Selinux By Example Using Security Enhanced Linux David Caplan

BREWER KERR

SELinux Cookbook Jones & Bartlett Publishers
Can a system be considered truly reliable if it isn't fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O'Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that's supportive of such change. You'll learn about secure and reliable systems through: Design strategies Recommendations for coding, testing, and debugging practices Strategies to prepare for, respond to, and recover from incidents Cultural best practices that help teams across your organization collaborate effectively
SELinux by Example Pearson Education
A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerabilitya bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold. Covers a range of operating system families — UNIX derivatives, Mac OS X, Windows Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions Delivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks
Fedora 12 Security-Enhanced Linux User Guide Fultus Corporation
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.
ICICT 2021, London, Volume 4 Simon and Schuster
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.
Implement mandatory access control to secure applications, users, and information flows on Linux
O'Reilly Media
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)
Fedora 11 Security-Enhanced Linux User Guide Oreilly & Associates Incorporated
"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"--
Docker in Practice Springer Nature
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.
Hardening Linux Springer Nature
More than 50 percent new and revised content for today's Linux environment gets you up and running in no time! Linux continues to be an excellent, low-cost alternative to expensive operating systems. Whether you're new to Linux or need a reliable update and reference, this is an excellent resource. Veteran bestselling author Christopher Negus provides a complete tutorial packed with major updates, revisions, and hands-on exercises so that you can confidently start using Linux today. Offers a complete restructure, complete with exercises, to make the book a better learning tool Places a strong focus on the Linux command line tools and can be used with all distributions and versions of Linux Features in-depth coverage of the tools that a power user and a Linux administrator need to get started This practical learning tool is ideal for anyone eager to set up a new Linux desktop system at home or curious to learn how to manage Linux server systems at work.
Tools and Jewels Pearson Education
Enhance Linux security, application platforms, and virtualization solutions with SELinux to work within your boundaries, your rules, and your policiesKey Features* Learn what SELinux is, and how it acts as a mandatory access control system on Linux* Apply and tune SELinux enforcement to users, applications, platforms, and virtualization solutions* Use real-life examples and custom policies to strengthen the security posture of your systemsBook DescriptionLinux is a dominant player in many organizations and in the cloud. Securing the Linux environment is extremely important for any organization, and Security-Enhanced Linux (SELinux) acts as an additional layer to Linux system security.SELinux System Administration covers basic SELinux concepts and shows you how to enhance Linux system protection measures. You will get to grips with SELinux and understand how it is integrated. As you progress, you'll get hands-on experience of tuning and configuring SELinux and integrating it into day-to-day administration tasks such as user management, network management, and application maintenance. Platforms such as Kubernetes, system services like systemd, and virtualization solutions like libvirt and Xen, all of which offer SELinux-specific controls, will be explained effectively so that you understand how to apply and configure SELinux within these applications. If applications do not exert the expected behavior, you'll learn how to fine-tune policies to securely host these applications. In case no policies exist, the book will guide you through developing custom policies on your own.By the end of this Linux book, you'll be able to harden any

Linux system using SELinux to suit your needs and fine-tune existing policies and develop custom ones to protect any app and service running on your Linux systems.What you will learn* Understand what SELinux is and how it is integrated into Linux* Tune Linux security using policies and their configurable settings* Manage Linux users with least-privilege roles and access controls* Use SELinux controls in system services and virtualization solutions* Analyze SELinux behavior through log events and policy analysis tools* Protect systems against unexpected and malicious behavior* Enhance existing policies or develop custom onesWho this book is forThis Linux sysadmin book is for Linux administrators who want to control the secure state of their systems using SELinux, and for security professionals who have experience in maintaining a Linux system and want to know about SELinux. Experience in maintaining Linux systems, covering user management, software installation and maintenance, Linux security controls, and network configuration is required to get the most out of this book.

SELinux System Administration - Second Edition Simon and Schuster

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

CentOS 7 Server Deployment Cookbook Springer

The Fedora Security-Enhanced Linux User Guide provides an introduction to fundamental concepts and practical applications of SELinux (Security-Enhanced Linux).

On the Move to Meaningful Internet Systems: OTM 2009 Apress

Provides information on using the latest Ubuntu release, covering such topics as installation, customizing the GNOME panel, installing applications, using printers and scanners, connecting to the Internet, using multimedia, and security.

Ubuntu for Non-Geeks, 4th Edition Payload Media

Deploy and manage today's essential services on an enterprise-class, open operating system About This Book Configure and manage Linux servers in varying scenarios and for a range of business requirements Explore the up-to-date features of CentOS using real-world scenarios See practical and extensive recipes to deploy and manage CentOS Who This Book Is For This book is for Linux professionals with basic Unix/Linux functionality experience, perhaps even having set up a server before, who want to advance their knowledge in administering various services. What You Will Learn See how to deploy CentOS easily and painlessly, even in multi-server environments Configure various methods of remote access to the server so you don't always have to be in the data center Make changes to the default configuration of many services to harden them and increase the security of the system Learn to manage DNS, emails and web servers Protect yourself from threats by monitoring and logging network intrusion and system intrusion attempts, rootkits, and viruses Take advantage of today's powerful hardware by running multiple systems using virtualization In Detail CentOS is derived from Red Hat Enterprise Linux (RHEL) sources and is widely used as a Linux server. This book will help you to better configure and manage Linux servers in varying scenarios and business requirements. Starting with installing CentOS, this book will walk you through the networking aspects of CentOS. You will then learn how to manage users and their permissions, software installs, disks, filesystems, and so on. You'll then see how to secure connection to remotely access a desktop and work with databases. Toward the end, you will find out how to manage DNS, e-mails, web servers, and more. You will also learn to detect threats by monitoring network intrusion. Finally, the book will cover virtualization techniques that will help you make the most of CentOS. Style and approach This easy-to-read cookbook is filled with practical recipes. Hands-on, task-based exercises will present you with real-world solutions to deploy and manage CentOS in varying business scenarios.

NSA's Open Source Security Enhanced Linux O'Reilly Media

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.

A Pain-Free, Get-Things-Done Guide Fultus Corporation

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.

Computer Security and the Internet Packt Publishing Ltd

This book constitutes the thoroughly refereed, selected papers on the Second Cyber Security and Privacy EU Forum, CSP 2014, held in Athens, Greece, in May 2014. The 14 revised full papers presented were carefully reviewed and selected from 90 submissions. The papers are organized in topical sections on security; accountability, data protection and privacy; research and innovation.

Fundamental Technology Concepts that Protect Containerized Applications No Starch Press

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).

Exploring SE for Android Apress

Arguably one of the most highly regarded and widely used enterprise level operating systems available today is the Red Hat Enterprise Linux 8 distribution. Not only is it considered to be among the most stable and reliable operating systems, it is also backed by the considerable resources and technical skills of Red Hat, Inc. Red Hat Enterprise Linux 8 Essentials is designed to provide detailed information on the installation, use and administration of the Red Hat Enterprise Linux 8 distribution. For beginners, the book covers topics such as operating system installation, the basics of the GNOME desktop environment, configuring email and web servers and installing packages and system updates using App Streams. Additional installation topics such as dual booting with Microsoft Windows are also covered, together with all important security topics such as configuring a firewall and user and group administration. For the experienced user, topics such as remote desktop access, the Cockpit web interface, logical volume management (LVM), disk partitioning, swap management, KVM virtualization, Secure Shell (SSH), Linux Containers and file sharing using both Samba and NFS are covered in detail to provide a thorough overview of this enterprise class operating system.

Demystifying Internet of Things Security Packt Publishing Ltd

Enhance Linux security, application platforms, and virtualization solutions with SELinux to work within your boundaries, your rules, and your policies Key Features Learn what SELinux is, and how it acts as a mandatory access control system on Linux Apply and tune SELinux enforcement to users, applications, platforms, and virtualization solutions Use real-life examples and custom policies to strengthen the security posture of your systems Book Description Linux is a dominant player in many organizations and in the cloud. Securing the Linux environment is extremely important for any organization, and Security-Enhanced Linux (SELinux) acts as an additional layer to Linux system security. SELinux System Administration covers basic SELinux concepts and shows you how to enhance Linux system protection measures. You will get to grips with SELinux and understand how it is integrated. As you progress, you'll get hands-on experience of tuning and configuring SELinux and integrating it into day-to-day administration tasks such as user management, network management, and application maintenance. Platforms such as Kubernetes, system services like systemd, and virtualization solutions like libvirt and Xen, all of which offer SELinux-specific controls, will be explained effectively so that you understand how to apply and configure SELinux within these applications. If applications do not exert the expected behavior, you'll learn how to fine-tune policies to securely host these applications. In case no policies exist, the book will guide you through developing custom policies on your own. By the end of this Linux book, you'll be able to harden any Linux system using SELinux to suit your needs and fine-tune existing policies and develop custom ones to protect any app and service running on your Linux systems. What you will learn Understand what SELinux is and how it is integrated into Linux Tune Linux security using policies and their configurable settings Manage Linux users with least-privilege roles and access controls Use SELinux controls in system services and virtualization solutions Analyze SELinux behavior through log events and policy analysis tools Protect systems against unexpected and malicious behavior Enhance existing policies or develop custom ones Who this book is for This Linux sysadmin book is for Linux administrators who want to control the secure state of their systems using SELinux, and for security professionals who have experience in maintaining a Linux system and want to know about SELinux. Experience in maintaining Linux systems, covering user management, software installation and maintenance, Linux security controls, and network configuration is required to get the most out of this book.

Linux Bible No Starch Press

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