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

Thank you extremely much for downloading Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang.Most likely you have knowledge that, people have see numerous period for their favorite books subsequent to this Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang, but end up in harmful downloads.

Rather than enjoying a good book when a cup of coffee in the afternoon, instead they juggled next some harmful virus inside their computer. Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang is nearby in our digital library an online entry to it is set as public for that reason you can download it instantly. Our digital library saves in multipart countries, allowing you to acquire the most less latency times to download any of our books with this one. Merely said, the Practical Reverse Engineering X86 X64 Arm Windows Kernel Reversing Tools And Obfuscation Bruce Dang is universally compatible subsequently any devices to read.

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.
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.

Perfect Gentlemen - Ein One-Night-Stand ist nicht genug Lexi Blake 2016-10-14 Gabriel Bond muss nicht nur seinen besten Freund beerdigen, sondern auch das Chaos beseitigen, das dieser hinterlassen hat - darunter eine Firma, die in finanziellen Schwierigkeiten steckt. Um all dem für eine kurze Weile zu entfliehen, sucht er Vergessen in den Armen einer Fremden - die sich am nächsten Tag als eine seiner neuen Angestellten entpuppt ...

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.

Exceptional C++. Herb Sutter 2000

Die Xbox hacken. Andrew Huang 2004

Hacking Jon Erickson 2008

JavaScript

David Flanagan 2002

Schutz des "Know-how" gegen ausspähende Produktanalysen ("Reverse Engineering") Kai Kochmann 2009 Urheberrechtliche Probleme rücken seit der Einbeziehung von Computersoftware in den 1980er Jahren und der kommerziellen Nutzbarkeit des Internet in den 1990er Jahren verstärkt in den Blick von Theorie und Praxis. Die neuen technischen Nutzungsmöglichkeiten beeinflussen das nationale und das europäische Urheberrecht in seiner traditionellen, kulturbezogenen und den Schutz der schöpferischen Persönlichkeit beabsichtigenden Konzeption. Urheberrecht ist Teil des Privatrechtssystems. Vermehrt wird aber eine Indienstnahme von geistigen Schöpfungen für öffentliche Zwecke durch Zugangserleichterung und Zugangsöffnung gefordert. Wie wirkt sich diese Pflichtenbindung auf den Charakter als subjektives Privatrecht aus? Urheberrecht ist territorial beschränkt wirkendes Recht. Innerhalb der Europäischen Gemeinschaft baut man nicht nur auf eine Harmonisierung der nationalen Rechte, sondern fordert auch europaweit wirkende Befugnisse zur Nutzung, Wahrnehmung und Verwertung von Werken. Entsteht ein Europäisches Urheberecht als supranationales Urheberrecht? Urheberrecht ist Persönlichkeits- und Kulturrecht. Doch drängt der zunehmende Einfluss technischer Gegebenheiten auf eine stärkere wirtschaftsrechtliche Orientierung. Verändert das Urheberrecht dadurch seine Grundlagen? Urheberrecht ist das Recht der kreativen, auch der marktfernen Schöpfung. Die starke Zunahme verwandter Schutzrechte und die Einbeziehung technisch beeinflusster Schutzmaterien haben aber zunehmende marktbeeinflussende Wirkungen. Wird das Urheberrecht auch in seinen klassischen Bereichen damit verstärkt zum Gegenstand kartellrechtlicher Fragen? Damit sind die vier Säulen gesetzt, deren Erforschung sich die in der EurUR-Schriftenreihe veröffentlichten Werke vornehmlich widmen sollen: Urheberrecht als Privatrecht - Grundlagenforschung im Urheberrecht - Europäisierung des Rechtsgebiets - Wettbewerbsbezug urhebergesetzlich geschützter Schöpfungen und Leistungen. In der EurUR-Schriftenreihe werden Monographien, Sammelwerke und Tagungsbände publiziert, die hier ihren Schwerpunkt haben.

Expert-C-Programmierung Peter Van der Linden 1995

Die Kunst des Einbruchs Kevin Mitnick 2012-07-10 Kevin Mitnick, einst der meistgesuchte Verbrecher der USA, saß fünf Jahre im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Heute ist er rehabilitiert, gilt aber nach wie vor weltweit als Prototyp des Hackers. Seit längerer Zeit hat Mitnick in der Hackerszene nach authentischen und spannenden Geschichten gesucht, die auch für Sicherheitsverantwortliche in Firmen hoch-interessante Erkenntnisse abwerfen. Die hier vorliegende Sammlung von Geschichten ist das Ergebnis dieser Suche. „Tauchen Sie aus der Sicherheit und Geborgenheit Ihres Lesesessels ein in die feindselige Welt der Computerkriminalität. Mitnick präsentiert zehn packende Kapitel, jedes das Ergebnis eines Interviews mit einem echten Hacker, der von einem echten Angriff erzählt. Pflichtlektüre für jeden, der sich für Computersicherheit interessiert.“ Tom Parker, Computer-Sicherheitsanalytiker und Gründer der Global InterSec LLC

Objektorientierte Programmierung in Oberon-2 Hanspeter Mössenböck 2013-03-13

?????????? ??????????? ??????? 2-? ???., ????. ? ???. ??????? ? ????????? ??? ????? ????? ??????? 2022-05-13 ? ????? ???????????? ???????????? ? ??????????? ????????? ?????????? ??????????? ???????, ?????? ???????, ??????, ?????????, ?????? ? ?????????? ??????????? ????-???????????. ???????? ??????????? ?????????? ?????????????? ??????????? ??????? ? ????????? ????????? ??????? ?????????, ?????????? ???????????, ????????? ???????????, ???????????????? ?????????? ????? ?????? ?????, ???????????????? ?????????? ? ?????? ?????????????? ??????, ? ????? ??????????? ??????????? ???????. ?????? ???? ????? ???????? ?????????, ?????????? ???????, ??????, ??????? ??? ???????????????? ??????. ????????????? ??????????

?????????? ???????????? ???????????????? ???????????????? ????????? ??????? ??????????. ???? ????? ??????? ????????? ???????????? ? ???????????? ????????????? ???????????????? ???????? ????????????, ?????????? ????????????? ??????? ??????????????, ?????????????? ????? ? ?????????, ????????????-????????? ? ??????? ????-??????????.

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.

Polnisch für Dummies Daria Gabryanczyk 2020-07-21 Mit diesem Buch lernen Sie Polnisch. Neben der Betonung und der Grammatik lernen Sie Redewendungen und Begriffe, mit denen Sie Alltagssituationen meistern: sich auf Polnisch vorstellen, über Ihre Hobbys sprechen oder einen Tisch in einem Restaurant reservieren. Nebenbei lernen Sie die polnische Kultur kennen und bekommen Tipps für das Leben in Polen. Am Ende eines jeden Kapitels gibt es kleine Übungen, mit denen Sie Ihre erworbenen Sprachfähigkeiten leicht prüfen können. Dem Buch liegt eine CD mit Übungen zum Hören und Nachsprechen bei.

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.

C programmieren lernen für Dummies Dan Gookin 2017-01-05 Für dieses Buch müssen Sie kein Vorwissen mitbringen. Trotzdem werden auch fortgeschrittene C-Themen wie Zeiger und verkettete Listen behandelt - und das alles im aktuellen C11-Standard. Der besondere Clou ist die Verwendung der Programmierumgebung Code::Blocks, die es für Windows-, Mac- und Linux-Betriebssysteme gibt. Zahlreiche Beispiele, viele, viele Übungen und die Programmtexte zum Herunterladen sorgen dafür, dass Sie nach dem Durcharbeiten dieses Buchs über solide Programmiertechniken verfügen. Dann sind Sie bereit für noch mehr: eigene Projekte und das Lernen weiterer Programmiersprachen.

Hacking mit Python Justin Seitz 2009-08-24 Python wird mehr und mehr zur bevorzugten Programmiersprache von Hackern, Reverse Engineers und Softwaretestern, weil sie es einfach macht, schnell zu entwickeln. Gleichzeitig bietet Python die Low-Level-Unterstützung und die Bibliotheken, die Hacker glücklich machen. Hacking mit Python bietet eine umfassende Anleitung, wie man diese Sprache für eine Vielzahl von Hacking-Aufgaben nutzen kann. Das Buch erläutert die Konzepte hinter Hacking-Tools und -Techniken wie Debugger, Trojaner, Fuzzer und Emulatoren. Doch der Autor Justin Seitz geht über die Theorie hinaus und zeigt, wie man existierende Python-basierte Sicherheits-Tools nutzt - und wie man eigene entwickelt, wenn die vorhandenen nicht ausreichen. Sie lernen, wie man: - lästige Reverse Engineering- und Sicherheits-Aufgaben automatisiert - einen eigenen Debugger entwirft und programmiert - Windows-Treiber "fuzzed" und mächtige Fuzzer von Grund auf entwickelt - Code- und Library-Injection, Soft- und Hard-Hooks und andere Software-Tricks vornimmt - gesicherten Traffic aus einer verschlüsselten Webbrowser-Session erschnüffelt - PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU und andere Software nutzt Die weltbesten Hacker nutzen Python für ihre Arbeit. Warum nicht auch Sie?

Intensivkurs C++ - Bafög-Ausgabe Andrew Koenig 2006

Die Kunst der Täuschung Kevin D. Mitnick 2012-07-10 Mitnick führt den Leser in die Denk- und Handlungsweise des Social Engineering ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die dramatischen Konsequenzen, die sich daraus ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers als auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso die Täuschung so erfolgreich war - und wie man sich effektiv dagegen schützen kann.

Das Phantom im Netz Kevin D. Mitnick 2012

UNIX in a nutshell Arnold Robbins 2000

Y: The Last Man (Deluxe Edition) Brian K. Vaughan 2022-02-22

Praktische C++-Programmierung Steve Oualline 2004

Die Kunst der Anonymität im Internet Kevin D. Mitnick 2017-11-24 Ob Sie wollen oder nicht – jede Ihrer Online-Aktivitäten wird beobachtet und analysiert Sie haben keine Privatsphäre. Im Internet ist jeder Ihrer Klicks für Unternehmen, Regierungen und kriminelle Hacker uneingeschränkt sichtbar. Ihr Computer, Ihr Smartphone, Ihr Auto, Ihre Alarmanlage, ja sogar Ihr Kühlschrank bieten potenzielle Angriffspunkte für den Zugriff auf Ihre Daten. Niemand kennt sich besser aus mit dem Missbrauch persönlicher Daten als Kevin Mitnick. Als von der US-Regierung ehemals meistgesuchter Computer-Hacker kennt er alle Schwachstellen und Sicherheitslücken des digitalen Zeitalters. Seine Fallbeispiele sind spannend und erschreckend: Sie werden Ihre Aktivitäten im Internet neu überdenken. Mitnick weiß aber auch, wie Sie Ihre Daten bestmöglich schützen. Er zeigt Ihnen anhand zahlreicher praktischer Tipps und Schritt-für-Schritt-Anleitungen, was Sie tun können, um online und offline

anonym zu sein. Bestimmen Sie selbst über Ihre Daten. Lernen Sie, Ihre Privatsphäre im Internet zu schützen. Kevin Mitnick zeigt Ihnen, wie es geht. Hinterlassen Sie keine Spuren ? Sichere Passwörter festlegen und verwalten ? Mit dem Tor-Browser im Internet surfen, ohne Spuren zu hinterlassen ? E-Mails und Dateien verschlüsseln und vor fremden Zugriffen schützen ? Öffentliches WLAN, WhatsApp, Facebook & Co. sicher nutzen ? Sicherheitsrisiken vermeiden bei GPS, Smart-TV, Internet of Things und Heimautomation ? Eine zweite Identität anlegen und unsichtbar werden

Quick Guide Game Hacking, Blockchain und Monetarisierung Lutz Anderie 2020-03-25 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.

Mit Java programmieren lernen für Dummies Barry Burd 2015-03-31 Steigen Sie mit diesem Buch in die Welt des Programmierens ein und zwar mit der beliebten Programmiersprache Java! Schritt für Schritt werden Sie mit den Grundlagen, wie zum Beispiel Variablen, Schleifen und objektorientierter Programmierung, vertraut gemacht, probieren viele anschauliche Beispiele aus und schreiben Ihr erstes eigenes Programm. Dieses Buch steht Ihnen bei allen Herausforderungen jederzeit mit hilfreichen Tipps und Lösungsvorschlägen zur Seite, sodass Sie für Ihren Weg zum Programmierer optimal gerüstet sind!

Compiler 2008

Windows Internals Pavel Yosifovich 2018-05-23 Der Standard-Leitfaden – komplett aktualisiert auf Windows 10 und Windows Server 2016 Tauchen Sie in die Architektur und die inneren Mechanismen von Windows ein und lernen Sie die Kernkomponenten kennen, die hinter den Kulissen arbeiten. Dieser klassische Leitfaden wurde von einem Expertenteam für die inneren Mechanismen von Windows verfasst und vollständig auf Windows 10 und Windows Server 2016 aktualisiert. Dieses Buch gibt Entwicklern und IT-Profis entscheidende Insiderinformationen über die Funktionsweise von Windows. Durch praktische Experimente können Sie das interne Verhalten selbst erfahren und nützliche Kenntnisse zur Verbesserung des Designs Ihrer Anwendungen, zur Steigerung der Leistung, für Debugging und Support gewinnen. In diesem Buch lernen Sie: Wie die Systemarchitektur von Windows aufgebaut ist und wie ihre wichtigsten Elemente aussehen,

insbesondere Prozesse und Threads Wie Prozesse Ressourcen und Threads verwalten Wie Windows virtuellen und physischen Arbeitsspeicher verwaltet Wie es in den Tiefen des E/A-Systems von Windows aussieht, wie Gerätetreiber funktionieren und wie sie mit dem Rest des Systems zusammenwirken Wie das Sicherheitsmodell von Windows Zugriff, Überwachung und Autorisierung handhabt und welche neuen Mechanismen es in Windows 10 und Windows Server 2016 gibt

Eine Tour durch C++ Bjarne Stroustrup 2015-06-08 EINE TOUR DURCH C++ // - Dieser Leitfaden will Ihnen weder das Programmieren beibringen noch versteht er sich als einzige Quelle, die Sie für die Beherrschung von C++ brauchen – aber diese Tour ist wahrscheinlich die kürzeste oder einfachste Einführung in C++11. - Für C- oder C++-Programmierer, die mit der aktuellen C++-Sprache vertrauter werden wollen - Programmierer, die in einer anderen Sprache versiert sind, erhalten ein genaues Bild vom Wesen und von den Vorzügen des modernen C++ . Mit dem C++11-Standard können Programmierer Ideen klarer, einfacher und direkter auszudrücken sowie schnelleren und effizienteren Code zu schreiben. Bjarne Stroustrup, der Designer und ursprüngliche Implementierer von C++, erläutert die Details dieser Sprache und ihre Verwendung in seiner umfassenden Referenz „Die C++-Programmiersprache“. In „Eine Tour durch C++“ führt Stroustrup jetzt die Übersichtskapitel aus der Referenz zusammen und erweitert sie so, dass auch erfahrene Programmierer in nur wenigen Stunden eine Vorstellung davon erhalten, was modernes C++ ausmacht. In diesem kompakten und eigenständigen Leitfaden behandelt Stroustrup – neben Grundlagen – die wichtigsten Sprachelemente und die wesentlichen Komponenten der Standardbibliothek. Er präsentiert die C++-Features im Kontext der Programmierstile, die sie unterstützen, wie die objektorientierte und generische Programmierung. Die Tour beginnt bei den Grundlagen und befasst sich dann mit komplexeren Themen, einschließlich vieler, die neu in C++11 sind wie z.B. Verschiebesemantik, einheitliche Initialisierung, Lambda-Ausdrücke, verbesserte Container, Zufallszahlen und Nebenläufigkeit. Am Ende werden Design und Entwicklung von C++ sowie die in C++11 hinzugekommenen Erweiterungen diskutiert. Programmierer erhalten hier – auch anhand von Schlüsselbeispielen – einen sinnvollen Überblick und praktische Hilfe für den Einstieg. AUS DEM INHALT // Die Grundlagen // Benutzerdefinierte Typen // Modularität // Klassen // Templates // Überblick über die Bibliothek // Strings und reguläre Ausdrücke // E/A-Streams // Container // Algorithmen // Utilities // Numerik // Nebenläufigkeit // Geschichte und Kompatibilität

Die unsichtbare Hand des Staates Nils Grosche 2020-10-27

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

Mehr Hacking mit Python Justin Seitz 2015-10-09 Wenn es um die Entwicklung leistungsfähiger und effizienter Hacking-Tools geht, ist Python für die meisten Sicherheitsanalytiker die Sprache der Wahl. Doch wie genau funktioniert das? In dem neuesten Buch von Justin Seitz - dem Autor des Bestsellers "Hacking mit Python" - entdecken Sie Pythons dunkle Seite. Sie entwickeln Netzwerk-Sniffer, manipulieren Pakete, infizieren virtuelle Maschinen, schaffen unsichtbare Trojaner und vieles mehr. Sie lernen praktisch, wie man • einen "Command-and-Control"-Trojaner mittels GitHub schafft • Sandboxing erkennt und gängige Malware-Aufgaben wie Keylogging und Screenshotting automatisiert • Windows-Rechte mittels kreativer Prozesskontrolle ausweitet • offensive Speicherforensik-Tricks nutzt, um Passwort-Hashes abzugreifen und Shellcode in virtuelle Maschinen einzuspeisen • das beliebte Web-Hacking-Tool Burp erweitert • die Windows COM-Automatisierung nutzt, um einen Man-in-the-Middle-Angriff durchzuführen • möglichst unbemerkt Daten aus einem Netzwerk abgreift Eine Reihe von Insider-Techniken und kreativen Aufgaben zeigen Ihnen, wie Sie die Hacks erweitern und eigene Exploits entwickeln können.

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.

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.

Mastering Reverse Engineering Ajay Kumar Tiwari 2016-02-08 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.

Rechnerarchitektur : Von der digitalen Logik zum Parallelrechner Andrew S. Tanenbaum 2014

Design Patterns für die Spieleprogrammierung Robert Nystrom 2015-08-26 - Die bekannten Design Patterns der Gang of Four im konkreten Einsatz für die Entwicklung von Games - Zahlreiche weitere vom Autor entwickelte Patterns - Sequenzierungs-, Verhaltens-, Entkopplungs- und Optimierungsmuster Für viele Spieleprogrammierer stellt die Finalisierung ihres Spiels die größte Herausforderung dar. Viele Projekte verlaufen im Sande, weil Programmierer der Komplexität des eigenen Codes nicht gewachsen sind. Die im Buch beschriebenen Design Patterns nehmen genau dieses Problem in Angriff. Der Autor blickt auf jahrelange Erfahrung in der Entwicklung von weltweit erfolgreichen Games zurück und stellt erprobte Patterns vor, mit deren Hilfe Sie Ihren Code entwirren und optimieren können. Die Patterns sind in Form unabhängiger Fallbeispiele organisiert, so dass Sie sich nur mit den für Sie relevanten zu befassen brauchen und das Buch auch hervorragend zum Nachschlagen verwenden können. Sie erfahren, wie man eine stabile Game Loop schreibt, wie Spielobjekte mithilfe von Komponenten organisiert werden können und wie man den CPU-Cache nutzt, um die Performance zu verbessern. Außerdem werden Sie sich damit beschäftigen, wie Skript-Engines funktionieren, wie Sie Ihren Code mittels Quadtrees und anderen räumlichen Aufteilungen optimieren und wie sich die klassischen Design Patterns in Spielen einsetzen lassen.

?????? ????????????????. C????????, ?????????, ?????? ? ???????? ??????????? ???????? ?????? 2021-03-30 ??? ????? ?????????? ???????????? ????? ??????-???????????? ???????????? ?? ??????????? ????????????????. ????? ????????????? ???????????, ???????, ?????? ? ??????????? ????????????????, ???????????????, ????????????? ? ????????????????, ????? ???????? ???????????, ?????? ? ???????? ??? ??????????, ???????????????? ????????? ??????????? (??????, ??????????? ?

?????????? ??????), ?????? ?????? (???????????? ?????????, ??????????? ???????????? ??????, ????????????? ???????????? ???????). ??????? ? ??????? ??????-??????????? ?????????? ????????? ?????????? ?????????? ?????????? ??????? ???? ????????? ???????????? ? ???????????? ???????? ???????????? – ? ???????????? ???????????, ????????????????? ??????????, ????????????????? ????????????, ? ???????????, ????????? ?????????, ? ???????? ??????????? ???????????? ???????????, ????????? ? ???? ??????. ????? ????? ???????????? ???????? ?????????, ???????????? ????????? ? ?????? ??????????? ????????????????? ??????????? ????????????? ???, ??????, ???????????, ??????, ? ????? ???????? ????????????? ?????????. ?????????? ? ?????? ????? ????? ?????????? ????????? ???? ?????? ????, ????????????????? ??? ?? ?????????? ?????????????, ???????????? ???????? ??????, ??? ? ???????????? ?? ?????????????????? ??????? ???????????, ??????? ???? ?????? ????? ??? ???? ????? ???????? ??????????.??????, ??????? ?? ???????? ?? ???? ?????, ??????? ??? ???????? ???????????? ?????? ? ?????????, ???????????? ??????? ? ???????? ?????????, ??????? ? ????????? ? ???????????? ???????????? ???????? ???????????? ? ???????????? ?? ???????? ???????? ????????????.