Windows Internals 7th Edition Alex Ionescu S Blog

If you ally need such a referred **windows internals 7th edition alex ionescu s blog** books that will find the money for you worth, get the very best seller from us currently from several preferred authors. If you want to humorous books, lots of novels, tale, jokes, and more fictions collections are after that launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every books collections windows internals 7th edition alex ionescu s blog that we will completely offer. It is not on the order of the costs. Its not quite what you need currently. This windows internals 7th edition alex ionescu s blog, as one of the most working sellers here will unconditionally be along with the best options to review.

Windows Internals - David A. Solomon 2009-06-17
See how the core components of the Windows operating system work behind the scenes—guided by a team of internationally renowned internals experts. Fully updated for Windows Server(R) 2008 and Windows Vista(R), this classic guide delivers key architectural insights on system design, debugging, performance, and support—along with hands-on experiments to experience Windows internal behavior firsthand. Delve inside Windows architecture and internals: Understand how the core system and management mechanisms work—from the object manager to services to the registry Explore internal system data structures using tools like the kernel debugger

Grasp the scheduler's priority and CPU placement algorithms Go inside the Windows security model to see how it authorizes access to data Understand how Windows manages physical and virtual memory Tour the Windows networking stack from top to bottom—including APIs, protocol drivers, and network adapter drivers Troubleshoot file-system access problems and system boot problems Learn how to analyze crashes

Learning Malware Analysis Monnappa K A 2018-06-29 Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject

and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

Windows Internals, Part 2 - Mark Russinovich 2020-07-06 Drill down into Windows architecture and internals, discover how core Windows components work behind the scenes, and master information you can continually apply to improve architecture, development, system administration, and support. Led by three renowned Windows internals experts, this classic guide is now fully updated for Windows 10 and 8.x. As always, it combines unparalleled insider perspectives on how Windows behaves "under the hood" with hands-on experiments that let you experience these hidden behaviors firsthand. Part 2 examines these and other key Windows 10 OS components and capabilities: Startup and shutdown The Windows Registry Windows management mechanisms WMI System mechanisms ALPC ETW Cache

Manager Windows file systems The hypervisor and virtualization UWP Activation Revised throughout, this edition also contains three entirely new chapters: Virtualization technologies Management diagnostics and tracing Caching and file system support

Bandit Algorithms - Tor Lattimore 2020-07-16

A comprehensive and rigorous introduction for graduate students and researchers, with applications in sequential decision-making problems.

Modern Authentication with Azure Active Directory for Web Applications - Vittorio Bertocci 2015-12-17

Build advanced authentication solutions for any cloud or web environment Active Directory has been transformed to reflect the cloud revolution, modern protocols, and today's newest SaaS paradigms. This is an authoritative, deep-dive guide to building Active Directory authentication solutions for these new environments. Author Vittorio Bertocci drove these technologies from initial concept to general availability, playing key roles in everything from technical design to documentation. In this book, he delivers comprehensive guidance for building complete solutions. For each app type, Bertocci presents high-level scenarios and quick implementation steps, illuminates key concepts in greater depth, and helps you refine your solution to improve performance and reliability. He helps you make sense of highly abstract architectural diagrams and nitty-gritty protocol and implementation details. This is the book for people motivated to become experts. Active Directory Program Manager Vittorio Bertocci shows you how to: Address authentication challenges in the cloud or on-premises Systematically protect apps with Azure AD and AD Federation Services Power sign-in flows with OpenID Connect, Azure AD, and AD libraries Make the most of OpenID Connect's middleware and supporting classes Work with the Azure AD representation of apps and

their relationships Provide fine-grained app access control via roles, groups, and permissions Consume and expose Web APIs protected by Azure AD Understand new authentication protocols without reading complex spec documents

Windows PowerShell Cookbook - Lee Holmes 2010-08-20

With more than 250 ready-to-use recipes, this solutions-oriented introduction to the Windows PowerShell scripting environment and language provides administrators with the tools to be productive immediately.

The Art of Memory Forensics - Michael Hale Ligh 2014-07-22

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the

incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Graphic Design School David Dabner 2013-10-24

Graphic Design School allows students to develop core competencies while understanding how these fundamentals translate into new and evolving media. With examples from magazines, websites, books, and mobile devices, the Fifth Edition provides an overview of the visual communications profession, with a new focus on the intersection of design specialties. A brand-new section on web and interactivity covers topics such as web tools, coding requirements, information architecture, web design and layout, mobile device composition, app design, CMS, designing for social media, and SEO.

PoC or GTFO - Manul Laphroaig 2017-10-31

This highly anticipated print collection gathers articles published in the much-loved International Journal of Proof-of-Concept or Get The Fuck Out. PoC||GTFO follows in the tradition of Phrack and Uninformed by publishing on the subjects of offensive security research, reverse engineering, and file format internals. Until now, the journal has only been available online or printed and distributed for free at hacker conferences worldwide. Consistent with the journal's quirky, biblical style, this book comes with all the trimmings: a leatherette cover, ribbon bookmark, bible paper, and gilt-edged pages. The book features more than 80 technical essays from numerous famous hackers, authors of classics like "Reliable Code Execution on a Tamagotchi," "ELFs are Dorky, Elves are Cool," "Burning a Phone," "Forget Not the Humble Timing Attack," and "A

Sermon on Hacker Privilege." Twenty-four full-color pages by Ange Albertini illustrate many of the clever tricks described in the text.

Microsoft Windows Internals - Mark E. Russinovich 2005

Windows Kernel Programming - Pavel Yosifovich 2019-06-07

There is nothing like the power of the kernel in Windows - but how do you write kernel drivers to take advantage of that power? This book will show you how.The book describes software kernel drivers programming for Windows. These drivers don't deal with hardware, but rather with the system itself: processes, threads, modules, registry and more. Kernel code can be used for monitoring important events, preventing some from occurring if needed. Various filters can be written that can intercept calls that a driver may be interested in.

Learn Windows Subsystem for Linux - Prateek Singh 2020-12-09

Become productive with seamless interoperability between Windows and the Linux subsystem, and understand the problems that Windows Subsystem for Linux (WSL) solves. Microsoft has pushed the boundaries of open source research with WSL and you don't want to miss this ride. You will learn keywords, definitions, new features, setup, and use cases around WSL, starting from downloading to setup to interoperability between Windows and Linux subsystems. You will understand the architecture of WSL and all the new features in WSL 2. This book includes wonderful use cases, including a dedicated chapter to how to start programming and web development on WSL, and the ability to use containerization solutions like Docker and Kubernetes. WSL is a great solution to work natively in a Linux environment from your Windows 10 machines. Modern applications demand integration of cross-platform tools, services and technologies. WSL makes life

for developers and system administrators easy because it allows Linux applications to run on Windows without worrying about installing a Linux distribution on a traditional Virtual Machine. It is remarkable product with powerful functionality – get started with it using this book today. What You'll Learn Review the workings and internals of WSL and WSL2 Run Linux-based applications natively on Windows Establish your development environment in WSL Build mixed experiences (Windows-Linux) Set up and manage WSL and supported distribution packages. Who This Book Is For Programmers, web developers and system administrators working on Windows and Linux environments who want to bridge the gap between operating systems by running a Linux as a subsystem on Windows to boost their overall productivity, performance and delivery.

Operating System Concepts, 10e Abridged Print Companion - Abraham Silberschatz 2018-01-11

The tenth edition of Operating System Concepts has been revised to keep it fresh and up-to-date with contemporary examples of how operating systems function, as well as enhanced interactive elements to improve learning and the student's experience with the material. It combines instruction on concepts with real-world applications so that students can understand the practical usage of the content. End-of-chapter problems, exercises, review questions, and programming exercises help to further reinforce important concepts. New interactive self-assessment problems are provided throughout the text to help students monitor their level of understanding and progress. A Linux virtual machine (including C and Java source code and development tools) allows students to complete programming exercises that help them engage further with the material. The Print Companion includes all of the

content found in a traditional text book, organized the way you would expect it, but without the problems.

Essential COM - Don Box 1998

Shows developers how COM operates and how to use it to create efficient and stable programs consistent with the COM philosophy, allowing disparate applications and components to work together across a variety of languages, platforms, and host machines. Original. (Advanced).

Attacking Network Protocols - James Forshaw 2018-01-02

Attacking Network Protocols is a deep dive into network protocol security from James Forshaw, one of the world's leading bug hunters. This comprehensive guide looks at networking from an attacker's perspective to help you discover, exploit, and ultimately protect vulnerabilities. You'll start with a rundown of networking basics and protocol traffic capture before moving on to static and dynamic protocol analysis, common protocol structures, cryptography, and protocol security. Then you'll turn your focus to finding and exploiting vulnerabilities, with an overview of common bug classes, fuzzing, debugging, and exhaustion attacks. Learn how to: - Capture, manipulate, and replay packets - Develop tools to dissect traffic and reverse engineer code to understand the inner workings of a network protocol - Discover and exploit vulnerabilities such as memory corruptions, authentication bypasses, and denials of service - Use capture and analysis tools like Wireshark and develop your own custom network proxies to manipulate - network traffic Attacking Network Protocols is a must-have for any penetration tester, bug hunter, or developer looking to understand and discover network vulnerabilities.

Inside Windows NT - Helen Custer 1993

Microsoft Windows NT is the foundation of the new 32-bit operating system designed to support the most powerful workstation and server

systems. The initial developer support for Windows NT has been phenomenal--developers have demonstrated more than 50 Windows NT applications only months after receiving the pre-release version of the software. This authoritative text--by a member of the Windows NT development group--is a a richly detailed technical overview of the design goals and architecture of Windows NT. (Operating Systems)

Windows via C/C++ - Christophe Nasarre 2007-11-28
Master the intricacies of application development with unmanaged C++ code—straight from the experts. Jeffrey Richter's classic book is now fully revised for Windows XP, Windows Vista, and Windows Server 2008. You get in-depth, comprehensive guidance, advanced techniques, and extensive code samples to help you program Windows–based applications. Discover how to: Architect and implement your applications for both 32-bit and 64-bit Windows Create and manipulate processes and jobs Schedule, manage, synchronize and destroy threads Perform asynchronous and synchronous device I/O operations with the I/O completion port Allocate memory using various techniques including virtual memory, memory-mapped files, and heaps Manipulate the default committed physical storage of thread stacks Build DLLs for delay-loading, API hooking, and process injection Using structured exception handling, Windows Error Recovery, and Application Restart services

Windows 10 System Programming, Part 1 - Pavel Yosifovich 2020-04-11
Delve into programming the Windows operating system through the Windows API in with C++. Use the power of the Windows API to working with processes, threads, jobs, memory, I/O and more. The book covers current Windows 10 versions, allowing you to get the most of what Windows has to offer to developers in terms of productivity, performance and scalability.

Troubleshooting Windows 7 Inside Out - Mike Halsey 2010-10-25

You're beyond the basics, so dive right into troubleshooting Windows 7 -- and really put your PC to work! This supremely organized reference describes hundreds of prevention tips, troubleshooting techniques, and recovery tools in one essential guide. It's all muscle and no fluff. Discover how the experts keep their Windows 7-based systems running smoothly -- and challenge yourself to new levels of mastery. Take control of essential Windows 7 maintenance and security features, such as the Action Center and User Account Control Master quick fixes to the most common problems using expert tips and step-by-step repair guides Implement best practices to help prevent and combat viruses, malware, and identity theft Apply advanced troubleshooting techniques by understanding how Windows 7 works Diagnose hardware problems and work safely with your PC Develop a recovery plan to restore your system and data in the event of a disaster Know when to use power utilities for advanced performance, maintenance, and diagnostics Your book -- online! Get your fully searchable online edition -- with unlimited access on the Web.

Windows NT/2000 Native API Reference - Gary Nebbett 2000

Windows NT/2000 Native API Reference is absolutely unique. Currently, documentation on WIndows NT's native APIs can only be found through access to the source code or occasionally Web sites where people have chosen to share bits of insight gained through reverse engineering. This book provides the first complete reference to the API functions native to Windows NT and covers the set of services that are offered by Windows NT to both kernel- and user-mode programs. Ideal for the intermediate and advanced level user- and kernel-mode developers of Windows systems, this books is devoted

to the NT native API and consists of documentation of the 210 routines included in the API. Also included are all the functions added in Windows 2000.

Dragons, Droids & Doom: Year One - Iulian Ionescu 2015-11-11

Wanna date a dragon? How about defend yourself in court with an orc as your lawyer? Or maybe you want to just sit in your loft and have a couple beers with your imaginary friend, or follow Merlin on his final days as he fights to stay alive. No seriously, what if your girlfriend's skin was stolen by a hag? Or if you found sheet music to a song to end the world… what would you do? Dragons, Droids & Doom: Year One is a collection of all the stories published online by Fantasy Scroll Magazine in its first year. It includes a wide range of speculative short stories from fantasy to science fiction to horror. Some stories deal with death, others will leave you laughing to death. It's all here, and it's fantastic. Take a look; you won't be disappointed.

Practical Reverse Engineering - Bruce Dang 2014-02-03

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples.

Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.

Windows 10 Inside Out (includes Current Book Service) - Ed Bott 2016-11-22 This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. Conquer today's Windows 10—from the inside out! Dive into Windows 10—and really put your Windows expertise to work. Focusing on the most powerful and innovative features of Windows 10, this supremely organized reference packs hundreds of timesaving solutions, tips, and workarounds—all fully reflecting the major Windows 10 Anniversary Update. From new Cortana and Microsoft Edge enhancements to the latest security and virtualization features, you'll discover how experts tackle today's essential tasks—and challenge yourself to new levels of mastery. Install, configure, and personalize the newest versions of Windows 10 Understand Microsoft's revamped activation and upgrade processes Discover major Microsoft Edge enhancements, including new support for extensions Use today's improved Cortana services to perform tasks, set reminders, and retrieve information Make the most of

the improved ink, voice, touch, and gesture support in Windows 10 Help secure Windows 10 in business with Windows Hello and Azure AD Deploy, use, and manage new Universal Windows Platform (UWP) apps Take advantage of new entertainment options, including Groove Music Pass subscriptions and connections to your Xbox One console Manage files in the cloud with Microsoft OneDrive and OneDrive for Business Use the improved Windows 10 Mail and Calendar apps and the new Skype app Fine-tune performance and troubleshoot crashes Master high-efficiency tools for managing Windows 10 in the enterprise Leverage advanced Hyper-V features, including Secure Boot, TPMs, nested virtualization, and containers In addition, this book is part of the Current Book Service from Microsoft Press. Books in this program will receive periodic updates to address significant software changes for 12 to 18 months following the original publication date via a free Web Edition. Learn more at https://www.microsoftpressstore.com/cbs.

Windows Vista Security - Roger A. Grimes 2007-07-02 Provides information on Windows Vista security issues and tools, covering such topics as password management, e-mail security, firewalls, browser security, data protection, network security protecting against viruses and spyware, and using encryption.

Windows 7 Inside Out, Deluxe Edition - Ed Bott 2011-07-15 Dive deeper into Windows 7—with new content and new resources on CD! The Deluxe Edition of the ultimate, in-depth reference to Windows 7 has been fully updated for SP1 and Internet Explorer 9, and features 300+ pages of additional coverage and advanced topics. It's now packed with even more timesaving solutions, troubleshooting tips, and workarounds from the experts—and includes a fully searchable eBook and other online resources. Topics include installation,

configuration, and setup; network connections and troubleshooting; remote access; managing programs; controlling user access and accounts; advanced file management; working with Internet Explorer 9; managing security features and issues; using Windows Live Essentials 2011; performance monitoring and tuning; backups and maintenance; sharing networked resources; hardware and device drivers. For customers who purchase an ebook version of this title, instructions for downloading the CD files can be found in the ebook.

Advanced Windows Debugging - Mario Hewardt 2007-10-29

The First In-Depth, Real-World, Insider's Guide to Powerful Windows Debugging For Windows developers, few tasks are more challenging than debugging--or more crucial. Reliable and realistic information about Windows debugging has always been scarce. Now, with over 15 years of experience two of Microsoft's system-level developers present a thorough and practical guide to Windows debugging ever written. Mario Hewardt and Daniel Pravat cover debugging throughout the entire application lifecycle and show how to make the most of the tools currently available--including Microsoft's powerful native debuggers and third-party solutions. To help you find real solutions fast, this book is organized around real-world debugging scenarios. Hewardt and Pravat use detailed code examples to illuminate the complex debugging challenges professional developers actually face. From core Windows operating system concepts to security, Windows® Vista™ and 64-bit debugging, they address emerging topics head-on–and nothing is ever oversimplified or glossed over!

Inside Windows Debugging - Tarik Soulami 2012-05-15

Use Windows debuggers throughout the development cycle—and build better software Rethink your use of

Windows debugging and tracing tools—and learn how to make them a key part of test-driven software development. Led by a member of the Windows Fundamentals Team at Microsoft, you'll apply expert debugging and tracing techniques—and sharpen your C++ and C# code analysis skills—through practical examples and common scenarios. Learn why experienced developers use debuggers in every step of the development process, and not just when bugs appear. Discover how to: Go behind the scenes to examine how powerful Windows debuggers work Catch bugs early in the development cycle with static and runtime analysis tools Gain practical strategies to tackle the most common code defects Apply expert tricks to handle user-mode and kernel-mode debugging tasks Implement postmortem techniques such as JIT and dump debugging Debug the concurrency and security aspects of your software Use debuggers to analyze interactions between your code and the operating system Analyze software behavior with Xperf and the Event Tracing for Windows (ETW) framework

Physics and Technology for Future Presidents - Richard A. Muller 2010-04-12

Physics for future world leaders Physics and Technology for Future Presidents contains the essential physics that students need in order to understand today's core science and technology issues, and to become the next generation of world leaders. From the physics of energy to climate change, and from spy technology to quantum computers, this is the only textbook to focus on the modern physics affecting the decisions of political leaders and CEOs and, consequently, the lives of every citizen. How practical are alternative energy sources? Can satellites really read license plates from space? What is the quantum physics behind iPods and supermarket scanners? And how much should we fear a terrorist

nuke? This lively book empowers students possessing any level of scientific background with the tools they need to make informed decisions and to argue their views persuasively with anyone—expert or otherwise. Based on Richard Muller's renowned course at Berkeley, the book explores critical physics topics: energy and power, atoms and heat, gravity and space, nuclei and radioactivity, chain reactions and atomic bombs, electricity and magnetism, waves, light, invisible light, climate change, quantum physics, and relativity. Muller engages readers through many intriguing examples, helpful facts to remember, a fun-to-read text, and an emphasis on real-world problems rather than mathematical computation. He includes chapter summaries, essay and discussion questions, Internet research topics, and handy tips for instructors to make the classroom experience more rewarding. Accessible and entertaining, Physics and Technology for Future Presidents gives students the scientific fluency they need to become well-rounded leaders in a world driven by science and technology. Leading universities that have adopted this book include: Harvard Purdue Rice University University of Chicago Sarah Lawrence College Notre Dame Wellesley Wesleyan University of Colorado Northwestern Washington University in St. Louis University of Illinois - Urbana-Champaign Fordham University of Miami George Washington University Some images inside the book are unavailable due to digital copyright restrictions.

Windows Sysinternals Administrator's Reference - Aaron Margosis 2011-06-15 Get in-depth guidance—and inside insights—for using the Windows Sysinternals tools available from Microsoft TechNet. Guided by Sysinternals creator Mark Russinovich and Windows expert Aaron Margosis, you'll drill into the features and functions of dozens of free file,

disk, process, security, and Windows management tools. And you'll learn how to apply the book's best practices to help resolve your own technical issues the way the experts do. Diagnose. Troubleshoot. Optimize. Analyze CPU spikes, memory leaks, and other system problems Get a comprehensive view of file, disk, registry, process/thread, and network activity Diagnose and troubleshoot issues with Active Directory Easily scan, disable, and remove autostart applications and components Monitor application debug output Generate trigger-based memory dumps for application troubleshooting Audit and analyze file digital signatures, permissions, and other security information Execute Sysinternals management tools on one or more remote computers Master Process Explorer, Process Monitor, and Autoruns

Beyond BIOS - Vincent Zimmer 2017-01-23

Chapter 4 - Protocols You Should Know ; EFI OS Loaders ; Device Path and Image Information of the OS Loader ; Accessing Files in the Device Path of the OS Loader ; Finding the OS Partition ; Getting the Current System Configuration ; Getting the Current Memory Map.

Windows NT Device Driver Development - Peter G. Viscarola 1999

An exhaustive technical manual outlines the Windows NT concepts related to drivers; shows how to develop the best drivers for particular applications; covers the I/O Subsystem and implementation of standard kernel mode drivers; and more. Original. (Intermediate).

Troubleshooting with the Windows Sysinternals Tools - Mark E. Russinovich 2016-10-10

Optimize Windows system reliability and performance with Sysinternals IT pros and power users consider the free Windows Sysinternals tools indispensable for diagnosing, troubleshooting, and deeply understanding the Windows platform. In this extensively updated guide, Sysinternals

creator Mark Russinovich and Windows expert Aaron Margosis help you use these powerful tools to optimize any Windows system's reliability, efficiency, performance, and security. The authors first explain Sysinternals' capabilities and help you get started fast. Next, they offer in-depth coverage of each major tool, from Process Explorer and Process Monitor to Sysinternals' security and file utilities. Then, building on this knowledge, they show the tools being used to solve real-world cases involving error messages, hangs, sluggishness, malware infections, and much more. Windows Sysinternals creator Mark Russinovich and Aaron Margosis show you how to: Use Process Explorer to display detailed process and system information Use Process Monitor to capture low-level system events, and quickly filter the output to narrow down root causes List, categorize, and manage software that starts when you start or sign in to your computer, or when you run Microsoft Office or Internet Explorer Verify digital signatures of files, of running programs, and of the modules loaded in those programs Use Autoruns, Process Explorer, Sigcheck, and Process Monitor features that can identify and clean malware infestations Inspect permissions on files, keys, services, shares, and other objects Use Sysmon to monitor security-relevant events across your network Generate memory dumps when a process meets specified criteria Execute processes remotely, and close files that were opened remotely Manage Active Directory objects and trace LDAP API calls Capture detailed data about processors, memory, and clocks Troubleshoot unbootable devices, file-in-use errors, unexplained communication, and many other problems Understand Windows core concepts that aren't well-documented elsewhere

Windows Internals - Mark E. Russinovich 2012-03-15

Delve inside Windows architecture and internals—and

see how core components work behind the scenes. Led by three renowned internals experts, this classic guide is fully updated for Windows 7 and Windows Server 2008 R2—and now presents its coverage in two volumes. As always, you get critical insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand—knowledge you can apply to improve application design, debugging, system performance, and support. In Part 1, you will: Understand how core system and management mechanisms work—including the object manager, synchronization, Wow64, Hyper-V, and the registry Examine the data structures and activities behind processes, threads, and jobs Go inside the Windows security model to see how it manages access, auditing, and authorization Explore the Windows networking stack from top to bottom—including APIs, BranchCache, protocol and NDIS drivers, and layered services Dig into internals hands-on using the kernel debugger, performance monitor, and other tools

Windows Internals, Part 1 Pavel Yosifovich 2017-05-05 The definitive guide–fully updated for Windows 10 and Windows Server 2016 Delve inside Windows architecture and internals, and see how core components work behind the scenes. Led by a team of internals experts, this classic guide has been fully updated for Windows 10 and Windows Server 2016. Whether you are a developer or an IT professional, you'll get critical, insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand–knowledge you can apply to improve application design, debugging, system performance, and support. This book will help you: · Understand the Window system architecture and its most important entities, such as processes and threads · Examine how processes manage resources and threads

scheduled for execution inside processes · Observe how Windows manages virtual and physical memory · Dig into the Windows I/O system and see how device drivers work and integrate with the rest of the system · Go inside the Windows security model to see how it manages access, auditing, and authorization, and learn about the new mechanisms in Windows 10 and Server 2016

Mastering Active Directory - Dishan Francis 2017-06-30 Become a master at managing enterprise identity infrastructure by leveraging Active Directory About This Book Manage your Active Directory services for Windows Server 2016 effectively Automate administrative tasks in Active Directory using PowerShell Manage your organization's network with ease Who This Book Is For If you are an Active Directory administrator, system administrator, or network professional who has basic knowledge of Active Directory and are looking to gain expertise in this topic, this is the book for you. What You Will Learn Explore the new features in Active Directory Domain Service 2016 Automate AD tasks with PowerShell Get to know the advanced functionalities of the schema Learn about Flexible Single Master Operation (FSMO) roles and their placement Install and migrate Active directory from older versions to Active Directory 2016 Manage Active Directory objects using different tools and techniques Manage users, groups, and devices effectively Design your OU structure in the best way Audit and monitor Active Directory Integrate Azure with Active Directory for a hybrid setup In Detail Active Directory is a centralized and standardized system that automates networked management of user data, security, and distributed resources and enables interoperation with other directories. If you are aware of Active Directory basics and want to gain expertise in it, this book is perfect for you. We will quickly go through the

architecture and fundamentals of Active Directory and then dive deep into the core components, such as forests, domains, sites, trust relationships, OU, objects, attributes, DNS, and replication. We will then move on to AD schemas, global catalogs, LDAP, RODC, RMS, certificate authorities, group policies, and security best practices, which will help you gain a better understanding of objects and components and how they can be used effectively. We will also cover AD Domain Services and Federation Services for Windows Server 2016 and all their new features. Last but not least, you will learn how to manage your identity infrastructure for a hybrid-cloud setup. All this will help you design, plan, deploy, manage operations on, and troubleshoot your enterprise identity infrastructure in a secure, effective manner. Furthermore, I will guide you through automating administrative tasks using PowerShell cmdlets. Toward the end of the book, we will cover best practices and troubleshooting techniques that can be used to improve security and performance in an identity infrastructure. Style and approach This step-by-step guide will help you master the core functionalities of Active Directory services using Microsoft Server 2016 and PowerShell, with real-world best practices at the end.

Operating Systems - William Stallings 2009

For a one-semester undergraduate course in operating systems for computer science, computer engineering, and electrical engineering majors. Winner of the 2009 Textbook Excellence Award from the Text and Academic Authors Association (TAA)! Operating Systems: Internals and Design Principles is a comprehensive and unified introduction to operating systems. By using several innovative tools, Stallings makes it possible to understand critical core concepts that can be fundamentally challenging. The new edition includes the

implementation of web based animations to aid visual learners. At key points in the book, students are directed to view an animation and then are provided with assignments to alter the animation input and analyze the results. The concepts are then enhanced and supported by end-of-chapter case studies of UNIX, Linux and Windows Vista. These provide students with a solid understanding of the key mechanisms of modern operating systems and the types of design tradeoffs and decisions involved in OS design. Because they are embedded into the text as end of chapter material, students are able to apply them right at the point of discussion. This approach is equally useful as a basic reference and as an up-to-date survey of the state of the art.

Windows Internals - Brian Catlin 2016-02-29

Delve inside Windows architecture and internals - and see how core components work behind the scenes. This classic guide has been fully updated for Windows 8.1 and Windows Server 2012 R2, and now presents its coverage in three volumes: Book 1, User Mode; Book 2, Kernel Mode; Book 3, Device Driver Models. In Book 1, you'll plumb Windows fundamentals, independent of platform - server, desktop, tablet, phone, Xbox. Coverage focuses on high-level functional descriptions of the various Windows components and features that interact with, or are manipulated by, user mode programs, or applications. You'll also examine management mechanisms and operating system components that are implemented in user mode, such as service processes. As always, you get critical insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand - knowledge you can apply to improve application design, debugging, system performance, and support. Planned chapters: Concepts & Tools; System Architecture; Windows Application Support; Windows

Store Apps; Graphics & the Desktop; Management Mechanisms; User Mode Memory Management; Security; Storage; Networking; Hyper-V.

Windows Server 2019 Inside Out - Orin Thomas 2020-05-07 Conquer Windows Server 2019—from the inside out! Dive into Windows Server 2019—and really put your Windows Serverexpertise to work. Focusing on Windows Server 2019's most powerful and innovative features, this supremely organized reference packs hundreds of timesaving solutions, tips, and workarounds—all you need to plan, implement, or manage Windows Server in enterprise, data center, cloud, and hybrid environments. Fully reflecting new innovations for security, hybrid cloud environments, and Hyper-Converged Infrastructure (HCI), it covers everything from cluster sets to Windows Subsystem for Linux. You'll discover how experts tackle today's essential tasks—and challenge yourself to new levels of mastery. • Optimize the full Windows Server 2019 lifecycle, from planning and configuration through rollout and administration • Leverage new configuration options including App Compatibility Features on Demand (FOD) or Desktop Experience • Ensure fast, reliable upgrades and migrations • Manage Windows servers, clients, and services through Windows Admin Center • Seamlessly deliver and administer core DNS, DHCP, fi le, print, storage, and Internet services • Use the Storage Migration Service to simplify storage moves and configuration at the destination • Seamlessly integrate Azure IaaS and hybrid services with Windows Server 2019 • Improve agility with advanced container technologies, including container networking and integration into Kubernetes orchestration clusters • Deliver Active Directory identity, certifi cate, federation, and rights management services • Protect servers, clients, VMs, assets, and users with advanced

Windows Server 2019 security features, from Just Enough Administration to shielded VMs and guarded virtualization fabrics • Monitor performance, manage event logs, confi gure advanced auditing, and perform backup/recovery Windows Server 2019 For Experienced Windows Server Users and IT Professionals • Your role: Experienced intermediate to-advanced level Windows Server user or IT professional • Prerequisites: Basic understanding of Windows Server procedures, techniques, and navigation

Windows Runtime via C# - Jeffrey Richter 2013-11-15

Delve inside the Windows Runtime - and learn best ways to design and build Windows Store apps. Guided by Jeffrey Richter, a recognized expert in Windows and .NET programming, along with principal Windows consultant Maarten van de Bospoort, you'll master essential concepts. And you'll gain practical insights and tips for how to architect, design, optimize, and debug your apps. With this book, you will: Learn how to consume Windows Runtime APIs from C# Understand the principles of architecting Windows Store apps See how to build, deploy, and secure app packages Understand how apps are activated and the process model controlling their execution Study the rich features available when working with files and folders Explore how to transfer, compress, and encrypt data via streams Design apps that give the illusion of running using live tiles, background transfers, and background tasks Share data between apps using the clipboard and the Share charm Get advice for monetizing your apps through the Windows Store About This Book Requires working knowledge of Microsoft .NET Framework, C#, and the Visual Studio IDE Targeted to programmers building Windows Store apps Some chapters also useful to those building desktop apps Technologies Covered Windows 8.1 Microsoft Visual Studio 2013

Windows Internals Mark E. Russinovich 2012-09-15 Delve inside Windows architecture and internals—and see how core components work behind the scenes. Led by three renowned internals experts, this classic guide is fully updated for Windows 7 and Windows Server 2008 R2—and now presents its coverage in two volumes. As always, you get critical insider perspectives on how Windows operates. And through hands-on experiments, you'll experience its internal behavior firsthand—knowledge you can apply to improve application design, debugging, system performance, and support. In Part 2, you'll examine: Core subsystems for I/O, storage, memory management, cache manager, and file systems Startup and shutdown processes Crash-dump analysis, including troubleshooting tools and techniques