container using the docker exec command and the nsenter tool. Finally, you will learn how to secure your containers with SELinux and other proven methods.

Embedded Linux Development Using Yocto Project Cookbook-Alex González 2018-01-25 Over 79 hands-on recipes for professional embedded Linux developers to optimize and boost their Yocto Project know-how
Key Features Optimize your Yocto setup to speed up development and debug build issues Use what is quickly becoming the standard embedded Linux product builder framework—the Yocto Project Recipe-based implementation of best practices to optimize your Linux system Book Description The Yocto Project has become the de facto distribution build framework for reliable and robust embedded systems with a reduced time to market. You'll get started by working on a build system where you set up Yocto, create a build directory, and learn how to debug it. Then, you'll explore everything about the BSP layer, from creating a custom layer to debugging device tree issues. In addition to this, you'll learn how to add a new software layer, packages, data, scripts, and configuration files to your system. You will then cover topics based on application development, such as using the Software Development Kit and how to use the Yocto project in various development environments. Toward the end, you will learn how to debug, trace, and profile a running system. This second edition has been updated to include new content based on the latest Yocto release. What you will learn Optimize your Yocto Project setup to speed up development and debug build issues Use Docker containers to build Yocto Project-based systems Take advantage of the user-friendly Toaster web interface to the Yocto Project build system Build and debug the Linux kernel and its device trees Customize your root filesystem with already-supported and new Yocto packages Optimize your production systems by reducing the size of both the Linux kernel and root filesystems Explore the mechanisms to increase the root filesystem security Understand the open source licensing requirements and how to comply with them when cohabiting with proprietary programs Create recipes, and build and run applications in C, C++, Python, Node.js, and Java Who this book is for If you are an embedded Linux developer with the basic knowledge of Yocto Project, this book is an ideal way to broaden your knowledge with recipes for embedded development.

Securing Your Cloud: IBM Security for LinuxONE-Lydia Parziale 2019-08-01 As workloads are being offloaded to IBM® LinuxONE based cloud environments, it is important to ensure that these workloads and environments are secure. This IBM Redbooks® publication describes the necessary steps to secure your environment from the hardware level through all of the components that are involved in a LinuxONE cloud infrastructure that use Linux and IBM z/VM®. The audience for this book is IT architects, IT Specialists, and those users who plan to use LinuxONE for their cloud environments.

Red Hat Linux Networking and System Administration-Terry Collings 2004-02-20 * Updated to cover Red Hat Linux Enterprise Workstation with the latest on advanced Linux kernel features, the Tux Web server, the latest Apache 2.x Web server, and the expanded suite of custom configuration tools * Starts with network planning and Red Hat installation and configuration, then progresses to optimizing network and Internet services and monitoring and maintaining the network * Examines the basics of Red Hat Linux security and offers trouble-shooting and problem-solving advice * Includes important new chapters that focus on optimizing standard network services, such as file and print services, and Internet-related servers, such as the Apache Web server Copyright © 2004 by Red Hat, Inc. Material from Chapters 4-6, 8-10, 17 and 21 may be distributed only subject to the terms and conditions set forth in the Open Publication License, V1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

Docker in Practice-Ian Miell 2019-01-28 Summary Docker in Practice, Second Edition presents over 100 practical techniques, hand-picked to help you get the most out of Docker. Following a Problem/Solution/Discussion format, you'll walk through specific examples that you can use immediately, and you'll get expert guidance on techniques that you can apply to a whole range of scenarios. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Docker's simple idea-wrapping an application and its dependencies into a single deployable container-created a buzz in the software industry. Now, containers are essential to enterprise infrastructure, and Docker is the undisputed industry standard. So what do you do after you've mastered the basics? To really streamline your applications and transform your dev process, you need relevant

examples and experts who can walk you through them. You need this book. About the Book Docker in Practice, Second Edition teaches you rock-solid, tested Docker techniques, such as replacing VMs, enabling microservices architecture, efficient network modeling, offline productivity, and establishing a container-driven continuous delivery process. Following a cookbook-style problem/solution format, you'll explore real-world use cases and learn how to apply the lessons to your own dev projects. What's inside

Continuous integration and delivery
The Kubernetes orchestration tool
Streamlining your cloud workflow
Docker in swarm mode
Emerging best practices and techniques
About the Reader
Written for developers and engineers using Docker in production. About the Author
Ian Miell and Aidan Hobson Sayers are seasoned infrastructure architects working in the UK. Together, they used Docker to transform DevOps at one of the UK's largest gaming companies.

Table of Contents
PART 1 - DOCKER FUNDAMENTALS
Discovering Docker
Understanding Docker: Inside the engine room
PART 2 - DOCKER AND DEVELOPMENT
Using Docker as a lightweight virtual machine
Building images
Running containers
Day-to-day Docker
Configuration management: Getting your house in order
PART 3 - DOCKER AND DEVOPS
Continuous integration: Speeding up your development pipeline
Continuous delivery: A perfect fit for Docker principles
Network simulation: Realistic environment testing without the pain
PART 4 - ORCHESTRATION FROM A SINGLE MACHINE TO THE CLOUD
A primer on container orchestration
The data center as an OS with Docker
Docker platforms
PART 5 - DOCKER IN PRODUCTION
Docker and security
Plain sailing: Running Docker in production
Docker in production: Dealing with challenges
Linux Security Cookbook-Daniel J. Barrett 2003-06-02
Computer security is an ongoing process, a relentless contest between system administrators and intruders. A good administrator needs to stay one step ahead of any adversaries, which often involves a continuing process of education. If you're grounded in the basics of security, however, you won't necessarily want a complete treatise on the subject each time you pick up a book. Sometimes you want to get straight to the point. That's exactly what the new Linux Security Cookbook does. Rather than provide a total security solution for Linux computers, the authors present a series of easy-to-follow recipes--short, focused pieces of code that administrators can use to improve security and perform common tasks securely. The Linux Security Cookbook includes real solutions to a wide range of targeted problems, such as sending encrypted email within Emacs, restricting access to network services at particular times of day, firewalling a webserver, preventing IP spoofing, setting up key-based SSH authentication, and much more. With over 150 ready-to-use scripts and configuration files, this unique book helps administrators secure their systems without having to look up specific syntax. The book begins with recipes devised to establish a secure system, then moves on to secure day-to-day practices, and concludes with techniques to help your system stay secure. Some of the "recipes" you'll find in this book are: Controlling access to your system from firewalls down to individual services, using iptables, ipchains, xinetd, inetd, and more
Monitoring your network with tcpdump, dsniff, netstat, and other tools
Protecting network connections with Secure Shell (SSH) and stunnel
Safeguarding email sessions with Secure Sockets Layer (SSL)
Encrypting files and email messages with GnuPG
Probing your own security with password crackers, nmap, and handy scripts
This cookbook's proven techniques are derived from hard-won experience. Whether you're responsible for security on a home Linux system or for a large corporation, or somewhere in between, you'll find valuable, to-the-point, practical recipes for dealing with everyday security issues. This book is a system saver.

Using Docker-Adrian Mouat 2015-12-09
Docker containers offer simpler, faster, and more robust methods for developing, distributing, and running software than previously available. With this hands-on guide, you'll learn why containers are so important, what you'll gain by adopting Docker, and how to make it part of your development process. Ideal for developers, operations engineers, and system administrators—especially those keen to embrace a DevOps approach—Using Docker will take you from Docker and container basics to running dozens of containers on a multi-host system with networking and scheduling. The core of the book walks you through the steps needed to develop, test, and deploy a web application with Docker. Get started with Docker by building and deploying a simple web application
Use Continuous Deployment techniques to push your application to production multiple times a day
Learn various options and techniques for logging and monitoring multiple containers
Examine networking and service discovery: how do containers find each other and how do you connect them?
Orchestrate and cluster containers to address load-balancing, scaling, failover, and scheduling
Secure your system by following the principles of defense-in-depth and least privilege

A Practical Guide to SysML-Sanford Friedenthal 2009-08-25
A Practical Guide to SysML: The Systems Modeling Language is a comprehensive guide to SysML for systems and software engineers. It provides an advanced and practical resource for modeling systems with SysML. The source describes the modeling

language and offers information about employing SysML in transitioning an organization or project to model-based systems engineering. The book also presents various examples to help readers understand the OMG Systems Modeling Professional (OCSMP) Certification Program. The text is organized into four parts. The first part provides an overview of systems engineering. It explains the model-based approach by comparing it with the document-based approach and providing the modeling principles. The overview of SysML is also discussed. The second part of the book covers a comprehensive description of the language. It discusses the main concepts of model organization, parametrics, blocks, use cases, interactions, requirements, allocations, and profiles. The third part presents examples that illustrate how SysML supports different model-based procedures. The last part discusses how to transition and deploy SysML into an organization or project. It explains the integration of SysML into a systems development environment. Furthermore, it describes the category of data that are exchanged between a SysML tool and other types of tools, and the types of exchange mechanisms that can be used. It also covers the criteria that must be considered when selecting a SysML. Software and systems engineers, programmers, IT practitioners, experts, and non-experts will find this book useful. *The authoritative guide for understanding and applying SysML *Authored by the foremost experts on the language *Language description, examples, and quick reference guide included

Learning Puppet Security-Jason Slagle 2015-03-27 If you are a security professional whose workload is increasing, or a Puppet professional looking to increase your knowledge of security, or even an experienced systems administrator, then this book is for you. This book will take you to the next level of security automation using Puppet. The book requires no prior knowledge of Puppet to get started.

Container Security-Liz Rice 2020-04-06 To facilitate scalability and resilience, many organizations now run applications in cloud native environments using containers and orchestration. But how do you know if the deployment is secure? This practical book examines key underlying technologies to help developers, operators, and security professionals assess security risks and determine appropriate solutions. Author Liz Rice, VP of open source engineering at Aqua Security, looks at how the building blocks commonly used in container-based systems are constructed in Linux. You'll understand what's happening when you deploy containers and learn how to assess potential security risks that could affect your deployments. If you run container applications with kubectl or docker and use Linux command-line tools such as ps and grep, you're ready to get started. Explore attack vectors that affect container deployments Dive into the Linux constructs that underpin containers Examine measures for hardening containers Understand how misconfigurations can compromise container isolation Learn best practices for building container images Identify container images that have known software vulnerabilities Leverage secure connections between containers Use security tooling to prevent attacks on your deployment

Right here, we have countless ebook **selinux by example using security enhanced linux david caplan** and collections to check out. We additionally pay for variant types and plus type of the books to browse. The within acceptable limits book, fiction, history, novel, scientific research, as without difficulty as various extra sorts of books are readily open here.

As this selinux by example using security enhanced linux david caplan, it ends taking place living thing one of the favored book selinux by example using security enhanced linux david caplan collections that we have. This is why you remain in the best website to see the unbelievable books to have.

[ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION](#)