

Windowsr Internals Part 1 Covering Windows Serverr 2008 R2 And 7 Mark Russinovich

Windows Internals
Windows Sysinternals Administrator's Reference
Inside Windows Debugging
Practical Malware Analysis
Windows Administration Resource Kit
Windows Internals, Part 1
Essential COM
Mac OS X Internals
Rogue Code
Zero Day
Windows System Programming
Clustering Windows Server
Practical Reverse Engineering
Trojan Horse
Windows® Internals, Part 1
Windows NT File System Internals
Network Programming with Windows Sockets
Ten Strategies of a World-Class Cybersecurity Operations Center
The Rootkit Arsenal
Inside Windows NT
Natural Language Processing with Python
Web Scraping with Python
A Guide to Kernel Exploitation
Kerberos
Windows Security Monitoring
Windows Internals
Developing Drivers with the Windows Driver Foundation
Troubleshooting with the Windows Sysinternals Tools
Windows Internals
Windows 10 System Programming, Part 1
The Elements of Computing Systems
Windows Internals
Rootkits
Linux Device Drivers
Pro XAML with C#
Programming the Microsoft Windows Driver Model
Windows Internals, Part 1
Windows NT Shell Scripting
Professional IIS 7
Windows Internals

Windows Internals

Windows Sysinternals Administrator's Reference

A guide to rootkits describes what they are, how they work, how to build them, and how to detect them.

Inside Windows Debugging

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).

Practical Malware Analysis

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.

Windows Administration Resource Kit

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

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

Essential COM

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.

Mac OS X Internals

Start developing robust drivers with expert guidance from the teams who developed Windows Driver Foundation. This comprehensive book gets you up to speed quickly and goes beyond the fundamentals to help you extend your Windows development skills. You get best practices, technical guidance, and extensive code samples to help you master the intricacies of the next-generation driver model—and simplify driver development. Discover how to: Use the Windows Driver Foundation to develop kernel-mode or user-mode drivers Create drivers that support Plug and Play and power management—with minimal code Implement robust I/O handling code Effectively manage synchronization and concurrency in driver code Develop user-mode drivers for protocol-based and serial-bus-based devices Use USB-specific features of the frameworks to quickly develop drivers for USB devices Design and implement kernel-mode drivers for DMA devices Evaluate your drivers with source code analysis and static verification tools Apply best practices to test, debug, and install drivers PLUS—Get driver code samples on the Web

Rogue Code

"Windows NT File System Internals" examines the NT/IO Manager, the Cache Manager, and the Memory Manager from the perspective of a software developer writing a file system driver or implementing a kernel-mode filter driver. The book provides numerous code examples, as well as the source for a complete, usable filter driver.

Zero Day

An airliner's controls abruptly fail mid-flight over the Atlantic. An oil tanker runs aground in Japan when its navigational system suddenly stops dead. Hospitals everywhere have to abandon their computer databases when patients die after being administered incorrect dosages of their medicine. In the Midwest, a nuclear power plant nearly becomes the next Chernobyl when its cooling systems malfunction. At first, these random computer failures seem like unrelated events. But Jeff Aiken, a former government analyst who quit in disgust after witnessing the gross errors that led up to 9/11, thinks otherwise. Jeff fears a more serious attack targeting the United States computer infrastructure is already under way. And as other menacing computer malfunctions pop up around the world, some with deadly results, he realizes that there isn't much time if he hopes to prevent an international catastrophe. Written by a global authority on cyber security, Zero Day presents a chilling "what if" scenario that, in a world completely reliant on technology, is more than possible today---it's a cataclysmic disaster just waiting to happen.

Windows System Programming

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

Clustering Windows Server

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

Practical Reverse Engineering

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

Trojan Horse

Pro XAML with C#: Application Development Strategies is your guide to real-world development practices on Microsoft's XAML-based platforms, with examples in WPF, Windows 8.1, and Windows Phone 8.1. Learn how to properly plan and architect an application on one or more of these platforms for a robust, scalable solution. In Part I, authors Buddy James and Lori Lalonde introduce you to XAML and reveal proven techniques for developing successful line-of-business applications. You'll also find out about some of the conflicting needs and interests that you might encounter as an enterprise XAML developer. Part II begins to lay the groundwork to help you properly architect your application, providing you with a deeper understanding of domain-driven design and the Model-View-ViewModel design pattern. You will also learn about proper exception handling and logging techniques, and how to cover your code with unit tests to reduce bugs and validate your design. Part III explores implementation and deployment details for each of Microsoft's XAML UIs, along with advice on deploying and maintaining your application across different devices using version control repositories and continuous integration. Pro XAML with C#: Application Development Strategies is for intermediate to experienced developers looking to improve their professional practice. Readers should have experience working with C# and at least one XAML-based technology (WPF, Silverlight, Windows Store, or Windows Phone).

Windows® Internals, Part 1

Introduces tools and techniques for analyzing and debugging malicious software, discussing how to set up a safe virtual environment, overcome malware tricks, and use five of the most popular packers.

Windows NT File System Internals

It's two years after the Zero Day attacks, and cyber-security analyst Jeff Aiken is reaping the rewards for crippling Al-Qaida's assault on the computer infrastructure of the Western world. His company is flourishing, and his relationship with former government agent Daryl Haugen has intensified since she became a part of his team. But the West is under its greatest threat yet. A revolutionary, invisible trojan that alters data without leaving a trace---more sophisticated than any virus seen before---has been identified, roiling international politics. Jeff and Daryl are summoned to root it out and discover its source. As the trojan penetrates Western intelligence, and the terrifying truth about its creator is revealed, Jeff and Daryl find themselves in a desperate race to reverse it as the fate of both East and West hangs in the balance. A thrilling suspense story and a sober warning from one of the world's leading experts on cyber-security, Trojan Horse exposes the already widespread use of international cyber-espionage as a powerful and dangerous weapon, and the lengths to which one man will go to stop it.

Network Programming with Windows Sockets

As the first update to Microsoft's server operating system in nearly five years, Windows Server 2008 boasts the new Internet Information Services 7.0 (IIS 7), which is the largest departure from previous versions of IIS ever. Written by an author team that includes four Microsoft MVPs, this book shows you how to take advantage of these exciting new features of IIS 7. With a clear understanding of IIS 7, you'll learn to deploy, install, monitor, manage, and secure an IIS environment with confidence and ease. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file.

Ten Strategies of a World-Class Cybersecurity Operations Center

Investigating a possible breach in the New York Stock Exchange, cyber security expert Jeff Aiken discovers that high-ranking officials both knew about the breach and allowed millions to be stolen, a finding that causes Jeff to be violently targeted by powerful enemies who would upend the U.S. economy. 40,000 first printing.

The Rootkit Arsenal

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

Inside Windows NT

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.

Natural Language Processing with Python

A guide to the architecture and internal structure of Microsoft Windows 7 and Microsoft Windows server 2008 R2.

Web Scraping with Python

Analyzing how hacks are done, so as to stop them in the future Reverse engineering is the process of analyzing hardware or software and understanding it, without having access to the source code or design documents. Hackers are able to reverse engineer systems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. Practical Reverse Engineering goes under the hood of reverse engineering for security analysts, security engineers, and system programmers, so they can learn how to use these same processes to stop hackers in their tracks. The book covers x86, x64, and ARM (the first book to cover all three); Windows kernel-mode code rootkits and drivers; virtual machine protection techniques; and much more. Best of all, it offers a systematic approach to the material, with

plenty of hands-on exercises and real-world examples. Offers a systematic approach to understanding reverse engineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architectures as well as deobfuscation and virtual machine protection techniques Provides special coverage of Windows kernel-mode code (rootkits/drivers), a topic not often covered elsewhere, and explains 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, Windows Kernel, and Reversing Tools provides crucial, up-to-date guidance for a broad range of IT professionals.

A Guide to Kernel Exploitation

The Definitive Guide to Windows API Programming, Fully Updated for Windows 7, Windows Server 2008, and Windows Vista Windows System Programming, Fourth Edition, now contains extensive new coverage of 64-bit programming, parallelism, multicore systems, and many other crucial topics. Johnson Hart's robust code examples have been updated and streamlined throughout. They have been debugged and tested in both 32-bit and 64-bit versions, on single and multiprocessor systems, and under Windows 7, Vista, Server 2008, and Windows XP. To clarify program operation, sample programs are now illustrated with dozens of screenshots. Hart systematically covers Windows externals at the API level, presenting practical coverage of all the services Windows programmers need, and emphasizing how Windows functions actually behave and interact in real-world applications. Hart begins with features used in single-process applications and gradually progresses to more sophisticated functions and multithreaded environments. Topics covered include file systems, memory management, exceptions, processes, threads, synchronization, interprocess communication, Windows services, and security. New coverage in this edition includes Leveraging parallelism and maximizing performance in multicore systems Promoting source code portability and application interoperability across Windows, Linux, and UNIX Using 64-bit address spaces and ensuring 64-bit/32-bit portability Improving performance and scalability using threads, thread pools, and completion ports Techniques to improve program reliability and performance in all systems Windows performance-enhancing API features available starting with Windows Vista, such as slim reader/writer locks and condition variables A companion Web site, jmhartsoftware.com, contains all sample code, Visual Studio projects, additional examples, errata, reader comments, and Windows commentary and discussion.

Kerberos

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 Windows 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

Windows Security Monitoring

A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerability—a bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold. Covers a range of operating system families — UNIX derivatives, Mac OS X, Windows Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions Delivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks

Windows Internals

An IT decision-maker's road map to creating scalable and reliable Windows 2000 clustered systems. Clustering Windows 2000 explains what a cluster is and what it is not. It explains the concepts and technology from the perspective of Microsoft's Windows family of operating systems. Mauler and Beebe thoroughly explore the critical interaction and integration of state-of-the-art computer hardware with these operating systems and also with third-party layered solutions. However, more than teaching technology, the book provides a unique framework by which readers can evaluate their

organizations' own clustering needs. The new Cluster Configuration MatrixC presented here allows them to determine the utility of the many clustering products and solutions given their companies' specific requirements for high availability. Clustering Windows 2000 enables IT professionals to create a highly effective clustering strategy that can grow with their organizations' needs and accommodate ongoing developments in clustering technology. This unique book is for everyone from system designers to IT managers who want a solid understanding of the optimal products and technologies they can use in creating "clusters" of computers to support truly enterprise-caliber programs. Demystifies Windows clustering from both a hardware and software viewpointDefines clustering terminology and concepts from a vendor-neutral perspectiveProvides a matrix for evaluating the multitude of cluster technology offerings

Developing Drivers with the Windows Driver Foundation

Learn web scraping and crawling techniques to access unlimited data from any web source in any format. With this practical guide, you'll learn how to use Python scripts and web APIs to gather and process data from thousands—or even millions—of web pages at once. Ideal for programmers, security professionals, and web administrators familiar with Python, this book not only teaches basic web scraping mechanics, but also delves into more advanced topics, such as analyzing raw data or using scrapers for frontend website testing. Code samples are available to help you understand the concepts in practice. Learn how to parse complicated HTML pages Traverse multiple pages and sites Get a general overview of APIs and how they work Learn several methods for storing the data you scrape Download, read, and extract data from documents Use tools and techniques to clean badly formatted data Read and write natural languages Crawl through forms and logins Understand how to scrape JavaScript Learn image processing and text recognition

Troubleshooting with the Windows Sysinternals Tools

Mac OS X was released in March 2001, but many components, such as Mach and BSD, are considerably older. Understanding the design, implementation, and workings of Mac OS X requires examination of several technologies that differ in their age, origins, philosophies, and roles. Mac OS X Internals: A Systems Approach is the first book that dissects the internals of the system, presenting a detailed picture that grows incrementally as you read. For example, you will learn the roles of the firmware, the bootloader, the Mach and BSD kernel components (including the process, virtual memory, IPC, and file system layers), the object-oriented I/O Kit driver framework, user libraries, and other core pieces of software. You will learn how these pieces connect and work internally, where they originated, and how they evolved. The book also covers several key areas of the Intel-based Macintosh computers. A solid understanding of system internals is immensely useful in design, development, and debugging for programmers of various skill levels. System programmers can use the book as a reference and to construct a better picture of how the core system works. Application programmers can gain a deeper

understanding of how their applications interact with the system. System administrators and power users can use the book to harness the power of the rich environment offered by Mac OS X. Finally, members of the Windows, Linux, BSD, and other Unix communities will find the book valuable in comparing and contrasting Mac OS X with their respective systems. Mac OS X Internals focuses on the technical aspects of OS X and is so full of extremely useful information and programming examples that it will definitely become a mandatory tool for every Mac OS X programmer.

Windows Internals

Complete information for developers designing network programs using the Windows Sockets standard. This book's easy-to-understand explanations and sample programs simplify working with the Windows Sockets API. Expert Patrice Bonner presents methods and tools for designing robust network applications, including sample stream and datagram client and server applications.

Windows 10 System Programming, Part 1

Kerberos, the single sign-on authentication system originally developed at MIT, deserves its name. It's a faithful watchdog that keeps intruders out of your networks. But it has been equally fierce to system administrators, for whom the complexity of Kerberos is legendary. Single sign-on is the holy grail of network administration, and Kerberos is the only game in town. Microsoft, by integrating Kerberos into Active Directory in Windows 2000 and 2003, has extended the reach of Kerberos to all networks large or small. Kerberos makes your network more secure and more convenient for users by providing a single authentication system that works across the entire network. One username; one password; one login is all you need. Fortunately, help for administrators is on the way. Kerberos: The Definitive Guide shows you how to implement Kerberos for secure authentication. In addition to covering the basic principles behind cryptographic authentication, it covers everything from basic installation to advanced topics like cross-realm authentication, defending against attacks on Kerberos, and troubleshooting. In addition to covering Microsoft's Active Directory implementation, Kerberos: The Definitive Guide covers both major implementations of Kerberos for Unix and Linux: MIT and Heimdal. It shows you how to set up Mac OS X as a Kerberos client. The book also covers both versions of the Kerberos protocol that are still in use: Kerberos 4 (now obsolete) and Kerberos 5, paying special attention to the integration between the different protocols, and between Unix and Windows implementations. If you've been avoiding Kerberos because it's confusing and poorly documented, it's time to get on board! This book shows you how to put Kerberos authentication to work on your Windows and Unix systems.

The Elements of Computing Systems

While forensic analysis has proven to be a valuable investigative tool in the field of computer security, utilizing anti-forensic technology makes it possible to maintain a covert operational foothold for extended periods, even in a high-security environment. Adopting an approach that favors full disclosure, the updated Second Edition of The Rootkit Arsenal presents the most accessible, timely, and complete coverage of forensic countermeasures. This book covers more topics, in greater depth, than any other currently available. In doing so the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented. The range of topics presented includes how to:

- Evade post-mortem analysis
- Frustrate attempts to reverse engineer your command & control modules
- Defeat live incident response
- Undermine the process of memory analysis
- Modify subsystem internals to feed misinformation to the outside
- Entrench your code in fortified regions of execution
- Design and implement covert channels
- Unearth new avenues of attack

Windows Internals

This title gives students an integrated and rigorous picture of applied computer science, as it comes to play in the construction of a simple yet powerful computer system.

Rootkits

Dig deep into the Windows auditing subsystem to monitor for malicious activities and enhance Windows system security. Written by a former Microsoft security program manager, DEFCON "Forensics CTF" village author and organizer, and CISSP, this book digs deep into the Windows security auditing subsystem to help you understand the operating system's event logging patterns for operations and changes performed within the system. Expert guidance brings you up to speed on Windows auditing, logging, and event systems to help you exploit the full capabilities of these powerful components. Scenario-based instruction provides clear illustration of how these events unfold in the real world. From security monitoring and event patterns to deep technical details about the Windows auditing subsystem and components, this book provides detailed information on security events generated by the operating system for many common operations such as user account authentication, Active Directory object modifications, local security policy changes, and other activities. This book is based on the author's experience and the results of his research into Microsoft Windows security monitoring and anomaly detection. It presents the most common scenarios people should be aware of to check for any potentially suspicious activity. Learn to: Implement the Security Logging and Monitoring policy Dig into the Windows security auditing subsystem Understand the most common monitoring event patterns related to operations and changes in the Microsoft Windows operating system

About the Author Andrei Miroshnikov is a former security program manager with Microsoft. He is an organizer and author for the DEFCON security conference "Forensics CTF" village and has been a speaker at Microsoft's

Bluehat security conference. In addition, Andrei is an author of the "Windows 10 and Windows Server 2016 Security Auditing and Monitoring Reference" and multiple internal Microsoft security training documents. Among his many professional qualifications, he has earned the (ISC)2 CISSP and Microsoft MCSE: Security certifications.

Linux Device Drivers

A guide to Windows administration describes how to design and implement installation and migration plans, create network connections, set up Internet services, use remote access features, and secure PCs and networks.

Pro XAML with C#

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

Programming the Microsoft Windows Driver Model

Windows NT Shell Scripting is a comprehensive reference for network professionals. It is the only book available on the practical use of the Windows NT shell scripting language. The book begins with a high-level introduction to the shell language itself, then describes the shell commands that are useful for controlling or managing different components of a network, i.e. file management, etc. The second part of the book is a comprehensive reference of all the commands, organized by function, for easy reference by the reader.

Windows Internals, Part 1

Provides information on writing a driver in Linux, covering such topics as character devices, network interfaces, driver

debugging, concurrency, and interrupts.

Windows NT Shell Scripting

This book offers a highly accessible introduction to natural language processing, the field that supports a variety of language technologies, from predictive text and email filtering to automatic summarization and translation. With it, you'll learn how to write Python programs that work with large collections of unstructured text. You'll access richly annotated datasets using a comprehensive range of linguistic data structures, and you'll understand the main algorithms for analyzing the content and structure of written communication. Packed with examples and exercises, Natural Language Processing with Python will help you: Extract information from unstructured text, either to guess the topic or identify "named entities" Analyze linguistic structure in text, including parsing and semantic analysis Access popular linguistic databases, including WordNet and treebanks Integrate techniques drawn from fields as diverse as linguistics and artificial intelligence This book will help you gain practical skills in natural language processing using the Python programming language and the Natural Language Toolkit (NLTK) open source library. If you're interested in developing web applications, analyzing multilingual news sources, or documenting endangered languages -- or if you're simply curious to have a programmer's perspective on how human language works -- you'll find Natural Language Processing with Python both fascinating and immensely useful.

Professional IIS 7

The Microsoft® Windows® driver model (WDM) supports Plug and Play, provides power management capabilities, and expands on the driver/minidriver approach. Written by long-time device-driver expert Walter Oney in cooperation with the Windows kernel team, this book provides extensive practical examples, illustrations, advice, and line-by-line analysis of code samples to clarify real-world driver-programming issues. And it's been updated with the latest details about the driver technologies in Windows XP and Windows 2000, plus more information about how to debug drivers. Topics covered include: Beginning a driver project and the structure of a WDM driver; NEW: Minidrivers and class drivers, driver taxonomy, the WDM development environment and tools, management checklist, driver selection and loading, approved API calls, and driver stacks Basic programming techniques; NEW: Safe string functions, memory limits, the Driver Verifier scheme and tags, the kernel handle flag, and the Windows 98 floating-point problem Synchronization; NEW: Details about the interrupt request level (IRQL) scheme, along with Windows 98 and Windows Me compatibility The I/O request packet (IRP) and I/O control operations; NEW: How to send control operations to other drivers, custom queue implementations, and how to handle and safely cancel IRPs Plug and Play for function drivers; NEW: Controller and multifunction devices, monitoring device removal in user mode, Human Interface Devices (HID), including joysticks and other game controllers, minidrivers for non-HID devices, and feature reports Reading and writing data, power management, and Windows Management Instrumentation

(WMI) NEW: System wakeup, the WMI control for idle detection, and using WMIMOFCK Specialized topics and distributing drivers; NEW: USB 2.0, selective suspend, Windows Hardware Quality Lab (WHQL) certification, driver selection and loading, officially approved API calls, and driver stacks COVERS WINDOWS 98, WINDOWS ME, WINDOWS 2000, AND WINDOWS XP! CD-ROM FEATURES: A fully searchable electronic copy of the book Sample code in Microsoft Visual C++® A Note Regarding the CD or DVD The print version of this book ships with a CD or DVD. For those customers purchasing one of the digital formats in which this book is available, we are pleased to offer the CD/DVD content as a free download via O'Reilly Media's Digital Distribution services. To download this content, please visit O'Reilly's web site, search for the title of this book to find its catalog page, and click on the link below the cover image (Examples, Companion Content, or Practice Files). Note that while we provide as much of the media content as we are able via free download, we are sometimes limited by licensing restrictions. Please direct any questions or concerns to booktech@oreilly.com.

Windows Internals

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

[ROMANCE](#) [ACTION & ADVENTURE](#) [MYSTERY & THRILLER](#) [BIOGRAPHIES & HISTORY](#) [CHILDREN'S](#) [YOUNG ADULT](#) [FANTASY](#)
[HISTORICAL FICTION](#) [HORROR](#) [LITERARY FICTION](#) [NON-FICTION](#) [SCIENCE FICTION](#)