OMB No. 7231976562489

Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012

Windows Debugging fundamentals WinDbg Crash Analyzer - Find Root Cause of Windows Blue Screen / Green Screen Debugging Like A Pro Windows Debugging and Troubleshooting How to Debug programs properties in Windows 7 The Debugging Book 11-3. Debugging - Locals and Autos Windows | C# Programming for Absolute Beginners BSidesSF 2018 - Introduction to Windows Kernel Mode Debugging (Yamin Tian) Windows Debugging-Access the KPRCB kernel data structure WinDbg Preview | Setup kernel debugging via fast network connection in WMware VM Vscode Windows Debugging Demo Windows Kernel Debugging Introduction Debug 2 computers simultaneously ? WinDBG remote debugging can do it ! Debug a windows service using WinDBG. Some techniques to try when attaching WinDBG Debugging JavaScript - Are you doing it wrong? How to debug a Windows Service how we write/review code in big tech companies Windows Internals - Processes Part 6 of 20 - Process related windbg commands. Breakpoint in the browser and debugging #javascript #codingshortvideo #coding Windows Kernel Debugging WinDbg

Learning Malware Analysis
Practical Foundations of Windows Debugging, Disassembling, Reversing
Advanced Windows Debugging
Debugging Windows Programs
Windows Sysinternals Administrator's Reference
Windows Debugging
Windows Server 2019 & PowerShell All-in-One For Dummies
Practical Mod_perl
Advanced Windows Memory Dump Analysis with Data Structures
Effective Debugging

Practical Reverse Engineering
Windows PowerShell Step by Step
Learning DCOM
Developing Drivers with the Windows Driver Foundation
Debugging Applications for Microsoft .NET and Microsoft Windows
Accelerated Windows Debugging 3
Advanced .NET Debugging
Practical Binary Analysis
Windows Internals
Windows Internals
Windows Runtime via C#
Gray Hat Python

Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012 ***OMB No. 7231976562489 edited by***

PORTER JAEDEN

Learning Malware Analysis

Pearson Education
Stop manually analyzing binary! Practical Binary Analysis is the first book of its kind to present advanced binary analysis topics, such as binary instrumentation, dynamic taint analysis, and symbolic execution, in an accessible way. As malware increasingly obfuscates itself and applies anti-analysis techniques to thwart our analysis, we need more sophisticated methods that allow us to raise that dark curtain designed to keep us out--binary analysis can help. The goal of all binary analysis is to determine (and possibly modify) the true properties of binary programs to understand what they really do, rather than what we think they should do. While reverse engineering and disassembly are critical first steps in many forms of binary analysis, there is much more to be learned. This hands-on guide teaches you how to tackle the fascinating but challenging topics of binary analysis and instrumentation and helps you become proficient in an area typically only mastered by a small group of expert hackers. It will take you from basic concepts to state-of-the-art methods as you dig into topics like code injection, disassembly, dynamic taint analysis, and binary instrumentation. Written for security engineers, hackers, and those with a basic working knowledge of C/C++ and x86-64, Practical Binary Analysis will teach you in-depth how binary programs work and help you acquire the tools and techniques needed to gain more control and insight into binary programs. Once you've completed an introduction to basic

binary formats, you'll learn how to analyze binaries using techniques like the GNU/Linux binary analysis toolchain, disassembly, and code injection. You'll then go on to implement profiling tools with Pin and learn how to build your own dynamic taint analysis tools with libdft and symbolic execution tools using Triton. You'll learn how to: - Parse ELF and PE binaries and build a binary loader with libbfd - Use data-flow analysis techniques like program tracing, slicing, and reaching definitions analysis to reason about runtime flow of your programs - Modify ELF binaries with techniques like parasitic code injection and hex editing - Build custom disassembly tools with Capstone - Use binary instrumentation to circumvent anti-analysis tricks commonly used by malware - Apply taint analysis to detect control hijacking and data leak attacks - Use symbolic execution to build automatic exploitation tools With exercises at the end of each chapter to help solidify your skills, you'll go from understanding basic assembly to performing some of the most sophisticated binary analysis and instrumentation. Practical Binary Analysis gives you what you need to work effectively with binary programs and transform your knowledge from basic understanding to expert-level proficiency.

Practical Foundations of Windows Debugging, Disassembling, Reversing

Pearson Education

Every software developer and IT professional understands the crucial importance of effective debugging. Often, debugging consumes most of a developer’s workday, and mastering the required techniques and skills can take a lifetime. In Effective Debugging, Diomidis Spinellis helps experienced programmers accelerate their journey to mastery, by systematically categorizing, explaining, and illustrating the most useful debugging methods, strategies, techniques, and tools. Drawing on more than thirty-five years of experience, Spinellis expands your arsenal of debugging techniques, helping you choose the best approaches for each challenge. He presents vendor-neutral, example-rich advice on general principles, high-level strategies, concrete techniques, high-efficiency tools, creative tricks, and the behavioral traits associated with effective debugging. Spinellis’s 66 expert techniques address every facet of debugging and are illustrated with step-by-step instructions and actual code. He addresses the full spectrum of problems that can arise in modern software systems, especially problems caused by complex interactions among components and services running on hosts scattered around the planet. Whether you’re debugging isolated runtime errors or catastrophic enterprise system failures, this guide will help you get the job done—more quickly, and with less pain. Key features include High-level strategies and methods for addressing diverse software failures Specific techniques to apply when programming, compiling, and running code Better ways to make the most of your debugger General-purpose skills and tools worth investing in Advanced ideas and techniques for escaping dead-ends and the maze of complexity Advice for making programs easier to debug Specialized approaches for debugging multithreaded, asynchronous, and embedded code Bug avoidance through improved software design, construction, and management

Advanced Windows Debugging No Starch Press
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

Debugging Windows Programs

"O'Reilly Media, Inc."
The full transcript of Software Diagnostics Services training with step-by-step exercises, notes, and source code to learn live local and remote debugging techniques in kernel, user process and managed .NET spaces using WinDbg debugger. The second edition was fully reworked and updated to use the latest WinDbg version and Windows 10.
Windows Sysinternals Administrator's Reference No Starch Press
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
Windows Debugging Fastprint Publishing
Your hands-on guide to Windows PowerShell scripting fundamentals Expand your expertise--and teach yourself the fundamentals of Windows PowerShell scripting, including features available in Windows PowerShell 5. If you are an IT professional, power user, or consultant, you'll get the guidance, exercises, and code you need to master core techniques for automating Windows setup,

deployment, and management. Discover how to: Run cmdlets and command-line utilities Administer Windows-based servers and desktops with built-in cmdlets Use providers to access external information Write and run scripts from the Windows ISE Create functions that are easy to maintain Build standardized environments with profiles Automate Windows systems with WMI, CIM cmdlets, and remoting Automate Active Directory Domain Services (AD DS) Debug scripts and handle errors Run commands that survive interruptions Use Desired State Configuration (DSC) to manage software services and their environments Get powerful new modules from PowerShell Gallery About You This book is for: IT professionals and power users who want to get productive with Windows PowerShell, including new features in Windows PowerShell 5 Windows system administrators who want to be more efficient and productive Anyone pursuing Windows PowerShell certifications No experience with Windows PowerShell or other scripting technologies necessary

Windows Server 2019 & PowerShell All-in-One For Dummies

Addison-Wesley Professional
Your one-stop reference for Windows Server 2019 and PowerShell know-how Windows Server 2019 & PowerShell All-in-One For Dummies offers a single reference to help you build and expand your knowledge of all things Windows Server, including the all-important PowerShell framework. Written by an information security pro and professor who trains aspiring system administrators, this book covers the broad range of topics a system administrator needs to know to run Windows Server 2019, including how to install, configure, and secure a system. This book includes coverage of: Installing & Setting Up Windows Server Configuring Windows Server 2019 Administering Windows Server 2019 Configuring Networking Managing Security Working with Windows PowerShell Installing and Administering Hyper-V Installing, Configuring, and Using Containers If you're a budding or experienced system administrator looking to build or expand your knowledge of Windows Server, this book has you covered.
Practical Mod_perl No Starch Press
"Mario Hewardt's Advanced .NET Debugging is an excellent resource for both beginner and experienced developers working with .NET. The book is also packed with many debugging tips and discussions of CLR internals, which will benefit developers architecting software." –Jeffrey Richter, consultant, trainer, and author at Wintellect "Mario has done it again. His Advanced Windows Debugging (coauthored with Daniel Pravat) is an invaluable resource for native code debugging, and Advanced .NET Debugging achieves the same quality, clarity, and breadth to make it just as invaluable for .NET debugging." –Mark Russinovich, Technical Fellow, Microsoft Corporation The Only Complete, Practical Guide to Fixing the Toughest .NET Bugs Advanced .NET Debugging is the first focused, pragmatic guide to tracking down today's most complex and challenging .NET application bugs. It is the only book to focus entirely on using powerful native debugging tools, including WinDBG, NTSD, and CDB, to debug .NET applications.

Using these tools, author Mario Hewardt explains how to identify the real root causes of problems—far more quickly than you ever could with other debuggers. Hewardt first introduces the key concepts needed to successfully use .NET's native debuggers. Next, he turns to sophisticated debugging techniques, using real-world examples that demonstrate many common C# programming errors. This book enables you to Make practical use of postmortem debugging, including PowerDBG and other "power tools" Understand the debugging details and implications of the new .NET CLR 4.0 Master and successfully use Debugging Tools for Windows, as well as SOS, SOSEX, CLR Profiler, and other powerful tools Gain a deeper, more practical understanding of CLR internals, such as examining thread-specific data, managed heap and garbage collector, interoperability layer, and .NET exceptions Solve difficult synchronization problems, managed heap problems, interoperability problems, and much more Generate and successfully analyze crash dumps A companion web site (advanceddotnetdebugging.com) contains all sample code, examples, and bonus content.

Advanced Windows Memory Dump Analysis with Data Structures

Pearson Education
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

Effective Debugging Microsoft Press
DCOM -- the Distributed Component Object Model -- is a recent upgrade of a time-honored and well-tested technology promoted by Microsoft for distributed object programming. Now that components are playing a larger and larger part in Windows 98, Windows NT 4.0, and Windows 2000, every Windows programmer will want to understand the technology. DCOM competes with CORBA as a rich and robust method for creating expandable and flexible components, allowing you to plug in new parts conveniently and upgrade without the need for code changes to every program that uses your component.This book introduces C++ programmers to DCOM and gives them the basic tools they need to write secure, maintainable programs. While using Visual C++ development tools

and wizards where appropriate, the author never leaves the results up to magic. The C++ code used to create distributed components and the communications exchanged between systems and objects are described at a level where the reader understands their significance and can use the insights for such tasks as debugging and improving performance.The first few chapters explain both the remote procedure calls that underlie DCOM's communication and the way DCOM uses C++ classes. Readers become firmly grounded in the relation between components, classes, and objects, the ways objects are created and destroyed, how clients find servers, and the basics of security and threading.After giving you a grounding in how DCOM works, this book introduces you to the Microsoft tools that make it all easy. By showing what really happens each time you choose a button in a wizard, Learning DCOM makes it possible for you to choose what you need.This book is for anyone who wants to understand DCOM. While thoroughly practical in its goals, it doesn't stint on the background you need to make your programs safe, efficient, and easy to maintain.Topics include: MIDL (Microsoft Interface Definition Language, the language for defining COM interfaces) COM error and exception handling Custom, dispatch, and dual interfaces Standard and custom factories Management of in-process versus out-of-process servers Distributed memory management Pragmatic explanation of the DCOM wire protocol Standard, custom, handler, and automation marshaling Multithreading and apartments Security at the system configuration and programming level Active Template Library (ATL), ATL wizards -- and what they don't do Writing a component that can be invoked from Visual Basic Techniques for using distributed components Creating an ActiveX control and embedding it in a Web client Authentication and the use of Windows NT security features Techniques for merging marshaling code Connection and distributed events management An introduction to COM+ features

Practical Reverse Engineering Pearson Education

This training course is a combined and reformatted version of the two previous books Windows Debugging: Practical Foundations and x64 Windows Debugging: Practical Foundations. The new format makes it easy to switch between and compare x86 and x64 versions. The book also has a larger format similar to other training courses from Software Diagnostics Services, punctuation and code highlighting improvements, the output and screenshots from the latest WinDbg 10, and consistently uses WinDbg (X86) for 32-bit examples and WinDbg (X64) for 64-bit examples. The book contains two separate sets of chapters and corresponding illustrations. They are named Chapter x86.NN and Chapter x64.NN respectively. There is some repetition of content due to the shared nature of x64 and x86 platforms. Both sets of chapters can be read independently. We included x86 chapters because many Windows applications are still 32-bit and executed in 32-bit compatibility mode on x64 Windows systems. This introductory training course can complement the more advanced course Accelerated Disassembly, Reconstruction and Reversing (ISBN: 978-1908043672).

Windows PowerShell Step by Step No Starch Press

Offers application debugging techniques for Microsoft .NET Framework and Windows, covering topics such as exception monitoring, crash handlers, and multithreaded deadlocks.

Learning DCOM Pearson Education

This book gives detailed instructions on how to use, optimize, and troubleshoot mod_perl. It shows how to get this Apache module running quickly and easily.

Developing Drivers with the Windows Driver Foundation Springer Nature

"Raymond Chen is the original raconteur of Windows." --Scott Hanselman, ComputerZen.com "Raymond has been at Microsoft for many years and has seen many nuances of Windows that others could only ever hope to get a glimpse of. With this book, Raymond shares his knowledge, experience, and anecdotal stories, allowing all of us to get a better understanding of the operating system that affects millions of people every day. This book has something for everyone, is a casual read, and I highly recommend it!" --Jeffrey Richter, Author/Consultant, Cofounder of Wintellect "Very interesting read. Raymond tells the inside story of why Windows is the way it is." --Eric Gunnerson, Program Manager, Microsoft Corporation "Absolutely essential reading for understanding the history of Windows, its intricacies and quirks, and why they came about." --Matt Pietrek, MSDN Magazine's Under the Hood Columnist "Raymond Chen has become something of a legend in the software industry, and in this book you'll discover why. From his high-level reminiscences on the design of the Windows Start button to his low-level discussions of GlobalAlloc that only your inner-geek could love, The Old New Thing is a captivating collection of anecdotes that will help you to truly appreciate the difficulty inherent in designing and writing quality software." --Stephen Toub, Technical Editor, MSDN Magazine Why does Windows work the way it does? Why is Shut Down on the Start menu? (And why is there a Start button, anyway?) How can I tap into the dialog loop? Why does the GetWindowText function behave so strangely? Why are registry files called "hives"? Many of Windows' quirks have perfectly logical explanations, rooted in history. Understand them, and you'll be more productive and a lot less frustrated. Raymond Chen--who's spent more than a decade on Microsoft's Windows development team--reveals the "hidden Windows" you need to know. Chen's engaging style, deep insight, and thoughtful humor have made him one of the world's premier technology bloggers. Here he brings together behind-the-scenes explanations, invaluable technical advice, and illuminating anecdotes that bring Windows to life--and help you make the most of it. A few of the things you'll find inside: What vending machines can teach you about effective user interfaces A deeper understanding of window and dialog management Why performance optimization can be so counterintuitive A peek at the underbelly of COM objects and the Visual C++ compiler Key details about backwards compatibility--what Windows does and why Windows program security holes most developers don't know about How to make your program a better Windows citizen

Debugging Applications for Microsoft .NET and Microsoft Windows Microsoft Press

Written by the founder of DumpAnalysis.org, this resource can help technical support and escalation engineers

and Windows software testers without the knowledge of assembly language master necessary prerequisites to understand and start debugging and crash dump analysis on X64 Windows platforms.

Accelerated Windows Debugging 3

Addison-Wesley Professional

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: –Set up a safe virtual environment to analyze malware –Quickly extract network signatures and host-based indicators –Use key analysis tools like IDA Pro, OllyDbg, and WinDbg –Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques –Use your newfound knowledge of Windows internals for malware analysis –Develop a methodology for unpacking malware and get practical experience with five of the most popular packers –Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

Advanced .NET Debugging

Microsoft Press

A reference book for technical support and escalation engineers troubleshooting and debugging complex software issues. The book is also invaluable for software maintenance and development engineers debugging Windows applications and services.

Practical Binary Analysis

"O'Reilly Media, Inc."

An Essential Reference for Intermediate and Advanced R Programmers Advanced R presents useful tools and techniques for attacking many types of R programming problems, helping you avoid mistakes and dead ends. With more than ten years of experience programming in R, the author illustrates the elegance, beauty, and flexibility at the heart of R. The book develops the necessary skills to produce quality code that can be used in a variety of circumstances. You will learn: The fundamentals of R, including standard data types and functions Functional programming as a useful framework for solving wide classes of problems The positives and negatives of metaprogramming How to write fast, memory-efficient code This book not only helps current R users become R programmers but also shows existing programmers what’s special about R.

Intermediate R programmers can dive deeper into R and learn new strategies for solving diverse problems while programmers from other languages can learn the details of R and understand why R works the way it does.
Windows Internals Pearson Education
The full transcript of Memory Dump Analysis Services Training with 10 step-by-step exercises, notes, and selected questions and answers. Learn how to navigate through memory dump space and Windows data structures to troubleshoot and debug complex software incidents. The training uses a unique and innovative pattern-driven analysis approach to speed up the learning curve. It consists of practical step-by-step exercises using WinDbg to diagnose structural and behavioural patterns in 64-bit kernel and complete (physical) memory dumps. Additional topics include memory search, kernel linked list navigation, practical WinDbg scripting, registry, system variables and objects, device drivers and I/O. Prerequisites are basic and intermediate level Windows memory dump analysis: ability to list processors, processes, threads, modules, apply symbols, walk through stack traces and raw stack data, diagnose patterns such as heap corruption, CPU spike, memory and handle leaks, access violation, stack overflow, critical section and resource wait chains and deadlocks. If you don't feel comfortable with prerequisites then Accelerated Windows Memory Dump Analysis training book is recommended before purchasing and reading this book course. Audience: Software developers, software technical support and escalation engineers, reverse and security research engineers. The 2nd edition contains updated exercises for the latest WinDbg version from Windows SDK 8.1.
Windows Internals "O'Reilly Media, Inc."
A detailed handbook for experienced developers explains how to get the most out of Microsoft's Visual Studio .NET, offering helpful guidelines on how to use its integrated develpment environment, start-up templates, and other features and tools to create a variety of applications, including Web services. Original. (Advanced)

Related with Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012:
© Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012 Self Guided Hollywood Homes Tour
© Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012 Self Guided Walking Tour Las Palmas
© Inside Windows Debugging A Practical Guide To Debugging And Tracing Strategies In Windows Author Tarik Soulami May 2012 Self Guided Lost Tour Oahu