Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang

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 good guys 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.

??????????????????????????????????????C???????????
Practical Reverse Engineeringx86, x64, ARM, Windows Kernel, Reversing Tools, and ObfuscationJohn Wiley & Sons
"?Programming Pearls??Jon??????????????????????????" -Steve McConnell??Code Complete??? ????????????????Jon Bentley??????????????????????(pearls)??Bentley?????(pearls)??Programming Pearls????????????? 14????????Bentley????????????????????????????????????(1)????????(2)????????(3)??????????????????????????????C?C++????????Web???? ????????????Bentley??????????????????????????????Bentley?????????????????????????????????????? #???? GOTOP
??????????????????.

Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises, and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In

this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode. We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for them. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for penetration testers, ethical hackers, and individuals breaking into the pentesting role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary

This book is an introduction to both offensive and defensive techniques of

cyberdeception. Unlike most books on cyberdeception, this book focuses on methods rather than detection. It treats cyberdeception techniques that are current, novel, and practical, and that go well beyond traditional honeypots. It contains features friendly for classroom use: (1) minimal use of programming details and mathematics, (2) modular chapters that can be covered in many orders, (3) exercises with each chapter, and (4) an extensive reference list.Cyberattacks have grown serious enough that understanding and using deception is essential to safe operation in cyberspace. The deception techniques covered are impersonation, delays, fakes, camouflage, false excuses, and social engineering. Special attention is devoted to cyberdeception in industrial control systems and within operating systems. This material is supported by a detailed discussion of how to plan deceptions and calculate their detectability and effectiveness. Some of the chapters provide further technical details of specific deception techniques and their application. Cyberdeception can be conducted ethically and efficiently when necessary by following a few basic principles. This book is intended for advanced undergraduate students and graduate students, as well as computer professionals learning on their own. It will be especially useful for anyone who helps run important and essential computer systems such as critical-infrastructure and military systems.

??????????????????????????, ??, ????????????????????????Linux??????????Linux?????, ?????Linux?????????.

????16?,??:“?????”?“?????”?“??????”?“???????”?“????????????”??????

The two volume set, LNCS 11735 and 11736, constitutes the proceedings of the 24th European Symposium on Research in Computer Security, ESORIC 2019, held in Luxembourg, in September 2019. The total of 67 full papers included in these proceedings was carefully reviewed and selected from 344 submissions. The papers were organized in topical sections named as follows:Part I: machine learning; information leakage; signatures and re-encryption; side channels; formal modelling and verification; attacks; secure protocols; useful tools; blockchain and smart contracts.Part II: software security; cryptographic protocols; security models; searchable encryption; privacy; key exchange protocols; and web security.

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 good guys 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.

A no-nonsense, practical guide to current and future processor and computer architectures, enabling you to design computer systems and develop better software applications across a

variety of domains Key Features Understand digital circuitry with the help of transistors, logic gates, and sequential logic Examine the architecture and instruction sets of x86, x64, ARM, and RISC-V processors Explore the architecture of modern devices such as the iPhone X and high-performance gaming PCs Book Description Are you a software developer, systems designer, or computer architecture student looking for a methodical introduction to digital device architectures but overwhelmed by their complexity? This book will help you to learn how modern computer systems work, from the lowest level of transistor switching to the macro view of collaborating multiprocessor servers. You'll gain unique insights into the internal behavior of processors that execute the code developed in high-level languages and enable you to design more efficient and scalable software systems. The book will teach you the fundamentals of computer systems including transistors, logic gates, sequential logic, and instruction operations. You will learn details of modern processor architectures and instruction sets including x86, x64, ARM, and RISC-V. You will see how to implement a RISC-V processor in a low-cost FPGA board and how to write a quantum computing program and run it on an actual quantum computer. By the end of this book, you will have a thorough understanding of modern processor and computer architectures and the future directions these architectures are likely to take. What you will learn Get to grips with transistor technology and digital circuit principles Discover the functional elements of computer processors Understand pipelining and superscalar execution Work with floating-point data formats Understand the purpose and operation of the supervisor mode Implement a complete RISC-V processor in a low-cost FPGA Explore the techniques used in virtual machine implementation Write a quantum computing program and run it on a quantum computer Who this book is for This book is for software

developers, computer engineering students, system designers, reverse engineers, and anyone looking to understand the architecture and design principles underlying modern computer systems from tiny embedded devices to warehouse-size cloud server farms. A general understanding of computer processors is helpful but not required.

??????????????Mark Russinovich?David Solomon???Windows????????????,?????????Windows??????????????????

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.

This much-anticipated revision, written by the ultimate group of top security experts in the world, features 40 percent new content on how to find security holes in any operating system or application New material addresses the many new exploitation techniques that have been discovered since the first edition, including attacking "unbreakable" software packages such as McAfee's Entercept, Mac OS X, XP, Office 2003, and Vista Also features the first-ever published information on exploiting Cisco's IOS, with content that has never before been explored The companion Web site features downloadable code files

??????????????????,??????????????,??????????????,??????????????

??????????IDEO????????,???IDEO???????????,????????????????????????????????

???????????,???????,??????????????

???????????,???????????C++???????,???????????,??????????????????????,???

???????????,????????????

???C++11????????????????????????????????????Bjarne Stroustrup?C++????????????????????????C++???????????????????????? ?The C++ Programming Language, Fourth Edition??C++??(??????????????????????)?????

?????????????Stroustrup?????????C++11?????????????????????????????C++?????
??????ISO???????????????

??C++11???????

??????? ????????????????????????? ??????????????for?????move???Unicode??
?Lambda?????????????????????????(variadic template)?????(template
alias)??????????? ??????

???????????

??????????????????(scope)?????(storage)??????
????(modularity)????????(namespace)?????????(exception handling)
?C++????(???class?class?????template)?????????????????????????????(generic
programming) ?????????(container)????????(iterator)?????(utility)???????I/O?locale??
?(numerics)? ?C++?????????????????? ???????????(???????C++98?????)????????C++1
1?????????????????????C++11???????????? #???? GOTOP Information Inc.
???????????
Künstliche Intelligenz, Digitalisierung und Algorithmen Diese Themen verändern unsere Gesellschaft. Game Hacking, die Blockchain und Monetarisierung durch KI Systeme sind

integraler Bestandteil der Computerspiele Branche, die mit ihrem Ökosystem seit Jahrzehnten Wachstum generiert und von hoher gesellschaftlicher und wirtschaftlicher Bedeutung ist. Dieser Quick Guide zeigt auf, wie Game Hacking und die damit einhergehende Entwicklung, Distribution und Vermarktung von Cheat Software funktioniert, einer Form der digitalen Produkt Piraterie und des Cybercrime. Auch die Blockchain, die nach dem Bitcoin-Hype ihr wahres Potenzial als Peer-to-Peer Distributed Ledger Technology entfaltet und mit welcher nicht nur Blockchain-Games entwickelt werden, ist verständlich erläutert und dokumentiert. Die Funktion und mögliche Bedeutung von In-Game Items als Crypto Currencies, Crypto Assets und Tokens wird hinterfragt Künstliche Intelligenz, Bestandteil einer jeden Game Engine, erfährt durch neue Monetarisierungsmodelle wie Cloud Gaming, Lootboxen und Steam Early Access neue Dimensionen, die in diesem Quick Guide verständlich erläutert sind. Finden Sie hier die wichtigsten inhaltlichen Punkte: Künstliche Intelligenz und Monetarisierung verstehen Cloud Gaming, Lootboxen und Steam Early Access erfolgreich managen In-Game Items, Crypto Assets und Tokenization wertsteigernd steuern Blockchain und Peer-to-Peer Distributed Ledger Technology anwenden Game Hacking, Cheat Software und Cybercrime abwehren Machine Learning, neuronale Netze und Cyberconsciousness sowie deren Bedeutung für die Computerspiele Branche, werden aggregiert dargelegt, die jüngsten und zukünftigen Entwicklungen aufgezeigt. Alle Themengebiete werden konsequent aus der betriebswirtschaftlichen oder Managementperspektive dargelegt und bilden einen hohen Praxisbezug. Drei Experten- Interviews vertiefen die juristischen, technologischen und betriebswirtschaftlichen Dimensionen.