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

Getting the books **Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang** now is not type of challenging means. You could not only going as soon as ebook accrual or library or borrowing from your connections to door them. This is an enormously easy means to specifically get lead by on-line. This online pronouncement Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang can be one of the options to accompany you next having supplementary time.

It will not waste your time. resign yourself to me, the e-book will definitely make public you new concern to read. Just invest little epoch to entry this on-line notice **Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang** as with ease as evaluation them wherever you are now.

Practical Foundations of ARM64 Linux Debugging, Disassembling, Reversing Dmitry Vostokov 2022-01-11 This training course is a Linux ARM64 (A64) version of the previous Practical Foundations of Linux Debugging, Disassembly, Reversing book. It also complements Accelerated Linux Core Dump Analysis training course. The book skeleton is the same as its x64 Linux predecessor, but the content was revised entirely because of a different Linux distribution and CPU architecture. The course is useful for: - Software support and escalation engineers, cloud security engineers, SRE, and DevSecOps; - Software engineers coming from JVM background; - Software testers; - Engineers coming from non-Linux environments, for example, Windows or Mac OS X; - Engineers coming from non-ARM environments, for example, x86/x64; - Linux C/C++ software engineers without assembly language background; - Security researchers without assembly language background; - Beginners learning Linux software reverse engineering techniques. This book can also be used as an ARM64 assembly language and Linux debugging supplement for relevant undergraduate-level courses.

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.

Practical Malware Analysis Michael Sikorski 2012-02-01 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.

Die unsichtbare Hand des Staates Nils Grosche 2020-10-27 W ä hrend Gestaltung immer eine Antwort auf ein Problem darstellt, k ö nnen die Probleme, auf die eine konkrete Gestaltung antwortet, verschiedenartig sein. Dies gilt auch f ü r den gestaltenden Staat, dem es bei der Auswahl seiner Mittel und Formen nicht nur um das Erzielen eines Erfolgs in der Wirklichkeit gehen muss. Nils Grosche behandelt die Begrenzungen des Rechts als denkbaren Problemmittelpunkt gestalterischen Handelns eines Tr ä gers von Hoheitsgewalt. Er wirft die Frage auf, wie die Wirklichkeit durch einen Tr ä ger von Hoheitsgewalt beeinflusst werden kann, obwohl das Recht den Zugriff eigentlich zu versperren scheint. Die spezifische, auf das Recht bezogene Art gestalterischen Handelns wird konzeptionell wie terminologisch erschlossen. Dabei zeigt der Autor Muster auf, mit deren Hilfe der gestaltende Hoheitstr ä ger die Sichtbarkeit eines offenen Normwiderspruchs vermeiden kann.

Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения 2016-03-30 Фактически представляет собой научно-практическую энциклопедию по современной кибербезопасности. Здесь анализируются предпосылки, история, методы и особенности кибер разведки и кибер контр разведки, этапы развития кибер оружия, теория и практика его применения, технологическая платформа кибераппаратные трояны), методы защиты (антивирусные программы, проактивная антивирусная защита, кибер иммунные операционные системы технической литературе приведены результаты системного авторского анализа всех известных уязвимостей в современных средствах обеспечении, криптографических алгоритмах, криптографическом оборудовании, в микросхемах, мобильных телефонах, в бортовом самолетов и даже дронов. Здесь также представлены основные концепции, национальные стандарты и методы обеспечения кибербезопасности США, Англии, Нидерландов, Канады, а также основные международные стандарты. Фактически в объеме одной книги содержатся материалы как на начинающих пользователей, специалистов среднего уровня, так и специалистов по кибербезопасности высокой компетенции полезной информации. Знания, которые вы получите из этой книги, помогут вам повысить безопасность работы в Интернете, безопасно изучить и применять в практической деятельности наиболее эффективные и опробованные на практике политики безопасности.

Hacking Jon Mark Erickson 2004

Cyber-Security Threats, Actors, and Dynamic Mitigation Nicholas Kolokotronis 2021-04-05 Cyber-Security Threats, Actors, and Dynamic Mitigation provides both a technical and state-of-the-art perspective as well as a systematic overview of the recent advances in different facets of cyber-security. It covers the methodologies for modeling attack strategies used by threat actors targeting devices, systems, and networks such as smart homes, critical infrastructures, and industrial IoT. With a comprehensive review of the threat landscape, the book explores both common and sophisticated threats to systems and networks. Tools and methodologies are presented for precise modeling of attack strategies, which can be used both proactively in risk management and reactively in intrusion prevention and response systems. Several contemporary techniques are offered ranging from reconnaissance and penetration testing to malware detection, analysis, and mitigation. Advanced machine learning-based approaches are also included in the area of anomaly-based detection, that are capable of detecting attacks relying on zero-day vulnerabilities and exploits. Academics, researchers, and professionals in cyber-security who want an in-depth look at the contemporary aspects of the field will find this book of interest. Those wanting a unique reference for various cyber-security threats and how they are detected, analyzed, and mitigated will reach for this book often.

Introduction to Cyberdeception Neil C. Rowe 2016-09-23 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.

Mastering Malware Analysis Alexey Kleymenov 2022-09-30 Learn effective malware analysis tactics to prevent your systems from getting infected Key Features Investigate cyberattacks and prevent malware-related incidents from occurring in the future Learn core concepts of static and dynamic malware analysis, memory forensics, decryption, and much more Get practical guidance in developing efficient solutions to handle malware incidents Book Description New and developing technologies inevitably bring new types of malware with them, creating a huge demand for IT professionals that can keep malware at bay. With the help of this updated second edition of Mastering Malware Analysis, you'll be able to add valuable reverse-engineering skills to your CV and learn how to protect organizations in the most efficient way. This book will familiarize you with multiple universal patterns behind different malicious software types and teach you how to analyze them using a variety of approaches. You'll learn how to examine malware code and determine the damage it can possibly cause to systems, along with ensuring that the right prevention or remediation steps are followed. As you cover all aspects of malware analysis for Windows, Linux, macOS, and mobile platforms in detail, you'll also get to grips with obfuscation, anti-debugging, and other advanced anti-reverse-engineering techniques. The skills you acquire in this cybersecurity book will help you deal with all types of modern malware, strengthen your defenses, and prevent or promptly mitigate breaches regardless of the platforms involved. By the end of this book, you will have learned how to efficiently analyze samples, investigate suspicious activity, and build innovative solutions to handle malware incidents. What you will learn Explore assembly languages to strengthen your reverse-engineering skills Master various file formats and relevant APIs used by attackers Discover attack vectors and start handling IT, OT, and IoT malware Understand how to analyze samples for x86 and

various RISC architectures Perform static and dynamic analysis of files of various types Get to grips with handling sophisticated malware cases Understand real advanced attacks, covering all their stages Focus on how to bypass anti-reverse-engineering techniques Who this book is for If you are a malware researcher, forensic analyst, IT security administrator, or anyone looking to secure against malicious software or investigate malicious code, this book is for you. This new edition is suited to all levels of knowledge, including complete beginners. Any prior exposure to programming or cybersecurity will further help to speed up your learning process.

Windows and Linux Penetration Testing from Scratch Phil Bramwell 2022-08-31 Master the art of identifying and exploiting vulnerabilities with Metasploit, Empire, PowerShell, and Python, turning Kali Linux into your fighter cockpit Key Features Map your client's attack surface with Kali Linux Discover the craft of shellcode injection and managing multiple compromises in the environment Understand both the attacker and the defender mindset Book Description Let's be honest—security testing can get repetitive. If you're ready to break out of the routine and embrace the art of penetration testing, this book will help you to distinguish yourself to your clients. This pen testing book is your guide to learning advanced techniques to attack Windows and Linux environments from the indispensable platform, Kali Linux. You'll work through core network hacking concepts and advanced exploitation techniques that leverage both technical and human factors to maximize success. You'll also explore how to leverage public resources to learn more about your target, discover potential targets, analyze them, and gain a foothold using a variety of exploitation techniques while dodging defenses like antivirus and firewalls. The book focuses on leveraging target resources, such as PowerShell, to execute powerful and difficult-to-detect attacks. Along the way, you'll enjoy reading about how these methods work so that you walk away with the necessary knowledge to explain your findings to clients from all backgrounds. Wrapping up with post-exploitation strategies, you'll be able to go deeper and keep your access. By the end of this book, you'll be well-versed in identifying vulnerabilities within your clients' environments and providing the necessary insight for proper remediation. 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 Get to grips with the exploitation of Windows and Linux clients and servers Understand advanced Windows concepts and protection and bypass them with Kali and living-off-the-land methods Get the hang of sophisticated attack frameworks such as Metasploit and Empire Become adept in generating and analyzing shellcode Build and tweak attack scripts and modules Who this book is for This book is for penetration testers, information technology professionals, cybersecurity professionals and students, and individuals breaking into a pentesting role after demonstrating advanced skills in boot camps. Prior experience with Windows, Linux, and networking is necessary.

International Joint Conference 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) 13th International Conference on EUropean Transnational Education (ICEUTE 2022) Pablo Garc í a Bringas 2022-12-09 This book of Lecture Notes in Networks and Systems contains accepted papers presented at the 15th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2022) and the 13th International Conference on EUropean Transnational Education (ICEUTE 2022). These conferences were held in the beautiful city of Salamanca, Spain, in September 2022. The aim of the CISIS 2022 conference is to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of computational intelligence, information security, and data mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event. After a thorough peer review process, the CISIS 2022 International Program Committee selected 20 papers, which are published in this conference proceedings. In this edition, three special sessions were organized: Cybersecurity in Future Connected Societies, Cybersecurity and Trusted Supply Chains of ICT, and Intelligent Solutions for Cybersecurity Systems. The aim of ICEUTE 2022 is to offer a meeting point for people working on transnational education within Europe. It provides a stimulating and fruitful forum for presenting and discussing the latest works and advances on transnational education within European countries. In the case of ICEUTE 2022, the International Program Committee selected 5 papers, which are also published in this conference proceedings. The selection of papers was extremely rigorous to maintain the high quality of the conferences. We want to thank the members of the Program Committees for their hard work during the reviewing process. This is a crucial process for creating a high-standard conference; the CISIS and ICEUTE would not exist without their help.

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.

Modern Computer Architecture and Organization Jim Ledin 2022-05-04 A no-nonsense, practical guide to current and future processor and computer architectures that enables you to design computer systems and develop better software applications across a variety of domains Key Features • Understand digital circuitry through the study of transistors, logic gates, and sequential logic • Learn the architecture of x86, x64, ARM, and RISC-V processors, iPhones, and high-performance gaming PCs • Study the design principles underlying the domains of cybersecurity, bitcoin, and self-driving cars Book Description Are you a software developer, systems designer, or computer architecture student looking for a methodical introduction to digital device architectures, but are overwhelmed by the complexity of modern systems? This step-by-step guide will teach you how modern computer systems work with the help of practical examples and exercises. You'll gain insights into the internal behavior of processors down to the circuit level and will understand how the hardware executes code developed in high-level languages. This book will teach you the fundamentals of computer systems including transistors, logic gates, sequential logic, and instruction pipelines. 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 write a quantum computing program and run it on an actual quantum computer. This edition has been updated to cover the architecture and design principles underlying the important domains of cybersecurity, blockchain and bitcoin mining, and self-driving vehicles. By the end of this book, you will have a thorough understanding of modern processors and computer architecture and the future directions these technologies are likely to take. What you will learn • Understand the fundamentals of transistor technology and digital circuits • Explore the concepts underlying pipelining and superscalar processing • Implement a complete RISC-V processor in a low-cost FPGA • Understand the technology used to implement virtual machines • Learn about security-critical computing applications like financial transaction processing • Get up to speed with blockchain and the hardware architectures used in bitcoin mining • Explore the capabilities of self-navigating vehicle computing architectures • Write a quantum computing program and run it on a real 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: ranging from tiny, embedded devices to warehouse-size cloud server farms. A general understanding of computer processors is helpful but not required.

Hands-On Penetration Testing on Windows Phil Bramwell 2018-07-30 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

Quick Guide Game Hacking, Blockchain und Monetarisierung Lutz Anderie 2020-03-25 K ü nstliche Intelligenz, Digitalisierung und Algorithmen Diese Themen ver ä ndern 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 verst ä ndlich erl ä utert und dokumentiert. Die Funktion und m ö gliche Bedeutung von In-Game Items als Crypto Currencies, Crypto Assets und Tokens wird hinterfragt K ü nstliche Intelligenz, Bestandteil einer jeden Game Engine, erf ä hrt durch neue Monetarisierungsmodelle wie Cloud Gaming, Lootboxen und Steam Early Access neue Dimensionen, die in diesem Quick Guide verst ä ndlich erl ä utert sind. Finden Sie hier die wichtigsten inhaltlichen Punkte: K ü nstliche 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 f ü r die Computerspiele Branche, werden aggregiert dargelegt, die j ü ngsten und zuk ü nftigen 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.