Linux Firewalls Enhancing Security With Nftables And Beyond 4th Edition

Getting the books **Linux Firewalls Enhancing Security With Nftables And Beyond 4th Edition** now is not type of inspiring means. You could not unaided going as soon as book addition or library or borrowing from your contacts to right of entry them. This is an categorically easy means to specifically get lead by on-line. This online declaration Linux Firewalls Enhancing Security With Nftables And Beyond 4th Edition can be one of the options to accompany you later than having extra time.

It will not waste your time. say yes me, the e-book will totally impression you additional business to read. Just invest little grow old to admittance this on-line pronouncement **Linux Firewalls Enhancing Security With Nftables And Beyond 4th Edition** as capably as evaluation them wherever you are now.

Pro Bash Programming - Chris Johnson 2010-04-29
The bash shell is a complete programming language, not merely a glue to combine external Linux commands. By taking full advantage of shell internals, shell programs can perform as snappily as utilities written in C or other compiled languages. And you will see how, without assuming Unix lore, you can write professional bash 4.0 programs through standard programming techniques. Complete bash coverage Teaches bash as a programming language Helps you master bash 4.0 features

Linux Networking Cookbook - Gregory Boyce 2016-06-28
Over 40 recipes to help you set up and configure Linux networks About This Book Move beyond the basics of how a Linux machine works and gain a better understanding of Linux networks and their configuration Impress your peers by setting up and configuring a Linux server and its various network elements like a pro This is a hands-on solution guide to building, maintaining, and securing a network using Linux Who This Book Is For This book is targeted at Linux systems administrators who have a good basic understanding and some prior experience of how a Linux machine operates, but want to better understand how various network services function, how to set them up, and how to secure them. You should be familiar with how to set up a Linux server and how to install additional software on them. What You Will Learn Route an IPv6 netblock to your local network Modify your named instance to support setting hostnames for your IPv6 addresses Use SSH for remote console access Configure NGINX with TLS Secure XMPP with TLS Leverage iptables6 to firewall your IPv6 traffic Configure Samba as an Active Directory compatible directory service In Detail Linux can be configured as a networked workstation, a DNS server, a mail server, a firewall, a gateway router, and many other things. These are all part of administration tasks, hence network administration is one of the main tasks of Linux system administration. By knowing how to configure system network interfaces in a reliable and optimal manner, Linux administrators can deploy and configure several network services including file, web, mail, and servers while working in large enterprise environments. Starting with a simple Linux router that passes traffic between two private networks, you will see how to enable NAT on the router in order to allow Internet access from the network, and will also enable DHCP on the network to ease configuration of client systems. You will then move on to configuring your own DNS server on your local network using bind9 and tying it into your DHCP server to allow automatic configuration of local hostnames. You will then future enable your network by setting up IPv6 via tunnel providers. Moving on, we'll configure Samba to centralize authentication for your network services; we will also configure Linux client to leverage it for authentication, and set up a RADIUS server that uses the directory server for authentication. Toward the end, you will have a network with a number of services running on it, and will implement monitoring in order to detect problems as they occur. Style and approach This book is packed with practical recipes and a task-based approach that will walk you through building, maintaining, and securing a computer network using Linux.

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.

Linux Hardening in Hostile Networks - Kyle Rankin 2017-03-30
In an age of massive global surveillance, when last year's most advanced cyberwarfare weapons quickly migrate into every hacker's toolkit, you can no longer afford to rely on outdated security methods. If you care about privacy and security today, you need to step up your game -- especially if you're a sysadmin responsible for Internet-facing services. That means you need to master and use advanced security technologies like the TLS communications security protocol, PGP encryption, and the Tor anonymity network. Tools like these have often been viewed as too complex or mysterious for mainstream use. In Security Under Surveillance, Kyle Rankin completely demystifies them, and offers practical, accessible guidance on protecting yourself and your users with them. Rankin begins with a user-oriented guide to safeguarding your own personal data with PGP, Off-the-Record Messaging (OTR), Tor, and the Tails "amnesic incognito" live Linux distribution. Next, he guides you through setting up secured versions of the services you manage every day, including web, email, and database servers that communicate over TLS; locked-down DNS servers with DNSSEC; Tor servers, and hidden services. Each category of solution is presented in its own chapter, with techniques organized based on difficulty level, time commitment, and overall threat. In each case, Rankin begins with techniques any system administrator can quickly implement to protect against entry-level hackers. Next, he moves on to intermediate and advanced techniques intended to safeguard against sophisticated and knowledgeable attackers. An accompanying DVD contains a full, pre-configured copy of the Tails live Linux distribution, making it simple for any sysadmin to bootstrap a highly-secure, privacy-protecting environment in minutes."

Advances in Information and Communication - Kohei Arai 2019-02-01
This book presents a remarkable collection of chapters that cover a wide range of topics in the areas of information and communication technologies and their real-world applications. It gathers the Proceedings of the Future of Information and Communication Conference 2019 (FICC 2019), held in San Francisco, USA from March 14 to 15, 2019. The conference attracted a total of 462 submissions from pioneering

researchers, scientists, industrial engineers, and students from all around the world. Following a double-blind peer review process, 160 submissions (including 15 poster papers) were ultimately selected for inclusion in these proceedings. The papers highlight relevant trends in, and the latest research on: Communication, Data Science, Ambient Intelligence, Networking, Computing, Security, and the Internet of Things. Further, they address all aspects of Information Science and communication technologies, from classical to intelligent, and both the theory and applications of the latest technologies and methodologies. Gathering chapters that discuss state-of-the-art intelligent methods and techniques for solving real-world problems, along with future research directions, the book represents both an interesting read and a valuable asset.

The Debian Administrator's Handbook - Raphaël Hertzog 2015-10-21

Debian GNU/Linux, a very popular non-commercial Linux distribution, is known for its reliability and richness. Built and maintained by an impressive network of thousands of developers throughout the world, the Debian project is cemented by its social contract. This foundation text defines the project's objective: fulfilling the needs of users with a 100% free operating system. The success of Debian and of its ecosystem of derivative distributions (with Ubuntu at the forefront) means that an increasing number of administrators are exposed to Debian's technologies. This Debian Administrator's Handbook, which has been entirely updated for Debian 8 “Jessie”, builds on the success of its 6 previous editions. Accessible to all, this book teaches the essentials to anyone who wants to become an effective and independent Debian GNU/Linux administrator. It covers all the topics that a competent Linux administrator should master, from installation to updating the system, creating packages and compiling the kernel, but also monitoring, backup and migration, without forgetting advanced topics such as setting up SELinux or AppArmor to secure services, automated installations, or virtualization with Xen, KVM or LXC. This book is not only designed for professional system administrators. Anyone who uses Debian or Ubuntu on their own computer is de facto an administrator and will find tremendous value in knowing more about how their system works. Being able to understand and resolve problems will save you invaluable time. Learn more about the book on its official website: debian-handbook.info

Understanding the Linux Kernel - Daniel Pierre Bovet 2002

To thoroughly understand what makes Linux tick and why it's so efficient, you need to delve deep into the heart of the operating system--into the Linux kernel itself. The kernel is Linux--in the case of the Linux operating system, it's the only bit of software to which the term "Linux" applies. The kernel handles all the requests or completed I/O operations and determines which programs will share its processing time, and in what order. Responsible for the sophisticated memory management of the whole system, the Linux kernel is the force behind the legendary Linux efficiency. The new edition of Understanding the Linux Kernel takes you on a guided tour through the most significant data structures, many algorithms, and programming tricks used in the kernel. Probing beyond the superficial features, the authors offer valuable insights to people who want to know how things really work inside their machine. Relevant segments of code are dissected and discussed line by line. The book covers more than just the functioning of the code, it explains the theoretical underpinnings for why Linux does things the way it does. The new edition of the book has been updated to cover version 2.4 of the kernel, which is quite different from version 2.2: the virtual memory system is entirely new, support for multiprocessor systems is improved, and whole new classes of hardware devices have been added. The authors explore each new feature in detail. Other topics in the book include: Memory management including file buffering, process swapping, and Direct memory Access (DMA) The Virtual Filesystem and the Second Extended Filesystem Process creation and scheduling Signals, interrupts, and the essential interfaces to device drivers Timing Synchronization in the kernel Interprocess Communication (IPC) Program execution Understanding the Linux Kernel, Second Edition will acquaint you with all the inner workings of Linux, but is more than just an academic exercise. You'll learn what conditions bring out Linux's best performance, and you'll see how it meets the challenge of providing good system response during process scheduling, file access, and memory management in a wide variety of environments. If knowledge is power, then this book will help you make the most of your Linux system.

Mastering Linux Security and Hardening - Donald A. Tevault 2020-02-21

A comprehensive guide to securing your Linux system against cyberattacks and intruders Key FeaturesDeliver a system that reduces the risk of being hackedExplore a variety of advanced Linux security techniques with the help of hands-on labsMaster the art of securing a Linux environment with this end-to-end practical guideBook Description From creating networks and servers to automating the entire working environment, Linux has been extremely popular with system administrators for the last couple of decades. However, security has always been a major concern. With limited resources available in the Linux security domain, this book will be an invaluable guide in helping you get your Linux systems properly secured. Complete with in-depth explanations of essential concepts, practical examples, and self-assessment questions, this book begins by helping you set up a practice lab environment and takes you through the core functionalities of securing Linux. You'll practice various Linux hardening techniques and advance to setting up a locked-down Linux server. As you progress, you will also learn how to create user accounts with appropriate privilege levels, protect sensitive data by setting permissions and encryption, and configure a firewall. The book will help you set up mandatory access control, system auditing, security profiles, and kernel hardening, and finally cover best practices and troubleshooting techniques to secure your Linux environment efficiently. By the end of this Linux security book, you will be able to confidently set up a Linux server that will be much harder for malicious actors to compromise. What you will learnCreate locked-down user accounts with strong passwordsConfigure firewalls with iptables, UFW, nftables, and firewalldProtect your data with different encryption technologiesHarden the secure shell service to prevent security break-insUse mandatory access control to protect against system exploitsHarden kernel parameters and set up a kernel-level auditing systemApply OpenSCAP security profiles and set up intrusion detectionConfigure securely the GRUB 2 bootloader and BIOS/UEFIWho this book is for This book is for Linux administrators, system administrators, and network engineers interested in securing moderate to complex Linux environments. Security consultants looking to enhance their Linux security skills will also find this book useful. Working experience with the Linux command line and package management is necessary to understand the concepts covered in this book.

Linux Firewalls - Steve Suehring 2015-01-23

The Definitive Guide to Building Firewalls with Linux As the security challenges facing Linux system and network administrators have grown, the security tools and techniques available to them have improved dramatically. In Linux® Firewalls, Fourth Edition, long-time Linux security expert Steve Suehring has revamped his definitive Linux firewall guide to cover the important advances in Linux security. An indispensable working resource for every Linux administrator concerned with security, this guide presents comprehensive coverage of both iptables and nftables. Building on the solid networking and firewalling foundation in previous editions, it also adds coverage of modern tools and techniques for detecting exploits and intrusions, and much more. Distribution neutral throughout, this edition is fully updated for today’s Linux kernels, and includes current code examples and support scripts for Red Hat/Fedora, Ubuntu, and Debian implementations. If you’re a Linux professional, it will help you establish an understanding of security for any Linux system, and for networks of all sizes, from home to enterprise. Inside, you’ll find just what you need to Install, configure, and update a Linux firewall running either iptables or nftables Migrate to nftables, or take advantage of the latest iptables enhancements Manage complex multiple firewall configurations Create, debug, and optimize firewall rules Use Samhain and other tools to protect filesystem integrity, monitor networks, and detect intrusions Harden systems against port scanning and other attacks Uncover exploits such as rootkits and backdoors with chkrootkit

Linux Administration Cookbook - Adam K. Dean 2018-12-31

Over 100 recipes to get up and running with the modern Linux administration ecosystem Key FeaturesUnderstand and implement the core system administration tasks in LinuxDiscover tools and techniques to troubleshoot your Linux systemMaintain a healthy system with good security and backup practicesBook Description Linux is one of the most widely used operating systems among system administrators,and even modern application and server development is heavily reliant on the Linux platform. The Linux Administration Cookbook is your go-to guide to get started on your Linux journey. It will help you understand what that strange little server is doing in the corner of your office, what the mysterious virtual machine languishing in Azure is crunching through, what that circuit-board-like thing is doing under your office TV, and why the LEDs on it are blinking rapidly. This book will get you started with administering Linux, giving you the knowledge and tools you need to troubleshoot day-to-day problems, ranging from a Raspberry Pi to a server in Azure, while giving you a good understanding of the fundamentals of how GNU/Linux works. Through the course of the book, you'll install and configure a system, while the author regales you with errors and anecdotes from his vast experience as a data center hardware engineer, systems administrator, and DevOps consultant. By the end of the book, you will have gained practical knowledge of Linux, which will serve as a bedrock for learning Linux administration and aid you in your Linux journey. What you will learnInstall and manage a Linux server, both locally and in the cloudUnderstand how to perform administration across all Linux distrosWork through evolving concepts such as IaaS versus PaaS, containers, and automationExplore security and configuration best practicesTroubleshoot your system if something goes wrongDiscover and mitigate hardware issues, such as faulty memory and failing drivesWho this book is for If you are a system engineer or system administrator with basic experience of working with Linux, this book is for you.

CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide - Raymond Lacoste 2020-02-24

Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. Master Cisco CCNP ENARSI exam topics Assess your knowledge with chapter-opening quizzes Review key concepts with exam preparation tasks This is the eBook edition of the CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide. This eBook does not include access to the Pearson Test Prep practice exams that comes with the print edition. CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide from Cisco Press allows you to succeed on the exam the first time and is the only self-study resource approved by Cisco. Expert authors Raymond Lacoste and Brad Edgeworth share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. This complete study package includes A test-preparation routine proven to help you pass the exams Do I Know This Already? quizzes, which allow you to decide how much time you need to spend on each section Chapter-ending exercises, which help you drill on key concepts you must know thoroughly Practice exercises that help you enhance your knowledge More than 60 minutes of video mentoring from the author A final preparation chapter, which guides you through tools and resources to help you craft your review and test-taking strategies Study plan suggestions and templates to help you organize and optimize your study time Well regarded for its level of detail, study plans, assessment features, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that ensure your exam success. This official study guide helps you master all the topics on the CCNP Enterprise Advanced Routing ENARSI exam, including Layer 3 technologies, including IPv4/IPv6 routing, EIGRP, OSPF, and BGP VPN services, including MPLS Layer 3 VPNs and DMVPN Infrastructure security, including ACLs, AAA, uRPF, CoPP, and IPv6 first hop security features Infrastructure services, including syslog, SNMP, IP SLA, Object Tracking, NetFlow, Flexible NetFlow, and more

How Linux Works, 2nd Edition - Brian Ward 2014-11-14

Unlike some operating systems, Linux doesn't try to hide the important bits from you—it gives you full control of your computer. But to truly master Linux, you need to understand its internals, like how the system boots, how networking works, and what the kernel actually does. In this completely revised second edition of the perennial best seller How Linux Works, author Brian Ward makes the concepts behind Linux internals accessible to anyone curious about the inner workings of the operating system. Inside, you'll find the kind of knowledge that normally comes from years of experience doing things the hard way. You'll learn: –How Linux boots, from boot loaders to init implementations (systemd, Upstart, and System V) –How the kernel manages devices, device drivers, and processes –How networking, interfaces, firewalls, and servers work –How development tools work and relate to shared libraries –How to write effective shell scripts You'll also explore the kernel and examine key system tasks inside user space, including system calls, input and output, and filesystems. With its combination of background, theory, real-world examples, and patient explanations, How Linux Works will teach you what you need to know to solve pesky problems and take control of your operating system.

Linux Kernel Networking - Rami Rosen 2014-02-28

Linux Kernel Networking takes you on a guided in-depth tour of the current Linux networking implementation and the theory behind it. Linux kernel networking is a complex topic, so the book won't burden you with topics not directly related to networking. This book will also not overload you with cumbersome line-by-line code walkthroughs not directly related to what you're searching for; you'll find just what you need, with in-depth explanations in each chapter and a quick reference at the end of each chapter. Linux Kernel Networking is the only up-to-date reference guide to understanding how networking is implemented, and it will be indispensable in years to come since so many devices now use Linux or operating systems based on Linux, like Android, and since Linux is so prevalent in the data center arena, including Linux-based virtualization technologies like Xen and KVM.

CompTIA Linux+ Practice Tests - Steve Suehring 2019-06-17

The best practice test preparation for the foundational CompTIA Linux+ certification exam If you're preparing for this all-important exam, turn to CompTIA Linux+ Practice Tests. The book covers the 5 objective domains, PLUS one additional 90-question practice exam, for a total of 1,000 practice test questions. Readers will also get one year of FREE access to the online test bank where they can study and work through the questions, reinforcing their skills and knowledge. Study for the CompTIA Linux+ certification with Sybex and get the advantage of exam day confidence. This book covers: Hardware and System Configuration Systems Operation and Maintenance Security Linux Troubleshooting and Diagnostics Automation and Scripting Linux is a UNIX-based operating system originally created by Linus Torvalds with the help of developers around the world. Developed under the GNU General Public License, the source code is free. Because of this, Linux is viewed by many organizations and companies as an excellent, low-cost, secure alternative to expensive OSs, such as Microsoft Windows. The CompTIA Linux+ exam tests a candidate's understanding and familiarity with the Linux Kernel. As the Linux server market share continues to grow, so too does demand for qualified and certified Linux administrators.

Learn Linux Quickly - Ahmed AlKabary 2020-08-21

Learn over 116 Linux commands to develop the skills you need to become a professional Linux system administrator Key FeaturesExplore essential Linux commands and understand how to use Linux help toolsDiscover the power of task automation with bash scripting and Cron jobsGet to grips with various network configuration tools and disk management techniquesBook Description Linux is one of the most sought-after skills in the IT industry, with jobs involving Linux being increasingly in demand. Linux is by far the most popular operating system deployed in both public and private clouds; it is the processing power behind the majority of IoT and embedded devices. Do you use a mobile device that runs on Android? Even Android is a Linux distribution. This Linux book is a practical guide that lets you explore the power of the Linux command-line interface. Starting with the history of Linux, you'll quickly progress to the Linux filesystem hierarchy and learn a variety of basic Linux commands. You'll then understand how to make use of the extensive Linux documentation and help tools. The book shows you how to manage users and groups and takes you through the process of installing and managing software on Linux systems. As you advance, you'll discover how you can interact with Linux processes and troubleshoot network problems before learning the art of writing bash scripts and automating administrative tasks with Cron jobs. In addition to this, you'll get to create your own Linux commands and analyze various disk management techniques. By the end of this book, you'll have gained the Linux skills required to become an efficient Linux system administrator and be able to manage and work productively on Linux systems. What you will learnMaster essential Linux commands and analyze the Linux filesystem hierarchyFind out how to manage users and groups in LinuxAnalyze Linux file ownership and permissionsAutomate monotonous administrative tasks with Cron jobs and bash scriptsUse aliases to create your own Linux commandsUnderstand how to interact with and manage Linux processesBecome well-versed with using a variety of Linux networking commandsPerform disk partitioning, mount filesystems, and create logical volumesWho this book is for This book doesn't assume any prior Linux knowledge, which makes it perfect for beginners. Intermediate and advanced Linux users will also find this book very useful as it covers a wide range of topics necessary for Linux administration.

Linux Firewalls - Michael Rash 2007-09-07

System administrators need to stay ahead of new security vulnerabilities that leave their networks exposed every day. A firewall and an intrusion detection systems (IDS) are two important weapons in that fight, enabling you to proactively deny access and monitor network traffic for signs of an attack. Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop. Concrete examples illustrate concepts such as firewall log analysis and policies, passive network authentication and authorization, exploit packet traces, Snort ruleset emulation, and more with coverage of these topics: –Passive network authentication and OS fingerprinting –iptables log analysis and policies –Application layer attack detection with the iptables string match extension –Building an iptables ruleset that emulates a Snort ruleset –Port knocking vs. Single Packet Authorization (SPA) –Tools for visualizing iptables logs Perl and C code snippets offer practical examples that will help you to maximize your deployment of Linux firewalls. If you're responsible for keeping a network secure, you'll find Linux Firewalls invaluable in your attempt to understand attacks and use iptables—along with psad and fwsnort—to detect and even prevent compromises.

Computer and Network Security Essentials - Kevin Daimi 2017-08-12

This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book’s website at Springer.com.

Linux iptables Pocket Reference - Gregor N. Purdy 2004-08-25

Firewalls, Network Address Translation (NAT), network logging and accounting are all provided by Linux's Netfilter system, also known by the name of the command used to administer it, iptables. The iptables interface is the most sophisticated ever offered onLinux and makes Linux an extremely flexible system for any kind of network filtering you might do. Large sets of filtering rules can be grouped in ways that makes it easy to test them and turn them on and off.Do you watch for all types of ICMP traffic--some of them quite dangerous? Can you take advantage of stateful filtering to simplify the management of TCP connections? Would you like to track how much traffic of various types you get?This pocket reference will help you at those critical moments when someone asks you to open or close a port in a hurry, either to enable some important traffic or to block an attack. The book will keep the subtle syntax straight and help you remember all the values you have to enter in order to be as secure as possible. The book has an introductory section that describes applications,followed by a reference/encyclopaedic section with all the matches and targets arranged alphabetically.

Linux Firewalls - Steve Suehring 2015

"As the security challenges facing Linux system and network administrators have grown, the security tools and techniques available to them have improved dramatically. In Linux firewalls, fourth edition, longt-time Linux security expert Steve Suehring has revamped his definitive Linux firewall guide to cover the important advances in Linux security."--Page 4 de la couverture

Linux Firewalls - Robert Loren Ziegler 2002

An Internet-connected Linux machine is in a high-risk situation. "Linux Firewalls, Third Edition" details security steps that any sized implementation--from home use to enterprise level--might take to protect itself from potential remote attackers. As with the first two editions, this book is especially useful for its explanations of iptables, packet filtering, and firewall optimization along with some advanced concepts including customizing the Linux kernel to enhance security.The third edition, while distribution neutral, has been updated for the current Linux Kernel and provides code examples for Red Hat, SUSE, and Debian implementations. Don' t miss out on the third edition of the critically acclaimed "Linux Firewalls,"

Certified Kubernetes Application Developer (CKAD) Study Guide - Benjamin Muschko 2021-02-02

Developers with the ability to operate, troubleshoot, and monitor applications in Kubernetes are in high demand today. To meet this need, the Cloud Native Computing Foundation created a certification exam to establish a developer's credibility and value in the job market to work in a Kubernetes environment. The Certified Kubernetes Application Developer (CKAD) exam is different from the typical multiple-choice format of other certifications. Instead, the CKAD is a performance-based exam that requires deep knowledge of the tasks under immense time pressure. This study guide walks you through all the topics you need to fully prepare for the exam. Author Benjamin Muschko also shares his personal experience with preparing for all aspects of the exam. Learn when and how to apply Kubernetes concepts to manage an application Understand the objectives, abilities, tips, and tricks needed to pass the CKAD exam Explore the ins and outs of the kubectl command-line tool Demonstrate competency for performing the responsibilities of a Kubernetes application developer Solve real-world Kubernetes problems in a hands-on command-line environment Navigate and solve questions during the CKAD exam

Practical Linux Forensics - Bruce Nikkel 2021-12-21

A resource to help forensic investigators locate, analyze, and understand digital evidence found on modern Linux systems after a crime, security incident or cyber attack. Practical Linux Forensics dives into the technical details of analyzing postmortem forensic images of Linux systems which have been misused, abused, or the target of malicious attacks. It helps forensic investigators locate and analyze digital evidence found on Linux desktops, servers, and IoT devices. Throughout the book, you learn how to identify digital artifacts which may be of interest to an investigation, draw logical conclusions, and reconstruct past activity from incidents. You’ll learn how Linux works from a digital forensics and investigation perspective, and how to interpret evidence from Linux environments. The techniques shown are intended to be independent of the forensic analysis platforms and tools used. Learn how to: Extract evidence from storage devices and analyze partition tables, volume managers, popular Linux filesystems (Ext4, Btrfs, and Xfs), and encryption Investigate evidence from Linux logs, including traditional syslog, the systemd journal, kernel and audit logs, and logs from daemons and applications Reconstruct the Linux startup process, from boot loaders (UEFI and Grub) and kernel initialization, to systemd unit files and targets leading up to a graphical login Perform analysis of power, temperature, and the physical environment of a Linux machine, and find evidence of sleep, hibernation, shutdowns, reboots, and crashes Examine installed software, including distro installers, package formats, and package management systems from Debian, Fedora, SUSE, Arch, and other distros Perform analysis of time and Locale settings, internationalization including language and keyboard settings, and geolocation on a Linux system Reconstruct user login sessions (shell, X11 and Wayland), desktops (Gnome, KDE, and others) and analyze keyrings, wallets, trash cans, clipboards, thumbnails, recent files and other desktop artifacts Analyze network configuration, including interfaces, addresses, network managers, DNS, wireless artifacts (Wi-Fi, Bluetooth, WWAN), VPNs (including WireGuard), firewalls, and proxy settings Identify traces of attached peripheral devices (PCI, USB, Thunderbolt, Bluetooth) including external storage, cameras, and mobiles, and reconstruct printing and scanning activity

Practical Linux Security Cookbook - Tajinder Kalsi 2018-08-31

Enhance file system security and learn about network attack, security tools and different versions of Linux build. Key Features Hands-on recipes to create and administer a secure Linux system Enhance file system security and local and remote user authentication Use various security tools and different versions of Linux for different tasks Book Description Over the last few years, system security has gained a lot of momentum and software professionals are focusing heavily on it. Linux is often treated as a highly secure operating system. However, the reality is that Linux has its share of security flaws, and these security flaws allow attackers to get into your system and modify or even destroy your important data. But there’s no need to panic, since there are various mechanisms by which these flaws can be removed, and this book will help you learn about different types of Linux security to create a more secure Linux system. With a step-by-step recipe approach, the book starts by introducing you to various threats to Linux systems. Then, this book will walk you through customizing the Linux kernel and securing local files. Next, you will move on to managing user authentication both locally and remotely and mitigating network attacks. Later, you will learn about application security and kernel vulnerabilities. You will also learn about patching Bash vulnerability, packet filtering, handling incidents, and monitoring system logs. Finally, you will learn about auditing using system services and performing vulnerability scanning on Linux. By the end of this book, you will be able to secure your Linux systems and create a robust environment. What you will learn Learn about vulnerabilities and exploits in relation to Linux systems Configure and build a secure kernel and test it Learn about file permissions and how to securely modify files Authenticate users remotely and securely copy files on remote systems Review different network security methods and tools Perform vulnerability scanning on Linux machines using tools Learn about malware scanning and read through logs Who this book is for This book 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.

Pro Linux System Administration - Dennis Matotek 2017-03-14

Implement a SOHO or SMB Linux infrastructure to expand your business and associated IT capabilities. Backed by the expertise and experienced guidance of the authors, this book provides everything you need to move your business forward. Pro Linux System Administration makes it easy for small- to medium–sized businesses to enter the world of zero–cost software running on Linux and covers all the distros you might want to use, including Red Hat, Ubuntu, Debian, and CentOS. Pro Linux System Administration takes a layered, component–based approach to open source business systems, while training system administrators as the builders of business infrastructure. Completely updated for this second edition, Dennis Matotek takes you through an infrastructure-as-code approach, seamlessly taking you through steps along the journey of Linux administration with all you need to master complex systems. This edition now includes Jenkins, Ansible, Logstash and more. What You'll Learn: Understand Linux architecture Build, back up, and recover Linux servers Create basic networks and network services with Linux Build and implement Linux infrastructure and services including mail, web, databases, and file and print Implement Linux security Resolve Linux performance and capacity planning issues Who This Book Is For: Small to medium–sized business owners looking to run their own IT, system administrators considering migrating to Linux, and IT systems integrators looking for an extensible Linux infrastructure management approach.

Mastering Linux Administration - Alexandru Calcatinge 2021-06-18

Develop advanced skills for working with Linux systems on-premises and in the cloud Key FeaturesBecome proficient in everyday Linux administration tasks by mastering the Linux command line and using automationWork with the Linux filesystem, packages, users, processes, and daemonsDeploy Linux to the cloud with AWS, Azure, and KubernetesBook Description Linux plays a significant role in modern data center management and provides great versatility in deploying and managing your workloads on-premises and in the cloud. This book covers the important topics you need to know about for your everyday Linux administration tasks. The book starts by helping you understand the Linux command line and how to work with files, packages, and filesystems. You'll then begin administering network services and hardening security, and learn about cloud computing, containers, and orchestration. Once you've learned how to work with the command line, you'll explore the essential Linux commands for managing users, processes, and daemons and discover how to secure your Linux environment using application security frameworks and firewall managers. As you advance through the chapters, you'll work with containers, hypervisors, virtual machines, Ansible, and Kubernetes. You'll also learn how to deploy Linux to the cloud using AWS and Azure. By the end of this Linux book, you'll be well-versed with Linux and have mastered everyday administrative tasks using workflows spanning from on-premises to the cloud. If you also find yourself adopting DevOps practices in the process, we'll consider our mission accomplished. What you will learnUnderstand how Linux works and learn basic to advanced Linux administration skillsExplore the most widely used commands for managing the Linux filesystem, network, security, and moreGet to grips with different networking and messaging protocolsFind out how Linux security works and how to configure SELinux, AppArmor, and Linux iptablesWork with virtual machines and containers and understand container orchestration with KubernetesWork with containerized workflows using Docker and KubernetesAutomate your configuration management workloads with AnsibleWho this book is for If you are a Linux administrator who wants to understand the fundamentals and as well as modern concepts of Linux system administration, this book is for you. Windows System Administrators looking to extend their knowledge to the Linux OS will also benefit from this book.

JavaScript Step by Step - Steve Suehring 2010

Provides information on creating Web applications with JavaScript.

Linux for Networking Professionals - Rob VandenBrink 2021-11-11

Get to grips with the most common as well as complex Linux networking configurations, tools, and services to enhance your professional skills Key Features Learn how to solve critical networking problems using real-world examples Configure common networking services step by step in an enterprise environment Discover how to build infrastructure with an eye toward defense against common attacks Book Description As Linux continues to gain prominence, there has been a rise in network services being deployed on Linux for cost and flexibility reasons. If you are a networking professional or an infrastructure engineer involved with networks, extensive knowledge of Linux networking is a must. This book will guide you in building a strong foundation of Linux networking concepts. The book begins by covering various major distributions, how to pick the right distro, and basic Linux network configurations. You'll then move on to Linux network diagnostics, setting up a Linux firewall, and using Linux as a host for network services. You'll discover a wide range of network services, why they're important, and how to configure them in an enterprise environment. Finally, as you work with the example builds in this Linux book, you'll learn to configure various services to defend against common attacks. As you advance to the final chapters, you'll be well on your way towards building the underpinnings for an all-Linux datacenter. By the end of this book, you'll be able to not only configure common Linux network services confidently, but also use tried-and-tested methodologies for future Linux installations. What you will learn Use Linux as a troubleshooting and diagnostics platform Explore Linux-based network services Configure a Linux firewall and set it up for network services Deploy and configure Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services securely Configure Linux for load balancing, authentication, and authorization services Use Linux as a logging platform for network monitoring Deploy and configure Intrusion Prevention Services (IPS) Set up Honeypot solutions to detect and foil attacks Who this book is for This book is for IT and Windows professionals and admins looking for guidance in managing Linux-based networks. Basic knowledge of networking is necessary to get started with this book.

Implementing and Administering Cisco Solutions: 200-301 CCNA Exam Guide - Glen D. Singh 2020-11-13

Prepare to take the Cisco Certified Network Associate (200-301 CCNA) exam and get to grips with the essentials of networking, security, and automation Key FeaturesSecure your future in network engineering with this intensive boot camp-style certification guideGain knowledge of the latest trends in Cisco networking and security and boost your career prospectsDesign and implement a wide range of networking technologies and services using Cisco solutionsBook Description In the dynamic technology landscape, staying on top of the latest technology trends is a must, especially if you want to build a career in network administration. Achieving CCNA 200-301 certification will validate your knowledge of networking concepts, and this book will help you to do just that. This exam guide focuses on the fundamentals to help you gain a high-level understanding of networking, security, IP connectivity, IP services, programmability, and automation. Starting with the functions of various networking components, you'll discover how they are used to build and improve an enterprise network. You'll then delve into configuring networking devices using a command-line interface (CLI) to provide network access, services, security, connectivity, and management. The book covers important aspects of network engineering using a variety of hands-on labs and real-world scenarios that will help you gain essential practical skills. As you make progress, this CCNA certification study guide will help you get to grips with the solutions and technologies that you need to implement and administer a broad range of modern networks and IT infrastructures. By the end of this book, you'll have gained the confidence to pass the Cisco CCNA 200-301 exam on the first attempt and be well-versed in a variety of network administration and security engineering solutions. What you will learnUnderstand the benefits of creating an optimal networkCreate and implement IP schemes in an enterprise networkDesign and implement virtual local area networks (VLANs)Administer dynamic routing protocols, network security, and automationGet to grips with various IP services that are essential to every networkDiscover how to troubleshoot networking devicesWho this book is for This guide is for IT professionals looking to boost their network engineering and security administration career prospects. If you want to gain a Cisco CCNA certification and start a career as a network security professional, you'll find this book useful. Although no knowledge about Cisco technologies is expected, a basic understanding of industry-level network fundamentals will help you grasp the topics covered easily.

Linux Advanced Routing and Traffic Control HOWTO - Gregory Maxwell 2019-11-06

Summary This classic howto was written in 2002, but it is still a must-read howto for any Linux networking professionals today. Many practical examples are included in the book.It is a very hands−on approach to iproute2, traffic shaping, policy routing and a bit of netfilter.This is a book you should have on your bookshelf. Table of Contents Dedication Introduction Introduction to iproute2 Rules-routing policy database GRE and other tunnles IPv6 tunning with Cisco and/or 6bone IPSec:secure IP over the internet Multicast routing Queueing Disciplines for Bandwdith Management Load sharing over multiple interfaces Netfilter & iproute - marking packets Advanced filters for (re-)classifying packets Kernel network parameters Advanced &less common queueing disciplines Cookbook Building bridges, and pseudo-bridges with Proxy ARP Dynamic routing - OSPF and BGP Other possibilities Further reading Acknowledgements

Beginning Ethical Hacking with Kali Linux - Sanjib Sinha 2018-11-29

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you’ll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will LearnMaster common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systemsWho This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

Exam Ref MCSE 70-413 - Steve Suehring 2012-11-15

Prepare for Exam 70-413—and help demonstrate your real-world mastery of enterprise server design and implementation. Designed for experienced, MCSA-certified professionals ready to advance their status—Exam Ref focuses on the critical-thinking and decision-making acumen needed for success at the MCSE level. Optimize your exam-prep by focusing on the expertise needed to: Plan and Deploy a Server Infrastructure Design and Implement Network Infrastructure Services Design and Implement Network Access Services Design and Implement an Active Directory Infrastructure (Logical) Design and Implement an Active Directory Infrastructure (Physical)

SQL Injection Strategies - Ettore Galluccio 2020-07-15

Learn to exploit vulnerable database applications using SQL injection tools and techniques, while understanding how to effectively prevent attacks Key FeaturesUnderstand SQL injection and its effects on websites and other systemsGet hands-on with SQL injection using both manual and automated toolsExplore practical tips for various attack and defense strategies relating to SQL injectionBook Description SQL injection (SQLi) is probably the most infamous attack that can be unleashed against applications on the internet. SQL Injection Strategies is an end-to-end guide for beginners looking to learn how to perform SQL injection and test the security of web applications, websites, or databases, using both manual and automated techniques. The book serves as both a theoretical and practical guide to take you through the important aspects of SQL injection, both from an attack and a defense perspective. You’ll start with a thorough introduction to SQL injection and its impact on websites and systems. Later, the book features steps to configure a virtual environment, so you can try SQL injection techniques safely on your own computer. These tests can be performed not only on web applications but also on web services and mobile applications that can be used for managing IoT environments. Tools such as sqlmap and others are then covered, helping you understand how to use them effectively to perform SQL injection attacks. By the end of this book, you will be well-versed with SQL injection, from both the attack and defense perspective. What you will learnFocus on how to defend against SQL injection attacksUnderstand web application securityGet up and running with a variety of SQL injection conceptsBecome well-versed with different SQL injection scenariosDiscover SQL injection manual attack techniquesDelve into SQL injection automated techniquesWho this book is for This book is ideal for penetration testers, ethical hackers, or anyone who wants to learn about SQL injection and the various attack and defense strategies against this web security vulnerability. No prior knowledge of SQL injection is needed to get started with this book.

SELinux System Administration - Third Edition - Sven Vermeulen 2020-12-04

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.

The Linux Programmer's Toolbox - John Fusco 2007-03-06

Master the Linux Tools That Will Make You a More Productive, Effective Programmer The Linux

Programmer's Toolbox helps you tap into the vast collection of open source tools available for GNU/Linux. Author John Fusco systematically describes the most useful tools available on most GNU/Linux distributions using concise examples that you can easily modify to meet your needs. You'll start by learning the basics of downloading, building, and installing open source projects. You'll then learn how open source tools are distributed, and what to look for to avoid wasting time on projects that aren't ready for you. Next, you'll learn the ins and outs of building your own projects. Fusco also demonstrates what to look for in a text editor, and may even show you a few new tricks in your favorite text editor. You'll enhance your knowledge of the Linux kernel by learning how it interacts with your software. Fusco walks you through the fundamentals of the Linux kernel with simple, thought-provoking examples that illustrate the principles behind the operating system. Then he shows you how to put this knowledge to use with more advanced tools. He focuses on how to interpret output from tools like sar, vmstat, valgrind, strace, and apply it to your application; how to take advantage of various programming APIs to develop your own tools; and how to write code that monitors itself. Next, Fusco covers tools that help you enhance the performance of your software. He explains the principles behind today's multicore CPUs and demonstrates how to squeeze the most performance from these systems. Finally, you'll learn tools and techniques to debug your code under any circumstances. Coverage includes Maximizing productivity with editors, revision control tools, source code browsers, and "beautifiers" Interpreting the kernel: what your tools are telling you Understanding processes–and the tools available for managing them Tracing and resolving application bottlenecks with gprof and valgrind Streamlining and automating the documentation process Rapidly finding help, solutions, and workarounds when you need them Optimizing program code with sar, vmstat, iostat, and other tools Debugging IPC with shell commands: signals, pipes, sockets, files, and IPC objects Using printf, gdb, and other essential debugging tools Foreword Preface Acknowledgments About the Author Chapter 1 Downloading and Installing Open Source Tools Chapter 2 Building from Source Chapter 3 Finding Help Chapter 4 Editing and Maintaining Source Files Chapter 5 What Every Developer Should Know about the Kernel Chapter 6 Understanding Processes Chapter 7 Communication between Processes Chapter 8 Debugging IPC with Shell Commands Chapter 9 Performance Tuning Chapter 10 Debugging Index

Guidelines on Firewalls and Firewall Policy - Karen Scarfone 2010-03

This updated report provides an overview of firewall technology, and helps organizations plan for and implement effective firewalls. It explains the technical features of firewalls, the types of firewalls that are available for implementation by organizations, and their security capabilities. Organizations are advised on the placement of firewalls within the network architecture, and on the selection, implementation, testing, and management of firewalls. Other issues covered in detail are the development of firewall policies, and recommendations on the types of network traffic that should be prohibited. The appendices contain helpful supporting material, including a glossary and lists of acronyms and abreviations; and listings of in-print and online resources. Illus.

Hands-On Penetration Testing on Windows - Phil Bramwell 2018-07-30

Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises, and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode. We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for them. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for penetration testers, ethical hackers, and individuals breaking into the pentesting role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary

PHP, MySQL, JavaScript & HTML5 All-in-One For Dummies - Steve Suehring 2013-04

Introduces the four essential programming languages required for creating dynamic Web sites, and explains how to install them on different operating systems, use CSS to create forms, code with jQuery, and administer a MySQL database.

E-Business and Telecommunications - Mohammad S. Obaidat 2021-10-30

The present book includes extended and revised versions of a set of selected papers presented at the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020, held as an online web-based event (due to the COVID-19 pandemic) in July 2020.ICETE 2020 is a joint conference aimed at bringing together researchers, engineers and practitioners interested in information and communication technologies, including data communication networking, e-business, optical communication systems, security and cryptography, signal processing and multimedia applications, and wireless networks and mobile systems.The 10 full papers included in the volume were carefully selected from the 30 submissions accepted to participate in the conference.

Hardening Linux - James Turnbull 2006-11-01

*Imparts good security doctrine, methodology, and strategies *Each application-focused chapter will be able to be used as a stand-alone HOW-TO for that particular application. *Offers users a selection of resources (websites, mailing lists, and books) to further their knowledge.

Linux Administration: A Beginner’s Guide, Eighth Edition - Wale Soyinka 2020-04-10

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. Gain Essential Linux Administration Skills Easily Effectively set up and manage popular Linux distributions on individual servers and build entire network infrastructures using this practical resource. Fully updated to cover the latest tools and techniques, Linux Administration: A Beginner’s Guide, Eighth Edition features clear explanations, step-by-step instructions, and real-world examples. Find out how to configure hardware and software, work from the command line or GUI, maintain Internet and network services, and secure your data. Performance tuning, virtualization, containers, software management, security, and backup solutions are covered in detail. Install and configure Linux, including the latest distributions from Fedora, Ubuntu, CentOS, openSUSE, Debian, and RHEL. Set up and administer core system services, daemons, users, and groups. Manage software applications from source code or binary packages. Customize, build, or patch the Linux kernel. Understand and manage the Linux network stack and networking protocols, including TCP/IP, ARP, IPv4, and IPv6. Minimize security threats and build reliable firewalls and routers with Netfilter (iptables and nftables) and Linux. Create and maintain DNS, FTP, web, e-mail, print, LDAP, VoIP, and SSH servers and services. Share resources using GlusterFS, NFS, and Samba. Spin-up and manage Linux-based servers in popular cloud environments, such as OpenStack, AWS, Azure, Linode, and GCE. Explore virtualization and container technologies using KVM, Docker, Kubernetes, and Open Container Initiative (OCI) tooling. Download specially curated Virtual Machine image and containers that replicate various exercises, software, servers, commands, and concepts covered in the book. Wale Soyinka is a father, system administrator, a DevOps/SecOps aficionado, an open source evangelist, a hacker, and a well-respected world-renowned chef (in his mind). He is the author of Advanced Linux Administration as well as other Linux, Network, and Windows administration training materials.