Linux Security And Hardening The Practical Security

Implement Mandatory Access Control to Secure Applications, Users, and Information Flows on Linux
Mastering Linux System Administration
Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition
Security Tools & Techniques
Hardening Network Security
Mastering Linux Security and Hardening
Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure
Linux Service Management Made Easy with systemd
Mastering Linux Security and Hardening
Mastering Defensive Security
Linux Server Security
Linux Server Best Practices
Mastering Linux Security and Hardening

Linux Security Fundamentals
Security Power Tools
Linux Security and Hardening Essential Training
Linux Security and Hardening Essential Training
Hardening Windows Systems
The Linux Operating System and Command Line Guide for Linux Administrators
Linux Security Cookbook
Mastering Windows Security and Hardening
Hardening Linux
Linux Essentials for Cybersecurity
Practical Linux Security Cookbook
The Practical Security Guide
Digital Forensics Field Guides
Advanced techniques to effectively manage, control, and monitor Linux systems and services
Hardening Linux
Using Security Enhanced Linux
Server Security from TLS to Tor
Secure your Linux server and protect it from intruders, malware attacks, and other external threats

Learn Linux in 5 Days
Malware Forensics Field Guide for Windows Systems
AIX V6 Advanced Security Features Introduction and Configuration
Mastering Linux Security and Hardening
SELinux by Example
Insightful recipes to work with system administration tasks on Linux
Building Secure Servers with Linux
Linux Server Security
DevOps Troubleshooting

DEMARCUS JACOBY

Implement Mandatory Access Control to Secure Applications, Users, and Information Flows on Linux McGraw Hill Professional

"If you're a developer trying to figure out why your application is not responding at 3 am, you need this book! This is now my go-to book when diagnosing production issues. It has saved me hours in troubleshooting complicated operations problems." –Trotter Cashion, cofounder, Mashion DevOps can help developers, QAs, and admins work together to solve Linux server problems far more rapidly, significantly improving IT performance,

availability, and efficiency. To gain these benefits, however, team members need common troubleshooting skills and practices. In DevOps Troubleshooting: Linux Server Best Practices , award-winning Linux expert Kyle Rankin brings together all the standardized, repeatable techniques your team needs to stop finger-pointing, collaborate effectively, and quickly solve virtually any Linux server problem. Rankin walks you through using DevOps techniques to troubleshoot everything from boot failures and corrupt disks to lost email and downed websites. You'll master indispensable skills for diagnosing high-load systems and network problems in production environments. Rankin shows how to Master DevOps' approach to troubleshooting and proven Linux server problem-solving principles Diagnose slow servers and applications by identifying CPU, RAM, and Disk I/O bottlenecks Understand healthy boots, so you can identify failure points and fix them Solve full or corrupt disk issues that prevent disk writes Track down the sources of network problems Troubleshoot DNS, email, and other network services Isolate and diagnose Apache and Nginx Web server failures and slowdowns Solve problems with MySQL and Postgres database servers and queries Identify hardware failures–even notoriously elusive intermittent failures *Mastering Linux System Administration* Packt

Publishing Ltd
An immersive learning experience enhanced with technical, hands-on labs to understand the concepts, methods, tools, platforms, and systems required to master the art of cybersecurity Key Features Get hold of the best defensive security strategies and tools Develop a defensive security strategy at an enterprise level Get hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and more Book Description Every organization has its own data and digital assets that need to be protected against an ever-growing threat landscape that compromises the availability, integrity, and confidentiality of crucial data. Therefore, it is important to train professionals in the latest defensive security skills and tools to secure them. Mastering Defensive Security provides you with in-depth knowledge of the latest cybersecurity threats along with the best tools and techniques needed to keep your infrastructure secure. The book begins by establishing a strong foundation of cybersecurity concepts and advances to explore the latest security technologies such as Wireshark, Damn Vulnerable Web App (DVWA), Burp Suite, OpenVAS, and Nmap, hardware threats such as a weaponized Raspberry Pi, and hardening techniques for Unix, Windows, web applications, and cloud

infrastructures. As you make progress through the chapters, you'll get to grips with several advanced techniques such as malware analysis, security automation, computer forensics, and vulnerability assessment, which will help you to leverage pentesting for security. By the end of this book, you'll have become familiar with creating your own defensive security tools using IoT devices and developed advanced defensive security skills. What you will learn Become well versed with concepts related to defensive security Discover strategies and tools to secure the most vulnerable factor – the user Get hands-on experience using and configuring the best security tools Understand how to apply hardening techniques in Windows and Unix environments Leverage malware analysis and forensics to enhance your security strategy Secure Internet of Things (IoT) implementations Enhance the security of web applications and cloud deployments Who this book is for This book is for IT professionals, including systems administrators, programmers, IT architects, solution engineers, system analysts, data scientists, DBAs, and any IT expert looking to explore the fascinating world of cybersecurity. Cybersecurity professionals who want to broaden their knowledge of security topics to effectively create and design a defensive security strategy for a

large organization will find this book useful. A basic understanding of concepts such as networking, IT, servers, virtualization, and cloud is required.

Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition "O'Reilly Media, Inc."

"This course will not only teach you the security concepts and guidelines that will keep your Linux servers safe, it will walk you through hardening measures step-by-step. By the end of this course, you will be able to tighten up the security on any Linux system. You'll learn the security weaknesses of the Linux operating system and will be given step-by-step instructions on how to protect those weaknesses. You'll even learn some security concepts that apply to information security as a whole while focusing on Linux-specific issues that require special consideration. What you learn in this course applies to any Linux environment or distribution including Ubuntu, Debian, Linux Mint, RedHat, CentOS, Fedora, OpenSUSE, Slackware, Kali Linux, and more."--Resource description page.

Security Tools & Techniques Pearson Education

Learn Linux Administration and Supercharge Your Career!If you're looking to make the jump from being a Linux user to being a Linux administrator, this book is for you! If you're in windows administration and want to learn the ins

and outs of Linux administration, start here. This book is also great for Unix administrators switching to Linux administration.Here is what you will learn by reading this Linux System Administration book: How the the boot process works on Linux servers and what you can do to control it. The various types of messages generated by a Linux system, where they're stored, and how to automatically prevent them from filling up your disks. Disk management, partitioning, and file system creation. Managing Linux users and groups. Exactly how permissions work and how to decipher the most cryptic Linux permissions with ease. Networking concepts that apply to system administration and specifically how to configure Linux network interfaces. How to use the nano, vi, and emacs editors. How to schedule and automate jobs using cron. How to switch users and run processes as others. How to configure sudo. How to find and install software. Managing process and jobs. How to make the most out of the Linux command line Several Linux commands you'll need to know Linux shell scripting What you learn in book applies to any Linux system including Ubuntu Linux, Debian, Linux Mint, RedHat Linux, CentOS, Fedora, SUSE Linux, Arch Linux, Kali Linux and more.Real Advice from a Real, Professional Linux AdministratorJason Cannon is the author of Linux for Beginners, the founder of the Linux

Training Academy, and an instructor to over 40,000 satisfied students. He started his IT career in the late 1990's as a Unix and Linux System Engineer and he'll be sharing his real-world Linux experience with you throughout this book.By the end of this book you will fully understand the most important and fundamental concepts of Linux server administration. More importantly, you will be able to put those concepts to use in practical real-world situations. You'll be able to configure, maintain, and support a variety of Linux systems. You can even use the skills you learned to become a Linux System Engineer or Linux System Administrator.

Hardening Network Security John Wiley & Sons

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.

Mastering Linux Security and Hardening

IBM Redbooks

Automate security-related tasks in a structured, modular fashion using the best open source automation tool available About This Book Leverage the agentless, push-based power of Ansible 2 to automate security tasks Learn to write playbooks that apply security to any part of your system This recipe-based guide will teach you to use Ansible 2 for various use cases such as fraud detection, network security, governance, and more Who This Book Is For If you are a system administrator or a DevOps engineer with responsibility for finding loop holes in your system or application, then this book is for you. It's also useful for security

consultants looking to automate their infrastructure's security model. What You Will Learn Use Ansible playbooks, roles, modules, and templating to build generic, testable playbooks Manage Linux and Windows hosts remotely in a repeatable and predictable manner See how to perform security patch management, and security hardening with scheduling and automation Set up AWS Lambda for a serverless automated defense Run continuous security scans against your hosts and automatically fix and harden the gaps Extend Ansible to write your custom modules and use them as part of your already existing security automation programs Perform automation security audit checks for applications using Ansible Manage secrets in Ansible using Ansible Vault In Detail Security automation is one of the most interesting skills to have nowadays. Ansible allows you to write automation procedures once and use them across your entire infrastructure. This book will teach you the best way to use Ansible for seemingly complex tasks by using the various building blocks available and creating solutions that are easy to teach others, store for later, perform version control on, and repeat. We'll start by covering various popular modules and writing simple playbooks to showcase those modules. You'll see how this can be applied over a variety of platforms and operating

systems, whether they are Windows/Linux bare metal servers or containers on a cloud platform. Once the bare bones automation is in place, you'll learn how to leverage tools such as Ansible Tower or even Jenkins to create scheduled repeatable processes around security patching, security hardening, compliance reports, monitoring of systems, and so on. Moving on, you'll delve into useful security automation techniques and approaches, and learn how to extend Ansible for enhanced security. While on the way, we will tackle topics like how to manage secrets, how to manage all the playbooks that we will create and how to enable collaboration using Ansible Galaxy. In the final stretch, we'll tackle how to extend the modules of Ansible for our use, and do all the previous tasks in a programmatic manner to get even more powerful automation frameworks and rigs. Style and approach This comprehensive guide will teach you to manage Linux and Windows hosts remotely in a repeatable and predictable manner. The book takes an in-depth approach and helps you understand how to set up complicated stacks of software with codified and easy-to-share best practices.

Effective techniques to secure your Windows, Linux, IoT, and cloud infrastructure "O'Reilly Media, Inc."

Mastering Linux Security and HardeningProtect your Linux systems from

intruders, malware attacks, and other cyber threats, 2nd EditionPackt Publishing Ltd

Linux Service Management Made Easy with systemd

Packt Publishing Ltd

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.

Mastering Linux Security and Hardening Packt Publishing Ltd

Linux consistently turns up high in the list of popular Internet servers, whether it's for the Web, anonymous FTP, or general services like DNS and routing mail. But security is uppermost on the mind of anyone providing such a service. Any server experiences casual probe attempts dozens of time a day, and serious break-in attempts with some frequency as well. As the cost of broadband and other high-speed Internet connectivity has gone down, and its availability has increased, more Linux users are providing or

considering providing Internet services such as HTTP, Anonymous FTP, etc., to the world at large. At the same time, some important, powerful, and popular Open Source tools have emerged and rapidly matured--some of which rival expensive commercial equivalents--making Linux a particularly appropriate platform for providing secure Internet services. Building Secure Servers with Linux will help you master the principles of reliable system and network security by combining practical advice with a firm knowledge of the technical tools needed to ensure security. The book focuses on the most common use of Linux--as a hub offering services to an organization or the larger Internet--and shows readers how to harden their hosts against attacks. Author Mick Bauer, a security consultant, network architect, and lead author of the popular Paranoid Penguin column in Linux Journal, carefully outlines the security risks, defines precautions that can minimize those risks, and offers recipes for robust security. The book does not cover firewalls, but covers the more common situation where an organization protects its hub using other systems as firewalls, often proprietary firewalls. The book includes: Precise directions for securing common services, including the Web, mail, DNS, and file transfer. Ancillary tasks, such as hardening Linux, using SSH and certificates for tunneling, and using

iptables for firewalling. Basic installation of intrusion detection tools. Writing for Linux users with little security expertise, the author explains security concepts and techniques in clear language, beginning with the fundamentals. Building Secure Servers with Linux provides a unique balance of "big picture" principles that transcend specific software packages and version numbers, and very clear procedures on securing some of those software packages. An all-inclusive resource for Linux users who wish to harden their systems, the book covers general security as well as key services such as DNS, the Apache Web server, mail, file transfer, and secure shell. With this book in hand, you'll have everything you need to ensure robust security of your Linux system. Mastering Defensive Security Pearson IT Certification Implement information security effectively as per your organization's needs. About This Book Learn to build your own information security framework, the best fit for your organization Build on the concepts of threat modeling, incidence response, and security analysis Practical use cases and best practices for information security Who This Book Is For This book is for security analysts and professionals who deal with security mechanisms in an organization. If you are looking for an end to end guide on information security and risk analysis with no prior knowledge

of this domain, then this book is for you. What You Will Learn Develop your own information security framework Build your incident response mechanism Discover cloud security considerations Get to know the system development life cycle Get your security operation center up and running Know the various security testing types Balance security as per your business needs Implement information security best practices In Detail Having an information security mechanism is one of the most crucial factors for any organization. Important assets of organization demand a proper risk management and threat model for security, and so information security concepts are gaining a lot of traction. This book starts with the concept of information security and shows you why it's important. It then moves on to modules such as threat modeling, risk management, and mitigation. It also covers the concepts of incident response systems, information rights management, and more. Moving on, it guides you to build your own information security framework as the best fit for your organization. Toward the end, you'll discover some best practices that can be implemented to make your security framework strong. By the end of this book, you will be well-versed with all the factors involved in information security, which will help you build a security

framework that is a perfect fit your organization's requirements. Style and approach This book takes a practical approach, walking you through information security fundamentals, along with information security best practices.

Linux Server Security

Mastering Linux Security and HardeningProtect your Linux systems from intruders, malware attacks, and other cyber threats, 2nd Edition
A comprehensive guide for teaching system administrators, developers, and security professionals how to create their own systemd units and maintain system security Key Features Get well-versed with maintaining and troubleshooting systemd services Learn to create, modify, and reload service files and use systemd utilities Use cgroups to control resource usage and enhance security Book Description systemd is a new type of Linux init system for today's high-performance, multi-CPU, and multi-core hardware that is now used on all major enterprise-grade Linux distros. The main goal of this Linux systemd book is to help you get an in-depth understanding of systemd to set up your servers securely and efficiently. This book starts by explaining systemd management, which will help you manage your servers effectively. You'll then learn how to edit and create your own systemd units, which will be particularly helpful if you need to create custom services or timers and add

features or security to an existing service. Next, you'll understand how to analyze and fix boot-up challenges and set system parameters. Later, you'll come across cgroups, that'll help you control system resource usage for both processes and users. The book also shows you how cgroups are structured, the differences between cgroups Version 1 and 2, and how to set resource limits on both. Finally, you'll learn about the systemd way of performing time-keeping, networking, logging, and login management. You'll discover how to configure servers accurately and gather system information to analyze system security and performance. By the end of this Linux book, you'll be able to efficiently manage all aspects of a server running the systemd init system. What you will learn Use basic systemd utilities to manage a system Create and edit your own systemd units Create services for Podman-Docker containers Enhance system security by adding security-related parameters Find important information with journald Analyze boot-up problems Configure system settings with systemd utilities Who this book is for This book is for Linux administrators who want to learn more about maintaining and troubleshooting Linux servers. Aspiring administrators studying for a Linux certification exam and developers looking to learn how to create systemd unit files will also find this book useful. Additionally, this

book will be helpful for security administrators who want to understand the security settings that can be used in systemd units and how to control resource usage with cgroups. Working knowledge of basic Linux commands is assumed.

Linux Server Best Practices Packt Publishing Ltd

Offers real world examples of computer security breeches and discusses common attacks, security policies, configuration and hardware preparation, and system scanning and repair.

Mastering Linux Security and Hardening Addison-Wesley Professional

Hardening a Linux system can make it much more difficult for an attacker to exploit it. This book will enable system administrators and network engineers to protect their Linux systems, and the sensitive data on those systems.

Linux Security Fundamentals IBM Redbooks

Provides steps to ensure the security of Windows systems, covering such topics as passwords, authentication, network infastructure, Windows directory information, application access, PKI, LAN communications, and security policies.

Security Power Tools Packt Publishing Ltd

The differences between well-designed security and poorly designed security are not always readily apparent. Poorly designed systems give the appearance of being secure but can over-

authorize users or allow access to non-users in subtle ways. The problem is that poorly designed security gives a false sense of confidence. In some ways, it is better to knowingly have no security than to have inadequate security believing it to be stronger than it actually is. But how do you tell the difference? Although it is not rocket science, designing and implementing strong security requires strong foundational skills, some examples to build on, and the capacity to devise new solutions in response to novel challenges. This IBM® Redbooks® publication addresses itself to the first two of these requirements. This book is intended primarily for security specialists and IBM WebSphere® MQ administrators that are responsible for securing WebSphere MQ networks but other stakeholders should find the information useful as well. Chapters 1 through 6 provide a foundational background for WebSphere MQ security. These chapters take a holistic approach positioning WebSphere MQ in the context of a larger system of security controls including those of adjacent platforms' technologies as well as human processes. This approach seeks to eliminate the simplistic model of security as an island, replacing it instead with the model of security as an interconnected and living system. The intended audience for these chapters includes all stakeholders in the messaging system from

architects and designers to developers and operations. Chapters 7 and 8 provide technical background to assist in preparing and configuring the scenarios and chapters 9 through 14 are the scenarios themselves. These chapters provide fully realized example configurations. One of the requirements for any scenario to be included was that it must first be successfully implemented in the team's lab environment. In addition, the advice provided is the cumulative result of years of participation in the online community by the authors and reflect real-world practices adapted for the latest security features in WebSphere MQ V7.1 and WebSphere MQ V7.5. Although these chapters are written with WebSphere MQ administrators in mind, developers, project leaders, operations staff, and architects are all stakeholders who will find the configurations and topologies described here useful. The third requirement mentioned in the opening paragraph was the capacity to devise new solutions in response to novel challenges. The only constant in the security field is that the technology is always changing. Although this book provides some configurations in a checklist format, these should be considered a snapshot at a point in time. It will be up to you as the security designer and implementor to stay current with security news for the products you work with and integrate fixes, patches, or new solutions as the state of the art

evolves.

Linux Security and Hardening Essential Training Createspace Independent Publishing Platform

Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treaterous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, Malware Forensics Field Guide for Windows Systems is a "tool" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code

Linux Security and Hardening Essential Training CreateSpace

This introduction to networking on Linux now covers firewalls, including the use of ipchains and Netfilter, masquerading, and accounting. Other new topics in this second edition include Novell (NCP/IPX) support and INN (news administration).

Hardening Windows Systems "O'Reilly Media, Inc."

"This course 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 course will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this course, you will be confident in delivering a system that will be much harder to compromise."--Resource description page.

The Linux Operating System and Command Line Guide for Linux Administrators McGraw Hill Professional

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. The Exam Ref is the official study guide for Microsoft certification exams. Featuring concise coverage of the skills measured by the exam, challenging Thought Experiments, and pointers to more in-depth material for the candidate needing additional study, exam candidates get professional-level preparation for the exam. The Exam Ref helps candidates determine their readiness for the exam, and provides Exam Tips to help maximize their performance on the exam. The organization of the material mirrors the skills measured by the

exam as presented on the certification exam webpage.

Linux Security Cookbook
Elsevier
An informative handbook for network administrators and professionals who use Linux offers practical guidelines on how to test, hack, and find security holes and secure them, explaining how to assess one's system, shut down unnecessary services and access, install filters and firewalls, eliminate unnecessary software, enhance authentication and user identity protocols, monitor network systems, and other important topics. Original. (Intermediate)

Related with Linux Security And Hardening The Practical Security:
• Indiana Drivers Manual Signs : click here