

Logging And Log Management The Authoritative Guide To Dealing With Syslog Audit Logs Events Alert

Eventually, you will agreed discover a supplementary experience and finishing by spending more cash. still when? attain you allow that you require to get those every needs subsequent to having significantly cash? Why dont you try to get something basic in the beginning? Thats something that will guide you to understand even more in the region of the globe, experience, some places, with history, amusement, and a lot more?

It is your utterly own grow old to ham it up reviewing habit. in the course of guides you could enjoy now is **Logging And Log Management The Authoritative Guide To Dealing With Syslog Audit Logs Events Alert** below.

VCP-DCV Official Cert Guide - John Davis 2020-06-20

VCP-DCV Official Cert Guide, Fourth Edition helps you systematically prepare for your VCP-DCV 2019 exam by mastering all key exam objectives associated with vSphere v.6.7. Thoroughly updated for VMware's 2019 exam changes, it offers an exceptionally well-organized and efficient test-preparation system based on proven series elements and techniques. Chapter-opening Do I Know This Already? quizzes help you decide how much time you need to spend on each section, exam topic lists make referencing easy, and chapter-ending Exam Preparation Tasks help you drill on the key concepts you must know thoroughly. The companion website contains a powerful Pearson IT Certification Practice Test engine that enables you to focus on individual topic areas or take a complete, timed exam. The assessment engine tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. Leading VMware consultants, trainers, and data center experts John A. Davis, Steve Baca, and Owen Thomas share preparation hints and test-taking tips, helping you identify areas of weakness and improve conceptual knowledge and hands-on skills. Material is presented concisely, focusing on promoting understanding and retention. Coverage includes: vSphere prerequisites Storage and network infrastructure (physical and virtual) vCenter Server features Clusters and virtual machines VMware product integration High availability solutions Securing vSphere Planning and performing vSphere installations Configuring vSphere (SSO and Virtual Networking) Monitoring resources VM configuration and performance Managing networking, storage, security, clusters, resources, vCenter Server, and VMs Well regarded for its detail, assessment features, comprehensive scenarios, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time.

IBM Power Systems Performance Guide: Implementing and Optimizing - Dino Quintero 2013-05-01

This IBM® Redbooks® publication addresses performance tuning topics to help leverage the virtualization strengths of the POWER® platform to solve clients' system resource utilization challenges, and maximize system throughput and capacity. We examine the performance monitoring tools, utilities, documentation, and other resources available to help technical teams provide optimized business solutions and support for applications running on IBM POWER systems' virtualized environments. The book offers application performance examples deployed on IBM Power Systems™ utilizing performance monitoring tools to leverage the comprehensive set of POWER virtualization features: Logical Partitions (LPARs), micro-partitioning, active memory sharing, workload partitions, and more. We provide a well-defined and documented performance tuning model in a POWER system virtualized environment to help you plan a foundation for scaling, capacity, and optimization . This book targets technical professionals (technical consultants, technical support staff, IT Architects, and IT Specialists) responsible for providing solutions and support on IBM POWER systems, including performance tuning.

CISA Certified Information Systems Auditor Study Guide - David L. Cannon 2016-03-14

The ultimate CISA prep guide, with practice exams Sybex's CISA: Certified Information Systems Auditor Study Guide, Fourth Edition is the newest edition of industry-leading study guide for the Certified Information System Auditor exam, fully updated to align with the latest ISACA standards and changes in IS auditing. This new edition provides complete guidance toward all content areas, tasks, and knowledge areas of the exam and is illustrated with real-world examples. All CISA terminology has been revised to reflect the most recent interpretations,

including 73 definition and nomenclature changes. Each chapter summary highlights the most important topics on which you'll be tested, and review questions help you gauge your understanding of the material. You also get access to electronic flashcards, practice exams, and the Sybex test engine for comprehensively thorough preparation. For those who audit, control, monitor, and assess enterprise IT and business systems, the CISA certification signals knowledge, skills, experience, and credibility that delivers value to a business. This study guide gives you the advantage of detailed explanations from a real-world perspective, so you can go into the exam fully prepared. Discover how much you already know by beginning with an assessment test Understand all content, knowledge, and tasks covered by the CISA exam Get more in-depths explanation and demonstrations with an all-new training video Test your knowledge with the electronic test engine, flashcards, review questions, and more The CISA certification has been a globally accepted standard of achievement among information systems audit, control, and security professionals since 1978. If you're looking to acquire one of the top IS security credentials, CISA is the comprehensive study guide you need.

Apache Security - Ivan Ristic 2005

"The complete guide to securing your Apache web server"--Cover.

Guide to Securing Microsoft Windows XP Systems for IT

Professionals: A NIST Security Configuration Checklist - Karen Scarfone 2009-08

When an IT security configuration checklist (e.g., hardening or lockdown guide) is applied to a system in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. This guide will assist personnel responsible for the administration and security of Windows XP systems. It contains information that can be used to secure local Windows XP workstations, mobile computers, and telecommuter systems more effectively in a variety of environments, including small office, home office and managed enterprise environments. The guidance should only be applied throughout an enterprise by trained and experienced system administrators. Illustrations.

Guide to Computer Network Security - Joseph Migga Kizza 2020-06-03

This timely textbook presents a comprehensive guide to the core topics in cybersecurity, covering issues of security that extend beyond traditional computer networks to the ubiquitous mobile communications and online social networks that have become part of our daily lives. In the context of our growing dependence on an ever-changing digital ecosystem, this book stresses the importance of security awareness, whether in our homes, our businesses, or our public spaces. This fully updated new edition features new material on the security issues raised by blockchain technology, and its use in logistics, digital ledgers, payments systems, and digital contracts. Topics and features: Explores the full range of security risks and vulnerabilities in all connected digital systems Inspires debate over future developments and improvements necessary to enhance the security of personal, public, and private enterprise systems Raises thought-provoking questions regarding legislative, legal, social, technical, and ethical challenges, such as the tension between privacy and security Describes the fundamentals of traditional computer network security, and common threats to security Reviews the current landscape of tools, algorithms, and professional best practices in use to maintain security of digital systems Discusses the security issues introduced by the latest generation of network technologies, including mobile systems, cloud computing, and blockchain Presents exercises of varying levels of difficulty at the end of each chapter, and concludes with a diverse selection of practical projects Offers supplementary material for students and instructors at an associated website, including slides, additional projects, and syllabus

suggestions This important textbook/reference is an invaluable resource for students of computer science, engineering, and information management, as well as for practitioners working in data- and information-intensive industries.

Network Security Through Data Analysis - Michael S Collins 2014-02-10
Traditional intrusion detection and logfile analysis are no longer enough to protect today's complex networks. In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You'll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. It's ideal for network administrators and operational security analysts familiar with scripting. Explore network, host, and service sensors for capturing security data Store data traffic with relational databases, graph databases, Redis, and Hadoop Use SiLK, the R language, and other tools for analysis and visualization Detect unusual phenomena through Exploratory Data Analysis (EDA) Identify significant structures in networks with graph analysis Determine the traffic that's crossing service ports in a network Examine traffic volume and behavior to spot DDoS and database raids Get a step-by-step process for network mapping and inventory

CEH Certified Ethical Hacker Study Guide - Kimberly Graves 2010-06-03

Full Coverage of All Exam Objectives for the CEH Exams 312-50 and EC0-350 Thoroughly prepare for the challenging CEH Certified Ethical Hackers exam with this comprehensive study guide. The book provides full coverage of exam topics, real-world examples, and includes a CD with chapter review questions, two full-length practice exams, electronic flashcards, a glossary of key terms, and the entire book in a searchable pdf e-book. What's Inside: Covers ethics and legal issues, footprinting, scanning, enumeration, system hacking, trojans and backdoors, sniffers, denial of service, social engineering, session hijacking, hacking Web servers, Web application vulnerabilities, and more Walks you through exam topics and includes plenty of real-world scenarios to help reinforce concepts Includes a CD with an assessment test, review questions, practice exams, electronic flashcards, and the entire book in a searchable pdf

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. *The Elastic Guide to Threat Hunting* - David French 2020-02-24

Network Security Through Data Analysis - Michael Collins 2017-09-08

Traditional intrusion detection and logfile analysis are no longer enough to protect today's complex networks. In the updated second edition of this practical guide, security researcher Michael Collins shows InfoSec personnel the latest techniques and tools for collecting and analyzing network traffic datasets. You'll understand how your network is used, and what actions are necessary to harden and defend the systems within it. In three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. New chapters focus on active monitoring and traffic manipulation, insider threat detection, data mining, regression and machine learning, and other topics. You'll learn how to: Use sensors to collect network, service, host, and active domain data Work with the SiLK toolset, Python, and other tools and techniques for manipulating data you collect Detect unusual phenomena through exploratory data analysis (EDA), using visualization and mathematical techniques Analyze text data, traffic behavior, and communications mistakes Identify significant structures in your network with graph analysis Examine insider threat data and acquire threat intelligence Map your network and identify significant hosts within it Work with operations to develop defenses and analysis techniques

Network Management Fundamentals - Alexander Clemm 2007

This book provides you with an accessible overview of network management covering management not just of networks themselves but also of services running over those networks. It also explains the different technologies that are used in network management and how they relate to each other.--[book cover].

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

CCNA 200-301 Official Cert Guide, Volume 2 - Wendell Odom 2019-12-10

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. This book, combined with CCNA 200-301 Official Cert Guide, Volume 1, covers all the exam topics on the CCNA 200-301 exam. · Master Cisco CCNA 200-301 exam topics · Assess your knowledge with chapter-opening quizzes · Review key concepts with exam preparation tasks This is the eBook edition of CCNA 200-301 Official Cert Guide, Volume 2. This eBook does not include access to the Pearson Test Prep practice exams that comes with the print edition. CCNA 200-301 Official Cert Guide, Volume 2 presents you with an organized test preparation routine through the use of proven series elements and techniques. "Do I Know This Already?" quizzes open each chapter and enable you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. CCNA 200-301 Official Cert Guide, Volume 2 from Cisco Press enables you to succeed on the exam the first time and is the only self-study resource approved by Cisco. Best-selling author Wendell Odom shares 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 enable you to decide how much time you need to spend on each section · Chapter-ending Key Topic tables, which help you drill on key concepts you must know thoroughly · The powerful Pearson Test Prep Practice Test software, complete with hundreds of well-reviewed, exam-realistic questions, customization options, and detailed performance reports · A free copy of the CCNA 200-301 Network Simulator, Volume 2 Lite software, complete with meaningful lab exercises that help you hone your hands-on skills with the command-line interface for routers and switches · Links to a series of hands-on config labs developed by the author · Online interactive practice exercises that help you enhance your knowledge · More than 50 minutes of video mentoring from the author · An online interactive Flash Cards application to help you drill on Key Terms by chapter · 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, hands-on labs, and challenging review questions and exercises, this official study guide helps you master the concepts and techniques that ensure your exam success. CCNA 200-301 Official Cert Guide, Volume 2, combined with CCNA 200-301 Official Cert Guide, Volume 1, walk you through all the exam topics found in the Cisco 200-301 exam. Topics covered in Volume 2 include · IP access control lists · Security services · IP services · Network architecture · Network automation Companion Website: Companion Website: The companion website contains CCNA Network Simulator Lite software, practice exercises, 50 minutes of video training, and other study resources. See the Where Are the Companion Files on the last page of your eBook file for instructions on how to access. In addition to the wealth of content, this new edition includes a series of free hands-on exercises to help you master several real-world configuration activities. These exercises can be performed on the CCNA 200-301 Network Simulator Lite, Volume 2 software included

for free on the companion website that accompanies this book.

Mastering Network Security - Chris Brenton 2006-09-30

The Technology You Need is Out There. The Expertise You Need is in Here. Expertise is what makes hackers effective. It's what will make you effective, too, as you fight to keep them at bay. Mastering Network Security has been fully updated to reflect the latest developments in security technology, but it does much more than bring you up to date. More importantly, it gives you a comprehensive understanding of the threats to your organization's network and teaches you a systematic approach in which you make optimal use of the technologies available to you. Coverage includes: Understanding security from a topological perspective Configuring Cisco router security features Selecting and configuring a firewall Configuring Cisco's PIX firewall Configuring an intrusion detection system Providing data redundancy Configuring a Virtual Private Network Securing your wireless network Implementing authentication and encryption solutions Recognizing hacker attacks Detecting and eradicating viruses Getting up-to-date security information Locking down Windows NT/2000/XP servers Securing UNIX, Linux, and FreeBSD systems

Guide to Computer Security Log Management - Karen Kent 2007-08-01

A log is a record of the events occurring within an org's. systems & networks. Many logs within an org. contain records related to computer security (CS). These CS logs are generated by many sources, incl. CS software, such as antivirus software, firewalls, & intrusion detection & prevention systems; operating systems on servers, workstations, & networking equip.; & applications. The no., vol., & variety of CS logs have increased greatly, which has created the need for CS log mgmt. -- the process for generating, transmitting, storing, analyzing, & disposing of CS data. This report assists org's. in understanding the need for sound CS log mgmt. It provides practical, real-world guidance on developing, implementing, & maintaining effective log mgmt. practices. Illus.

Juniper SRX Series - Brad Woodberg 2013-06-07

This complete field guide, authorized by Juniper Networks, is the perfect hands-on reference for deploying, configuring, and operating Juniper's SRX Series networking device. Authors Brad Woodberg and Rob Cameron provide field-tested best practices for getting the most out of SRX deployments, based on their extensive field experience. While their earlier book, Junos Security, covered the SRX platform, this book focuses on the SRX Series devices themselves. You'll learn how to use SRX gateways to address an array of network requirements—including IP routing, intrusion detection, attack mitigation, unified threat management, and WAN acceleration. Along with case studies and troubleshooting tips, each chapter provides study questions and lots of useful illustrations. Explore SRX components, platforms, and various deployment scenarios Learn best practices for configuring SRX's core networking features Leverage SRX system services to attain the best operational state Deploy SRX in transparent mode to act as a Layer 2 bridge Configure, troubleshoot, and deploy SRX in a highly available manner Design and configure an effective security policy in your network Implement and configure network address translation (NAT) types Provide security against deep threats with AppSecure, intrusion protection services, and unified threat management tools

Database and Expert Systems Applications - Sven Hartmann 2018-08-20

This two volume set of LNCS 11029 and LNCS 11030 constitutes the refereed proceedings of the 29th International Conference on Database and Expert Systems Applications, DEXA 2018, held in Regensburg, Germany, in September 2018. The 35 revised full papers presented together with 40 short papers were carefully reviewed and selected from 160 submissions. The papers of the first volume discuss a range of topics including: Big data analytics; data integrity and privacy; decision support systems; data semantics; cloud data processing; time series data; social networks; temporal and spatial databases; and graph data and road networks. The papers of the second volume discuss a range of the following topics: Information retrieval; uncertain information; data warehouses and recommender systems; data streams; information networks and algorithms; database system architecture and performance; novel database solutions; graph querying and databases; learning; emerging applications; data mining; privacy; and text processing.

Information Security Analytics - Mark Talabis 2014-11-25

Information Security Analytics gives you insights into the practice of analytics and, more importantly, how you can utilize analytic techniques to identify trends and outliers that may not be possible to identify using

traditional security analysis techniques. Information Security Analytics dispels the myth that analytics within the information security domain is limited to just security incident and event management systems and basic network analysis. Analytic techniques can help you mine data and identify patterns and relationships in any form of security data. Using the techniques covered in this book, you will be able to gain security insights into unstructured big data of any type. The authors of Information Security Analytics bring a wealth of analytics experience to demonstrate practical, hands-on techniques through case studies and using freely-available tools that will allow you to find anomalies and outliers by combining disparate data sets. They also teach you everything you need to know about threat simulation techniques and how to use analytics as a powerful decision-making tool to assess security control and process requirements within your organization. Ultimately, you will learn how to use these simulation techniques to help predict and profile potential risks to your organization. Written by security practitioners, for security practitioners Real-world case studies and scenarios are provided for each analytics technique Learn about open-source analytics and statistical packages, tools, and applications Step-by-step guidance on how to use analytics tools and how they map to the techniques and scenarios provided Learn how to design and utilize simulations for "what-if" scenarios to simulate security events and processes Learn how to utilize big data techniques to assist in incident response and intrusion analysis

Operationalizing VMware NSX - Kevin Lees 2017-08-25

Cybersecurity Blue Team Toolkit - Nadean H. Tanner 2019-04-04

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracer, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices • Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

IBM Tivoli Workload Scheduler for Z/OS Best Practices - 2006

Data Lake for Enterprises - Tomcy John 2017-05-31

A practical guide to implementing your enterprise data lake using Lambda Architecture as the base About This Book Build a full-fledged data lake for your organization with popular big data technologies using the Lambda architecture as the base Delve into the big data technologies required to meet modern day business strategies A highly practical guide to implementing enterprise data lakes with lots of examples and real-world use-cases Who This Book Is For Java developers and architects who would like to implement a data lake for their enterprise will find this book useful. If you want to get hands-on experience with the Lambda Architecture and big data technologies by implementing a practical solution using these technologies, this book will also help you. What You Will Learn Build an enterprise-level data lake using the relevant big data technologies Understand the core of the Lambda architecture and how to apply it in an enterprise Learn the technical details around Sqoop and its

functionalities Integrate Kafka with Hadoop components to acquire enterprise data Use flume with streaming technologies for stream-based processing Understand stream-based processing with reference to Apache Spark Streaming Incorporate Hadoop components and know the advantages they provide for enterprise data lakes Build fast, streaming, and high-performance applications using Elasticsearch Make your data ingestion process consistent across various data formats with configurability Process your data to derive intelligence using machine learning algorithms In Detail The term "Data Lake" has recently emerged as a prominent term in the big data industry. Data scientists can make use of it in deriving meaningful insights that can be used by businesses to redefine or transform the way they operate. Lambda architecture is also emerging as one of the very eminent patterns in the big data landscape, as it not only helps to derive useful information from historical data but also correlates real-time data to enable business to take critical decisions. This book tries to bring these two important aspects — data lake and lambda architecture—together. This book is divided into three main sections. The first introduces you to the concept of data lakes, the importance of data lakes in enterprises, and getting you up-to-speed with the Lambda architecture. The second section delves into the principal components of building a data lake using the Lambda architecture. It introduces you to popular big data technologies such as Apache Hadoop, Spark, Sqoop, Flume, and Elasticsearch. The third section is a highly practical demonstration of putting it all together, and shows you how an enterprise data lake can be implemented, along with several real-world use-cases. It also shows you how other peripheral components can be added to the lake to make it more efficient. By the end of this book, you will be able to choose the right big data technologies using the lambda architectural patterns to build your enterprise data lake. Style and approach The book takes a pragmatic approach, showing ways to leverage big data technologies and lambda architecture to build an enterprise-level data lake.

Control Baselines for Information Systems and Organizations - National In Standards and Technology 2021-03-17

This publication provides security and privacy control baselines for the Federal Government. There are three security control baselines (one for each system impact level—low-impact, moderate-impact, and high-impact), as well as a privacy baseline that is applied to systems irrespective of impact level. In addition to the control baselines, this publication provides tailoring guidance and a set of working assumptions that help guide and inform the control selection process. Finally, this publication provides guidance on the development of overlays to facilitate control baseline customization for specific communities of interest, technologies, and environments of operation.

Managing Information Security - John R. Vacca 2013-08-21

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management solutions. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Cisco ISP Essentials - Barry Raveendran Greene 2002

A comprehensive guide to the best common practices for Internet service providers Learn the best common practices for configuring routers on the Internet from experts who helped build the Internet Gain specific advice through comprehensive coverage of all Cisco routers and current versions of Cisco IOS Software Understand the Cisco IOS tools essential to building and maintaining reliable networks Increase your knowledge of network security Learn how to prevent problems and improve performance through detailed configuration examples and diagrams Cisco IOS Software documentation is extensive and detailed and is often too hard for many Internet service providers (ISPs) who simply want to switch on and get going. Cisco ISP Essentials highlights many of the key Cisco IOS features in everyday use in the major ISP backbones of the world to help new network engineers gain understanding of the power of

Cisco IOS Software and the richness of features available specifically for them. Cisco ISP Essentials also provides a detailed technical reference for the expert ISP engineer, with descriptions of the various knobs and special features that have been specifically designed for ISPs. The configuration examples and diagrams describe many scenarios, ranging from good operational practices to network security. Finally a whole appendix is dedicated to using the best principles to cover the configuration detail of each router in a small ISP Point of Presence.

Server Time Protocol Planning Guide - Octavian Lascu 2016-04-12 Server Time Protocol (STP) is a server-wide facility that is implemented in the Licensed Internal Code (LIC) of the IBM® zEnterprise Servers (zEC12, z196 and z114), System z10TM Enterprise Class (z10 EC), System z10 Business Class (z10 BC), IBM System z9® Enterprise Class (z9 EC), System z9 Business Class (z9 BC), and zSeries® z990 and z890 servers. It provides improved time synchronization in a sysplex or non-sysplex configuration. This IBM Redbooks® publication is intended for infrastructure architects and system programmers who need to understand the IBM STP functions. Readers are expected to be generally familiar with System z® technology and terminology. This book provides planning information for Server Time Protocol functions and associated software support. For more detailed installation, operation, and recovery information, refer to the companion books Server Time Protocol Implementation Guide, SG24-7281, and Server Time Protocol Recovery Guide, SG24-7380.

iSCSI Implementation and Best Practices on IBM Storwize Storage Systems - Jonathan Burton 2017-10-26

This IBM® Redbooks® publication helps administrators and technical professionals understand Internet Small Computer System Interface (iSCSI) and how to implement it for use with IBM Storwize® storage systems. iSCSI can be used alone or with other technologies. This publication provides an overview of the iSCSI protocol and helps you understand how it is similar to and different from Fibre Channel (FC) technology. It helps you plan and design your network topology. It explains how to configure your IBM Storwize storage systems and hosts (including IBM AIX®, Linux, VMware, and Microsoft Windows hosts) to interact with it. It also provides an overview of using IBM Storwize storage systems with OpenStack. This book describes configuring iSCSI for IBM Storwize and SAN Volume Controller storage systems at Version 7.6 or later. In addition to configuration, this publication provides information about performance and troubleshooting.

IBM Security Solutions Architecture for Network, Server and Endpoint - Axel Buecker 2011-02-17

Threats come from a variety of sources. Insider threats, as well as malicious hackers, are not only difficult to detect and prevent, but many times the authors of these threats are using resources without anybody being aware that those threats are there. Threats would not be harmful if there were no vulnerabilities that could be exploited. With IT environments becoming more complex every day, the challenges to keep an eye on all potential weaknesses are skyrocketing. Smart methods to detect threats and vulnerabilities, as well as highly efficient approaches to analysis, mitigation, and remediation, become necessary to counter a growing number of attacks against networks, servers, and endpoints in every organization. In this IBM® Redbooks® publication, we examine the aspects of the holistic Threat and Vulnerability Management component in the Network, Server and Endpoint domain of the IBM Security Framework. We explain the comprehensive solution approach, identify business drivers and issues, and derive corresponding functional and technical requirements, which enables us to choose and create matching security solutions. We discuss IBM Security Solutions for Network, Server and Endpoint to effectively counter threats and attacks using a range of protection technologies and service offerings. Using two customer scenarios, we apply the solution design approach and show how to address the customer requirements by identifying the corresponding IBM service and software products.

Securing the Cloud - Vic (J.R.) Winkler 2011-04-21

Securing the Cloud is the first book that helps you secure your information while taking part in the time and cost savings of cloud computing. As companies turn to burgeoning cloud computing technology to streamline and save money, security is a fundamental concern. The cloud offers flexibility, adaptability, scalability, and in the case of security - resilience. Securing the Cloud explains how to make the move to the cloud, detailing the strengths and weaknesses of securing a company's information with different cloud approaches. It offers a clear and concise framework to secure a business' assets while making the most of this new technology. This book considers alternate

approaches for securing a piece of the cloud, such as private vs. public clouds, SaaS vs. IaaS, and loss of control and lack of trust. It discusses the cloud's impact on security roles, highlighting security as a service, data backup, and disaster recovery. It also describes the benefits of moving to the cloud - solving for limited availability of space, power, and storage. This book will appeal to network and security IT staff and management responsible for design, implementation and management of IT structures from admins to CSOs, CTOs, CIOs and CISOs. Named The 2011 Best Identity Management Book by InfoSec Reviews Provides a sturdy and stable framework to secure your piece of the cloud, considering alternate approaches such as private vs. public clouds, SaaS vs. IaaS, and loss of control and lack of trust Discusses the cloud's impact on security roles, highlighting security as a service, data backup, and disaster recovery Details the benefits of moving to the cloud-solving for limited availability of space, power, and storage

Mastering FreeBSD and OpenBSD Security - Yanek Korff 2005-03-24
FreeBSD and OpenBSD are increasingly gaining traction in educational institutions, non-profits, and corporations worldwide because they provide significant security advantages over Linux. Although a lot can be said for the robustness, clean organization, and stability of the BSD operating systems, security is one of the main reasons system administrators use these two platforms. There are plenty of books to help you get a FreeBSD or OpenBSD system off the ground, and all of them touch on security to some extent, usually dedicating a chapter to the subject. But, as security is commonly named as the key concern for today's system administrators, a single chapter on the subject can't provide the depth of information you need to keep your systems secure. FreeBSD and OpenBSD are rife with security "building blocks" that you can put to use, and Mastering FreeBSD and OpenBSD Security shows you how. Both operating systems have kernel options and filesystem features that go well beyond traditional Unix permissions and controls. This power and flexibility is valuable, but the colossal range of possibilities need to be tackled one step at a time. This book walks you through the installation of a hardened operating system, the installation and configuration of critical services, and ongoing maintenance of your FreeBSD and OpenBSD systems. Using an application-specific approach that builds on your existing knowledge, the book provides sound technical information on FreeBSD and Open-BSD security with plenty of real-world examples to help you configure and deploy a secure system. By imparting a solid technical foundation as well as practical know-how, it enables administrators to push their server's security to the next level. Even administrators in other environments--like Linux and Solaris--can find useful paradigms to emulate. Written by security professionals with two decades of operating system experience, Mastering FreeBSD and OpenBSD Security features broad and deep explanations of how how to secure your most critical systems. Where other books on BSD systems help you achieve functionality, this book will help you more thoroughly secure your deployments.

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.

Practical Linux Forensics - Bruce Nikkel 2021-10-12

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

Official Google Cloud Certified Associate Cloud Engineer Study Guide - Dan Sullivan 2019-04-01

The Only Official Google Cloud Study Guide The Official Google Cloud Certified Associate Cloud Engineer Study Guide, provides everything you need to prepare for this important exam and master the skills necessary to land that coveted Google Cloud Engineering certification. Beginning with a pre-book assessment quiz to evaluate what you know before you begin, each chapter features exam objectives and review questions, plus the online learning environment includes additional complete practice tests. Written by Dan Sullivan, a popular and experienced online course author for machine learning, big data, and Cloud topics, Official Google Cloud Certified Associate Cloud Engineer Study Guide is your ace in the hole for deploying and managing Google Cloud Services.

- Select the right Google service from the various choices based on the application to be built
- Compute with Cloud VMs and managing VMs
- Plan and deploying storage
- Network and configure access and security

Google Cloud Platform is a leading public cloud that provides its users to many of the same software, hardware, and networking infrastructure used to power Google services. Businesses, organizations, and individuals can launch servers in minutes, store petabytes of data, and implement global virtual clouds with the Google Cloud Platform. Certified Associate Cloud Engineers have demonstrated the knowledge and skills needed to deploy and operate infrastructure, services, and networks in the Google Cloud. This exam guide is designed to help you understand the Google Cloud Platform in depth so that you can meet the needs of those operating resources in the Google Cloud.

OpenStack Operations Guide - Tom Fifield 2014-04-24

Design, deploy, and maintain your own private or public Infrastructure as a Service (IaaS), using the open source OpenStack platform. In this practical guide, experienced developers and OpenStack contributors show you how to build clouds based on reference architectures, as well as how to perform daily administration tasks. Designed for horizontal scalability, OpenStack lets you build a cloud by integrating several technologies. This approach provides flexibility, but knowing which options to use can be bewildering. Once you complete this book, you'll know the right questions to ask while you organize compute, storage, and networking resources. If you already know how to manage multiple Ubuntu machines and maintain MySQL, you're ready to: Set up automated deployment and configuration Design a single-node cloud controller Use metrics to improve scalability Explore compute nodes, network design, and storage Install OpenStack packages Use an example architecture to help simplify decision-making Build a working environment to explore an IaaS cloud Manage users, projects, and quotas Tackle maintenance, debugging, and network troubleshooting Monitor, log, backup, and restore

PTFM - Tim Bryant 2021-01-16

Red teams can show flaws that exist in your network before they are compromised by malicious actors and blue teams traditionally assess current security measures and identify security flaws. The teams can provide valuable feedback to each other, but this is often overlooked, enter the purple team. The purple team allows for the integration of red team tactics and blue team security measures. The purple team field

manual is a manual for all security professionals and integrates red and blue team methodologies.

Hardening Cisco Routers - Thomas Akin 2002-02-21

As a network administrator, auditor or architect, you know the importance of securing your network and finding security solutions you can implement quickly. This succinct book departs from other security literature by focusing exclusively on ways to secure Cisco routers, rather than the entire network. The rationale is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. Hardening Cisco Routers is a reference for protecting the protectors. Included are the following topics: The importance of router security and where routers fit into an overall security plan Different router configurations for various versions of Cisco's IOS Standard ways to access a Cisco router and the security implications of each Password and privilege levels in Cisco routers Authentication, Authorization, and Accounting (AAA) control Router warning banner use (as recommended by the FBI) Unnecessary protocols and services commonly run on Cisco routers SNMP security Anti-spoofing Protocol security for RIP, OSPF, EIGRP, NTP, and BGP Logging violations Incident response Physical security Written by Thomas Akin, an experienced Certified Information Systems Security Professional (CISSP) and Certified Cisco Academic Instructor (CCAI), the book is well organized, emphasizing practicality and a hands-on approach. At the end of each chapter, Akin includes a Checklist that summarizes the hardening techniques discussed in the chapter. The Checklists help you double-check the configurations you have been instructed to make, and serve as quick references for future security procedures. Concise and to the point, Hardening Cisco Routers supplies you with all the tools necessary to turn a potential vulnerability into a strength. In an area that is otherwise poorly documented, this is the one book that will help you make your Cisco routers rock solid.

Logging and Log Management - Anton Chuvakin 2013-01

Effectively analyzing large volumes of diverse logs can pose many challenges, such as huge log-volumes, Logging and Log Management helps to simplify this necessary but complex process. Everything you need to know about system, network and security logging as well as about dealing with logs including log management and log analysis. From approaches to creating useful logs on systems and applications to log analysis, log searching and log review. Comprehensive coverage of log management including analysis, visualization, reporting and more Discover different uses for logs -- from system operations to regulatory

compliance Includes Case Studies including one on building your own Log Analysis System

Netzwerkforensik in virtuellen Umgebungen - Daniel Spiekermann 2017-10-17

Cloud-Umgebungen auf Basis virtueller Maschinen und virtueller Netzwerke gewinnen immer mehr an Bedeutung. Während diese Infrastrukturen für Kunden und Anbieter viele Vorteile bieten, verkomplizieren sich zeitgleich netzwerkforensische Untersuchungen, die durch Strafverfolgungsbehörden oder IT-Sicherheitsteams durchgeführt werden. Dieses Buch untersucht und bewertet die neu auftretenden Probleme, definiert ein angepasstes Vorgehensmodell für die Netzwerkforensik in virtuellen Umgebungen und stellt zwei Lösungen vor, die in hochdynamischen und flexiblen virtuellen Netzwerken auf Basis von Open vSwitch und OpenFlow geeignete Techniken zur Untersuchung bieten. Somit sind forensische Arbeiten zur Aufklärung von Straftaten oder IT-Sicherheitsvorfällen möglich, die bisher mit den traditionellen Techniken nicht umgesetzt werden konnten.

Security Warrior - Cyrus Peikari 2004-01-12

When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm. What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antifoensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle. Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability. Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands.