Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance

Right here, we have countless ebook **Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance** and collections to check out. We additionally find the money for variant types and after that type of the books to browse. The up to standard book, fiction, history, novel, scientific research, as skillfully as various other sorts of books are readily affable here.

As this Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance, it ends taking place subconscious one of the favored ebook Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance collections that we have. This is why you remain in the best website to see the incredible ebook to have.

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

Research Anthology on Securing Mobile Technologies and Applications Management Association, Information Resources 2021-02-05 Mobile technologies have become a staple in society for their accessibility and diverse range of applications that are continually growing and advancing. Users are increasingly using these devices for activities beyond simple communication including gaming and e-commerce and to access confidential information including banking accounts and medical records. While mobile devices are being so widely used and accepted in daily life, and subsequently housing more and more personal data, it is evident that the security of these devices is paramount. As mobile applications now create easy access to personal information, they can incorporate location tracking services, and data collection can happen discreetly behind the scenes. Hence, there needs to be more security and privacy measures enacted to ensure that mobile technologies can be used safely. Advancements in trust and privacy, defensive strategies, and steps for securing the device are important foci as mobile technologies are highly popular and rapidly developing. The Research Anthology on Securing Mobile Technologies and Applications discusses the strategies, methods, and technologies being employed for security amongst mobile devices and applications. This comprehensive book explores the security support that needs to be required on mobile devices to avoid application damage, hacking, security breaches and attacks, or unauthorized accesses to personal data. The chapters cover the latest technologies that are being used such as cryptography, verification systems, security policies and contracts, and general network security procedures along with a look into cybercrime and forensics. This book is essential for software engineers, app developers, computer scientists, security and IT professionals, practitioners, stakeholders, researchers, academicians, and students interested in how mobile technologies and applications are implementing security protocols and tactics amongst devices.

Endpoint Security Mark Kadrich 2007 Reveals how to protect one's network from potential security threats that might enter via such endpoints as employee laptops, PDAs, and other end-user devices, explaining how to identify the products, tools, and processes required to secure endpoint devices; how to configure them securely; how to identify and remediate a compromised device; and how to protect a network from the growing number of endpoint viruses and malware. Original. (Advanced)

Security Strategies in Windows Platforms and Applications Michael G. Solomon 2010-11-15 PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! More than 90 percent of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Written by an industry expert, Security Strategies in Windows Platforms and Applications focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and step-by-step examples, this must-have resource will ensure readers are educated on the latest Windows security strategies and techniques.

LSC (GLOBE UNIVERSITY) SD256: VS ePub for Mobile Application Security Himanshu Dwivedi 2010-02-18 Secure today's mobile devices and applications Implement a systematic approach to security in your mobile application development with help from this practical guide. Featuring case studies, code examples, and best practices, Mobile Application Security details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware, and buffer overflow exploits are also covered in this comprehensive resource. Design highly isolated, secure, and authenticated mobile applications Use the Google Android emulator, debugger, and third-party security tools Configure Apple iPhone APIs to prevent overflow and SQL injection attacks Employ private and public key cryptography on Windows Mobile devices Enforce fine-grained security policies using the BlackBerry Enterprise Server Plug holes in Java Mobile Edition, SymbianOS, and WebOS applications Test for XSS, CSRF, HTTP redirects, and phishing attacks on WAP/Mobile HTML applications Identify and eliminate threats from Bluetooth, SMS, and GPS services Himanshu Dwivedi is a co-founder of iSEC Partners (www.isecpartners.com), an information security firm specializing in application security. Chris Clark is a principal security consultant with iSEC Partners. David Thiel is a principal security consultant with iSEC Partners.

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.
Network Security Strategies Aditya Mukherjee 2020-11-06 Build a resilient network and prevent advanced cyber attacks and breaches Key Features Explore modern cybersecurity techniques to protect your networks from ever-evolving cyber threats Prevent cyber attacks by using robust cybersecurity strategies Unlock the secrets of network security Book Description With advanced cyber attacks severely impacting industry giants and the constantly evolving threat landscape, organizations are adopting complex systems to maintain robust and secure environments. Network Security Strategies will help you get well-versed with the tools and techniques required to protect any network environment against modern cyber threats. You'll understand how to identify security vulnerabilities across the network and how to effectively use a variety of network security techniques and platforms. Next, the book will show you how to design a robust network that provides top-notch security to protect against traditional and new evolving attacks. With the help of detailed solutions and explanations, you'll be able to monitor networks skillfully and identify potential risks. Finally, the book will cover topics relating to thought leadership and the management aspects of network security. By the end of this network security book, you'll be well-versed in defending your network from threats and be able to consistently maintain operational efficiency, security, and privacy in your environment. What you will learn Understand network security essentials, including concepts, mechanisms, and solutions to implement secure networks Get to grips with setting up and threat monitoring cloud and wireless networks Defend your network against emerging cyber threats in 2020 Discover tools, frameworks, and best practices for network penetration testing Understand digital forensics to enhance your network security skills Adopt a proactive approach to stay ahead in network security Who this book is for This book is for anyone looking to explore information security, privacy, malware, and cyber threats. Security experts who want to enhance their skill set will also find this book useful. A prior understanding of cyber threats and information security will help you understand the key concepts covered in the book more effectively.
Security Strategies in Linux Platforms and Applications + Virtual Lab Access Michael Jang 2018-05-10 .
Mastering Defensive Security Cesar Bravo 2022-01-06 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 FeaturesGet hold of the best defensive security strategies and toolsDevelop a defensive security strategy at an enterprise levelGet hands-on with advanced cybersecurity threat detection, including XSS, SQL injections, brute forcing web applications, and moreBook 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 learnBecome well versed with concepts related to defensive securityDiscover strategies and tools to secure the most vulnerable factor – the userGet hands-on experience using and configuring the best security toolsUnderstand how to apply hardening techniques in Windows and Unix environmentsLeverage malware analysis and forensics to enhance your security strategySecure Internet of Things (IoT) implementationsEnhance the security of web applications and cloud deploymentsWho this book is for This book is for all IT professionals who want to take their first steps into the world of defensive security; from system admins and programmers to data analysts and data scientists with an interest in security. Experienced cybersecurity professionals working on broadening their knowledge and keeping up to date with the latest defensive developments will also find plenty of useful information in this book. You'll need a basic understanding of networking, IT, servers, virtualization, and cloud platforms before you get started with this book.
The Linux Development Platform Rafeeq Ur Rehman 2003 Two leading Linux developers show how to choose the best tools for your specific needs and integrate them into a complete development environment that maximizes your effectiveness in any project, no matter how large or complex. Includes research, requirements, coding, debugging, deployment, maintenance and beyond, choosing and implementing editors, compilers, assemblers, debuggers, version control systems, utilities, using Linux Standard Base to deliver applications that run reliably on a wide range of Linux systems, comparing Java development options for Linux platforms, using Linux in cross-platform and embedded development environments.
Ten Strategies of a World-Class Cybersecurity Operations Center Carson Zimmerman 2014-07-01 Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.
Principles of Modern Operating Systems Jose M Garrido 2011-09-26 This revised and updated Second Edition presents a practical introduction to operating systems and illustrates these principles through a hands-on approach using accompanying simulation models developed in Java and C++. This text is appropriate for upper-level undergraduate courses in computer science. Case studies throughout the text feature the implementation of Java and C++ simulation models, giving students a thorough look at both the theoretical and the practical concepts discussed in modern OS courses. This pedagogical approach is designed to present a clearer, more practical look at OS concepts, techniques, and methods without sacrificing the theoretical rigor that is necessary at this level. It is an ideal choice for those interested in gaining comprehensive, hands-on experience using the modern techniques and methods necessary for working with these complex systems. Every new printed copy is accompanied with a CD-ROM containing simulations (eBook version does not include CD-ROM). New material added to the Second Edition: - Chapter 11 (Security) has been revised to include the most up-to-date information - Chapter 12 (Firewalls and Network Security) has been updated to include material on middleware that allows applications on separate machines to communicate (e.g. RMI, COM+, and Object Broker) - Includes a new chapter dedicated to Virtual Machines - Provides introductions to various types of scams - Updated to include information on Windows 7 and Mac OS X throughout the text - Contains new material on basic hardware architecture that operating systems depend on - Includes new material on handling multi-core CPUs Instructor Resources: -Answers to the end of chapter questions - PowerPoint Lecture Outlines
Application Security for the Android Platform Jeff Six 2011-12-08 This book will educate readers on the need for application security and secure coding practices when designing any app. No prior knowledge of

security or secure programming techniques is assumed. The book will discuss the need for such practices, how the Android environment is structured with respect to security considerations, what services and techniques are available on the platform to protect data, and how developers can build and code applications that address the risk to their applications and the data processed by them. This text is especially important now, as Android is fast becoming the mobile platform target of choice for attackers attempting to steal data from mobile devices.
Security Strategies in Linux Platforms and Applications Ric Messier 2024 "Incorporating real-world examples and exercises throughout, Security Strategies in Linux Platforms and Applications discusses every major aspect of security on a Linux system, including coverage of the latest Linux distributions and kernels. Written by industry experts, the text opens with a review of the risks, threats, and vulnerabilities associated with Linux as an operating system. Part 2 discusses how to take advantage of the layers of security available to Linux - user and group options, filesystems, and security options for important services. The text concludes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments"--
Security Strategies in Linux Platforms and Applications Michael Jang 2010-10-25 PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux--user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.
Laboratory Manual Version 1.5 Security Strategies in Linux Platforms and Applications Vlab Solutions 2013-06-10 The Laboratory Manual Version 1.5 To Accompany Security Strategies In Linux Platforms And Applications Is The Lab Companion To The Information Systems And Security Series Title, Security Strategies In Linux Platforms And Applications. It Provides Hands-On Exercises Using The Jones & Bartlett Learning Virtual Security Cloud Labs, That Provide Real-World Experience With Measurable Learning Outcomes. About The Series: Visit Www.Issaseries.Com For A Complete Look At The Series! The Jones & Bartlett Learning Information System & Assurance Series Delivers Fundamental IT Security Principles Packed With Real-World Applications And Examples For IT Security, Cybersecurity, Information Assurance, And Information Systems Security Programs. Authored By Certified Information Systems Security Professionals (Cissps), And Reviewed By Leading Technical Experts In The Field, These Books Are Current Forward-Thinking Resources That Enable Readers To Solve The Cybersecurity Challenges Of Today And Tomorrow.
Identity Attack Vectors Morey J. Haber 2019-12-17 Discover how poor identity and privilege management can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments
Android Security Internals Nikolay Elenkov 2014-10-14 There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In Android Security Internals, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions, cryptographic providers, and device administration. You'll learn: –How Android permissions are declared, used, and enforced –How Android manages application packages and employs code signing to verify their authenticity –How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks –About Android's credential storage system and APIs, which let applications store cryptographic keys securely –About the online account management framework and how Google accounts integrate with Android –About the implementation of verified boot, disk encryption, lockscreen, and other device security features –How Android's bootloader and recovery OS are used to perform full system updates, and how to obtain root access With its unprecedented level of depth and detail, Android Security Internals is a must-have for any security-minded Android developer.
Network Security Essentials William Stallings 2007 Network Security Essentials, Third Edition is a thorough, up-to-date introduction to the deterrence, prevention, detection, and correction of security violations involving information delivery across networks and the Internet.
CWNA Guide to Wireless LANs Mark Ciampa 2012-06-19 CWNA GUIDE TO WIRELESS LANS, 3rd Edition provides students with the conceptual knowledge and hands-on skills needed to work with wireless technology in a network administration environment as well as pass the Certified Wireless Network Administrator (CWNA) exam. The text covers fundamental topics, such as planning, designing, installing, securing, and configuring wireless LANs. It also details common wireless LAN uses including maintenance, security, and business applications. The third edition is designed around the latest version of the CWNA exam, as well as the new IEEE 802.11 standard, making CWNA GUIDE TO WIRELESS LANS the practical guide that prepares students for real-world wireless networking. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Linux Mastery Jonathan Bates 2016-08-30 Discover and learn one of the most reliable and easy-to-use Operating Systems around!Do you want an excellent Operating System and be able to use it for FREE? Come on, you're close on the right path of discovering and experiencing it!If you are in need of a fast, reliable, secured, flexible, easy to use and understand, and most importantly, it is a compatible software to all devices; here it is, the Linux Operating System.Linux is one of the most reliable Operating System (OS), a fast way to use different applications, and it's FREE to use and download. That makes this Operating System stand out with the others. It is just ONE CLICK away and you'll enjoy the perks of having this OS in your own computers or devices. More than anything, Linux can be used for a variety of applications. Whether you're opting to create a better system for business, or just want to be more creative and play around with things, Linux can help you do a great job. If you're too curious and eager enough to know more about this Operating System (OS) and its process, this book will help you understand it better. The "Linux Mastery - The Ultimate Linux Operating System and Command Line Mastery Guide" book gives you all the information that you want to know about this "one of a kind" Operating System.Moreover, in this book you will learn the following:* What is

Linux?* Why Linux - The Benefits of Linux* Choosing a Distribution* Preparing to Install Linux* Installing Linux* Using Linux for Work and Play* Getting to Know Commands* Managing Files and Directories* Administration and SecurityFurthermore, this book contains proven steps and strategies on how to make use of Linux, whether for work or play, understand the commands that you have to use, choose distributions, and understand exactly why Linux matters-and more.So what are you waiting for? Experience and explore the Linux Operating System

Practical Industrial Internet of Things Security Sravani Bhattacharjee 2018-07-30 Skillfully navigate through the complex realm of implementing scalable, trustworthy industrial systems and architectures in a hyper-connected business world. Key Features Gain practical insight into security concepts in the Industrial Internet of Things (IIoT) architecture Demystify complex topics such as cryptography and blockchain Comprehensive references to industry standards and security frameworks when developing IIoT blueprints Book Description Securing connected industries and autonomous systems is a top concern for the Industrial Internet of Things (IIoT) community. Unlike cybersecurity, cyber-physical security is an intricate discipline that directly ties to system reliability as well as human and environmental safety. Practical Industrial Internet of Things Security enables you to develop a comprehensive understanding of the entire spectrum of securing connected industries, from the edge to the cloud. This book establishes the foundational concepts and tenets of IIoT security by presenting real-world case studies, threat models, and reference architectures. You'll work with practical tools to design risk-based security controls for industrial use cases and gain practical know-how on the multi-layered defense techniques including Identity and Access Management (IAM), endpoint security, and communication infrastructure. Stakeholders, including developers, architects, and business leaders, can gain practical insights in securing IIoT lifecycle processes, standardization, governance and assess the applicability of emerging technologies, such as blockchain, Artificial Intelligence, and Machine Learning, to design and implement resilient connected systems and harness significant industrial opportunities. What you will learn Understand the crucial concepts of a multi-layered IIoT security framework Gain insight on securing identity, access, and configuration management for large-scale IIoT deployments Secure your machine-to-machine (M2M) and machine-to-cloud (M2C) connectivity Build a concrete security program for your IIoT deployment Explore techniques from case studies on industrial IoT threat modeling and mitigation approaches Learn risk management and mitigation planning Who this book is for Practical Industrial Internet of Things Security is for the IIoT community, which includes IIoT researchers, security professionals, architects, developers, and business stakeholders. Anyone who needs to have a comprehensive understanding of the unique safety and security challenges of connected industries and practical methodologies to secure industrial assets will find this book immensely helpful. This book is uniquely designed to benefit professionals from both IT and industrial operations backgrounds.

Securing DevOps Julien Vehent 2018-08-20 Summary Securing DevOps explores how the techniques of DevOps and security should be applied together to make cloud services safer. This introductory book reviews the latest practices used in securing web applications and their infrastructure and teaches you techniques to integrate security directly into your product. You'll also learn the core concepts of DevOps, such as continuous integration, continuous delivery, and infrastructure as a service. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology An application running in the cloud can benefit from incredible efficiencies, but they come with unique security threats too. A DevOps team's highest priority is understanding those risks and hardening the system against them. About the Book Securing DevOps teaches you the essential techniques to secure your cloud services. Using compelling case studies, it shows you how to build security into automated testing, continuous delivery, and other core DevOps processes. This experience-rich book is filled with mission-critical strategies to protect web applications against attacks, deter fraud attempts, and make your services safer when operating at scale. You'll also learn to identify, assess, and secure the unique vulnerabilities posed by cloud deployments and automation tools commonly used in modern infrastructures. What's inside An approach to continuous security Implementing test-driven security in DevOps Security techniques for cloud services Watching for fraud and responding to incidents Security testing and risk assessment About the Reader Readers should be comfortable with Linux and standard DevOps practices like CI, CD, and unit testing. About the Author Julien Vehent is a security architect and DevOps advocate. He leads the Firefox Operations Security team at Mozilla, and is responsible for the security of Firefox's high-traffic cloud services and public websites. Table of Contents Securing DevOps PART 1 - Case study: applying layers of security to a simple DevOps pipeline Building a barebones DevOps pipeline Security layer 1: protecting web applications Security layer 2: protecting cloud infrastructures Security layer 3: securing communications Security layer 4: securing the delivery pipeline PART 2 - Watching for anomalies and protecting services against attacks Collecting and storing logs Analyzing logs for fraud and attacks Detecting intrusions The Caribbean breach: a case study in incident response PART 3 - Maturing DevOps security Assessing risks Testing security Continuous security

Network Security, Firewalls and VPNs J. Michael Stewart 2013-07-15 PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Fully revised and updated with the latest data from the field, Network Security, Firewalls, and VPNs, Second Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization s network is connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks. Key Features: -Introduces the basics of network security exploring the details of firewall security and how VPNs operate -Illustrates how to plan proper network security to combat hackers and outside threats -Discusses firewall configuration and deployment and managing firewall security -Identifies how to secure local and internet communications with a VPN Instructor Materials for Network Security, Firewalls, VPNs include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts About the Series This book is part of the Information Systems Security and Assurance Series from Jones and Bartlett Learning. Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well."

Advanced Persistent Security Ira Winkler 2016-11-30 Advanced Persistent Security covers secure network design and implementation, including authentication, authorization, data and access integrity, network monitoring, and risk assessment. Using such recent high profile cases as Target, Sony, and Home Depot, the book explores information security risks, identifies the common threats organizations face, and presents tactics on how to prioritize the right countermeasures. The book discusses concepts such as malignant versus malicious threats, adversary mentality, motivation, the economics of cybercrime, the criminal infrastructure, dark webs, and the criminals organizations currently face. Contains practical and cost-effective recommendations for proactive and reactive protective measures Teaches users how to establish a viable threat intelligence program Focuses on how social networks present a double-edged sword against security programs

Kali Linux Network Scanning Cookbook Justin Hutchens 2014-08-21 Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

SELinux by Example Frank Mayer 2006-07-27 SELinux: Bring World-Class Security to Any Linux Environment! SELinux offers Linux/UNIX integrators, administrators, and developers a state-of-the-art platform for building and maintaining highly secure solutions. Now that SELinux is

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

Designing Data-Intensive Applications Martin Kleppmann 2017-03-16 Data is at the center of many challenges in system design today. Difficult issues need to be figured out, such as scalability, consistency, reliability, efficiency, and maintainability. In addition, we have an overwhelming variety of tools, including relational databases, NoSQL datastores, stream or batch processors, and message brokers. What are the right choices for your application? How do you make sense of all these buzzwords? In this practical and comprehensive guide, author Martin Kleppmann helps you navigate this diverse landscape by examining the pros and cons of various technologies for processing and storing data. Software keeps changing, but the fundamental principles remain the same. With this book, software engineers and architects will learn how to apply those ideas in practice, and how to make full use of data in modern applications. Peer under the hood of the systems you already use, and learn how to use and operate them more effectively Make informed decisions by identifying the strengths and weaknesses of different tools Navigate the trade-offs around consistency, scalability, fault tolerance, and complexity Understand the distributed systems research upon which modern databases are built Peek behind the scenes of major online services, and learn from their architectures

Windows Security Monitoring Andrei Miroshnikov 2018-03-13 Dig deep into the Windows auditing subsystem to monitor for malicious activities and enhance Windows system security Written by a former Microsoft security program manager, DEFCON "Forensics CTF" village author and organizer, and CISSP, this book digs deep into the Windows security auditing subsystem to help you understand the operating system's event logging patterns for operations and changes performed within the system. Expert guidance brings you up to speed on Windows auditing, logging, and event systems to help you exploit the full capabilities of these powerful components. Scenario–based instruction provides clear illustration of how these events unfold in the real world. From security monitoring and event patterns to deep technical details about the Windows auditing subsystem and components, this book provides detailed information on security events generated by the operating system for many common operations such as user account authentication, Active Directory object modifications, local security policy changes, and other activities. This book is based on the author's experience and the results of his research into Microsoft Windows security monitoring and anomaly detection. It presents the most common scenarios people should be aware of to check for any potentially suspicious activity. Learn to: Implement the Security Logging and Monitoring policy Dig into the Windows security auditing subsystem Understand the most common monitoring event patterns related to operations and changes in the Microsoft Windows operating system About the Author Andrei Miroshnikov is a former security program manager with Microsoft. He is an organizer and author for the DEFCON security conference "Forensics CTF" village and has been a speaker at Microsoft's Bluehat security conference. In addition, Andrei is an author of the "Windows 10 and Windows Server 2016 Security Auditing and Monitoring Reference" and multiple internal Microsoft security training documents. Among his many professional qualifications, he has earned the (ISC)2 CISSP and Microsoft MCSE: Security certifications.

Cloud Computing For Dummies Judith S. Hurwitz 2010-01-19 The easy way to understand and implement cloud computing technology written by a team of experts Cloud computing can be difficult to understand at first, but the cost-saving possibilities are great and many companies are getting on board. If you've been put in charge of implementing cloud computing, this straightforward, plain-English guide clears up the confusion and helps you get your plan in place. You'll learn how cloud computing enables you to run a more green IT infrastructure, and access technology-enabled services from the Internet ("in the cloud") without having to understand, manage, or invest in the technology infrastructure that supports them. You'll also find out what you need to consider when implementing a plan, how to handle security issues, and more. Cloud computing is a way for businesses to take advantage of storage and virtual services through the Internet, saving money on infrastructure and support This book provides a clear definition of cloud computing from the utility computing standpoint and also addresses security concerns Offers practical guidance on delivering and managing cloud computing services effectively and efficiently Presents a proactive and pragmatic approach to implementing cloud computing in any organization Helps IT managers and staff understand the benefits and challenges of cloud computing, how to select a service, and what's involved in getting it up and running Highly experienced author team consults and gives presentations on emerging technologies Cloud Computing For Dummies gets straight to the point, providing the practical information you need to know.

Building Internet Firewalls Elizabeth D. Zwicky 2000-06-26 In the five years since the first edition of this classic book was published, Internet use has exploded. The commercial world has rushed headlong into doing business on the Web, often without integrating sound security technologies and policies into their products and methods. The security risks--and the need to protect both business and personal data--have never been greater. We've updated Building Internet Firewalls to address these newer risks. What kinds of security threats does the Internet pose? Some, like password attacks and the exploiting of known security holes, have been around since the early days of networking. And others, like the distributed denial of service attacks that crippled Yahoo, E-Bay, and other major e-commerce sites in early 2000, are in current headlines. Firewalls, critical components of today's computer networks, effectively protect a system from most Internet security threats. They keep damage on one part of the network--such as eavesdropping, a worm program, or file damage--from spreading to the rest of the network. Without firewalls, network security problems can rage out of control, dragging more and more systems down. Like the bestselling and highly respected first edition, Building Internet Firewalls, 2nd Edition, is a practical and detailed step-by-step guide to designing and installing firewalls and configuring Internet services to work with a firewall. Much expanded to include Linux and Windows coverage, the second edition describes: Firewall technologies: packet filtering, proxying, network address translation, virtual private networks Architectures such as screening routers, dual-homed hosts, screened hosts, screened subnets, perimeter networks, internal firewalls Issues involved in a variety of new Internet services and protocols through a firewall Email and News Web services and scripting languages (e.g., HTTP, Java, JavaScript, ActiveX, RealAudio, RealVideo) File transfer and sharing services such as NFS, Samba Remote access services such as Telnet, the BSD "r" commands, SSH, BackOrifice 2000 Real-time conferencing services such as ICQ and talk Naming and directory services (e.g., DNS, NetBT, the Windows Browser) Authentication and auditing services (e.g., PAM, Kerberos, RADIUS); Administrative services (e.g., syslog, SNMP, SMS, RIP and other routing protocols, and ping and other network diagnostics) Intermediary protocols (e.g., RPC, SMB, CORBA, IIOP) Database protocols (e.g., ODBC, JDBC, and protocols for Oracle, Sybase, and Microsoft SQL Server) The book's complete list of resources includes the location of many publicly available firewall construction tools.

Practical Web Penetration Testing Gus Khawaja 2018-06-22 Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing using real-life scenarios. To start with, you'll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security

threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn Learn how to use Burp Suite effectively Use Nmap, Metasploit, and more tools for network infrastructure tests Practice using all web application hacking tools for intrusion tests using Kali Linux Learn how to analyze a web application using application threat modeling Know how to conduct web intrusion tests Understand how to execute network infrastructure tests Master automation of penetration testing functions for maximum efficiency using Python Who this book is for Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.
Practical UNIX and Internet Security Simson Garfinkel 2003-02-21 When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.
Building Secure and Reliable Systems Heather Adkins 2020-03-16 Can a system be considered truly reliable if it isn't fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O’Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that’s supportive of such change. You’ll learn about secure and reliable systems through: Design strategies Recommendations for coding, testing, and debugging practices Strategies to prepare for, respond to, and recover from incidents Cultural best practices that help teams across your organization collaborate effectively
Security Strategies in Linux Platforms and Applications Jones & Bartlett Learning, LLC 2011-10-15 PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.
Security Strategies in Linux Platforms and Applications Michael Jang 2010-10-25 PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.
Android Hacker's Handbook Joshua J. Drake 2014-03-26 The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.
Privileged Attack Vectors Morey J. Haber 2017-12-08 See how privileges, passwords, vulnerabilities, and exploits can be combined as an attack vector and breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Attackers target the perimeter network, but, in recent years, have refocused their efforts on the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today’s environmental complexity means privileged credentials are needed for a multitude of different account types (from domain admin and sysadmin to workstations with admin rights), operating systems (Windows, Unix, Linux, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. There is no one silver bullet to provide the protection you need against all vectors and stages of an attack. And while some new and innovative solutions will help protect against or detect the initial

infection, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor privilege management, the techniques that hackers and insiders leverage, and the defensive measures that organizations must adopt to protect against a breach, protect against lateral movement, and improve the ability to detect hacker activity or insider threats in order to mitigate the impact. What You'll Learn Know how identities, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and auditing strategies to mitigate the threats and risk Understand a 12-step privileged access management Implementation plan Consider deployment and scope, including risk, auditing, regulations, and oversight solutions Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privileged escalation threats

Linux Server Security Michael D. Bauer 2005 Provides advice on ways to ensure network security, covering such topics as DNS, Apache web server, OpenLDAP, email encryption, Cyrus IMAP service, and FTP server.

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