Read Free Blunden Bill System Of Corners Dark In Evasion And Escape Arsenal Rootkit The

Thank you for downloading **Blunden Bill System Of Corners Dark In Evasion And Escape Arsenal Rootkit The**. Maybe you have knowledge that, people have look numerous times for their chosen novels like this Blunden Bill System Of Corners Dark In Evasion And Escape Arsenal Rootkit The, but end up in harmful downloads.
Rather than reading a good book with a cup of tea in the afternoon, instead they cope with some malicious virus inside their laptop.

Blunden Bill System Of Corners Dark In Evasion And Escape Arsenal Rootkit The is available in our book collection an online access to it is set as public so you can get it instantly.
Our books collection saves in multiple locations, allowing you to get the most less latency time to download any of our books like this one.
Merely said, the Blunden Bill System Of Corners Dark In Evasion And Escape Arsenal Rootkit The is universally compatible with any devices to read

KEY=SYSTEM - CLARK KELLEY

The Rootkit Arsenal

Escape and Evasion in the Dark Corners of the System

Jones & Bartlett Publishers While forensic analysis has proven to be a valuable investigative tool in the field of computer security, utilizing anti-forensic technology makes it possible to maintain a covert operational foothold for extended periods, even in a high-security environment. Adopting an approach that favors full disclosure, the updated Second Edition of The Rootkit Arsenal presents the most accessible, timely, and complete coverage of forensic countermeasures. This book covers more topics, in greater depth, than any other currently available. In doing so the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented. The range of topics presented includes how to: -Evade post-mortem analysis -Frustrate attempts to reverse engineer your command & control modules -Defeat live incident response -Undermine the process of memory analysis -Modify subsystem internals to feed misinformation to the outside -Entrench your code in fortified regions of execution -Design and implement covert channels -Unearth new avenues of attack

The Rootkit Arsenal

Escape and Evasion in the Dark Corners of the System

The Rootkit Arsenal: Escape and Evasion

Jones & Bartlett Publishers With the growing prevalence of the Internet, rootkit technology has taken center stage in the battle between White Hats and Black Hats. Adopting an approach that favors full disclosure, The Rootkit Arsenal presents the most accessible, timely, and complete coverage of rootkit technology. This book covers more topics, in greater depth, than any other currently available. In doing so, the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented.

The Rootkit Arsenal

Escape and Evasion

Jones & Bartlett Learning A guide to rootkit technology covers such topics as using kernal debugger, modifying privilege levels on Windows Vista, establishing covert network channels, and using detour patches.

System Forensics, Investigation, and Response

Jones & Bartlett Publishers Computer crimes call for forensics specialists---people who know to find and follow the evidence. System Forensics, Investigation, and Response examines the fundamentals of system forensics what forensics is, an overview of computer crime, the challenges of system forensics, and forensics methods. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation, including evidence collection, investigating information-hiding, recovering data, and more. The book closes with an exploration of incident and intrusion response, emerging technologies and future directions of the field, and additional system forensics resources. The Jones & Bartlett Learning Information Systems Security & Assurance Series delivers fundamental IT security principles packed with real world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information Systems, Security programs. Authored by Certified Information Systems Security professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of today and tomorrow.

Detecting Peripheral-based Attacks on the Host Memory

Springer This work addresses stealthy peripheral-based attacks on host computers and presents a new approach to detecting them. Peripherals can be regarded as separate systems that have a dedicated processor and dedicated runtime memory to handle their tasks. The book addresses the problem that peripherals generally communicate with the host via the host’s main memory, storing cryptographic keys, passwords, opened files and other sensitive data in the process – an aspect attackers are quick to exploit. Here, stealthy malicious software based on isolated micro-controllers is implemented to conduct an attack analysis, the results of which provide the basis for developing a novel runtime detector. The detector reveals stealthy peripheral-based attacks on the host’s main memory by exploiting certain hardware properties, while a permanent and resource-efficient measurement strategy ensures that the detector is also capable of detecting transient attacks, which can otherwise succeed when the applied strategy only measures intermittently. Attackers exploit this strategy by attacking the system in between two measurements and erasing all traces of the attack before the system is measured again.

How to Stop E-mail Spam, Spyware, Malware, Computer Viruses, and Hackers from Ruining Your Computer Or Network

The Complete Guide for Your Home and Work

Atlantic Publishing Company Presents an introduction to different types of malware and viruses, describes antivirus solutions, offers ways to detect spyware and malware, and discusses the use of firewalls and other security options.

Game Hacking

Developing Autonomous Bots for Online Games

No Starch Press You don’t need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: –Scan and modify memory with Cheat Engine –Explore program structure and execution flow with OllyDbg –Log processes and pinpoint useful data files with Process Monitor –Manipulate control flow through NOPing, hooking, and more –Locate and dissect common game memory structures You’ll even discover the secrets behind common game bots, including: –Extrasensory perception hacks, such as wallhacks and heads-up displays –Responsive hacks, such as autohealers and combo bots –Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn’t have to be. Once you understand how bots are made, you’ll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

Introduction to Computer and Network Security

Navigating Shades of Gray

CRC Press Guides Students in Understanding the Interactions between Computing/Networking Technologies and Security Issues Taking an interactive, "learn-by-doing" approach to teaching, Introduction to Computer and Network Security: Navigating Shades of Gray gives you a clear course to teach the technical issues related to security. Unlike most computer security books, which concentrate on software design and implementation, cryptographic tools, or networking issues, this text also explores how the interactions between hardware, software, and users affect system security. The book presents basic principles and concepts, along with examples of current threats to illustrate how the principles can either enable or neutralize exploits. Students see the importance of these concepts in existing and future technologies. In a challenging yet enjoyable way, they learn about a variety of technical topics, including current security exploits, technical factors that enable attacks, and economic and social factors that determine the security of future systems. Extensively classroom-tested, the material is structured around a set of challenging projects. Through staging exploits and choosing countermeasures to neutralize the attacks in the projects, students learn: How computer systems and networks operate How to reverse-engineer processes How to use systems in ways that were never foreseen (or supported) by the original developers Combining hands-on work with technical overviews, this text helps you integrate security analysis into your technical computing curriculum. It will educate your students on security issues, such as side-channel attacks, and deepen their understanding of how computers and networks work.

Virtual Machine Design and Implementation in C/C++

Wordware This is an in-depth look at the construction and underlying theory of a fullyfunctional virtual machine and an entire suite of related development tools.

Software Exorcism

A Handbook for Debugging and Optimizing Legacy Code

Apress This is a special title that will be both technically useful and visually stimulating to the reader.

Rootkits

Subverting the Windows Kernel

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

Computer Security Handbook, Set

John Wiley & Sons Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.

Windows Malware Analysis Essentials

Packt Publishing Ltd Master the fundamentals of malware analysis for the Windows platform and enhance your anti-malware skill set About This Book Set the baseline towards performing malware analysis on the Windows platform and how to use the tools required to deal with malware Understand how to decipher x86 assembly code from source code inside your favourite development environment A step-by-step based guide that reveals malware analysis from an industry insider and demystifies the process Who This Book Is For This book is best for someone who has prior experience with reverse engineering Windows executables and wants to specialize in malware analysis. The book presents the malware analysis thought process using a show-and-tell approach, and the examples included will give any analyst confidence in how to approach this task on their own the next time around. What You Will Learn Use the positional number system for clear conception of Boolean algebra, that applies to malware research purposes Get introduced to static and dynamic analysis methodologies and build your own malware lab Analyse destructive malware samples from the real world (ITW) from fingerprinting and static/dynamic analysis to the final debrief Understand different modes of linking and how to compile your own libraries from assembly code and integrate the codein your final program Get to know about the various emulators, debuggers and their features, and sandboxes and set them up effectively depending on the required scenario Deal with other malware vectors such as pdf and MS-Office based malware as well as scripts and shellcode In Detail Windows OS is the most used operating system in the world and hence is targeted by malware writers. There are strong ramifications if things go awry. Things will go wrong if they can, and hence we see a salvo of attacks that have continued to disrupt the normal scheme of things in our day to day lives. This book will guide you on how to use essential tools such as debuggers, disassemblers, and sandboxes to dissect malware samples. It will expose your innards and then build a report of their indicators of compromise along with detection rule sets that will enable you to help contain the outbreak when faced with such a situation. We will start with the basics of computing fundamentals such as number systems and Boolean algebra. Further, you'll learn about x86 assembly programming and its integration with high level languages such as C++.You'll understand how to decipher disassembly code obtained from the compiled source code and map it back to its original design goals. By delving into end to end analysis with real-world malware samples to solidify your understanding, you'll sharpen your technique of handling destructive malware binaries and vector mechanisms. You will also be encouraged to consider analysis lab safety measures so that there is no infection in the process. Finally, we'll have a rounded tour of various emulations, sandboxing, and debugging options so that you know what is at your disposal when you need a specific kind of weapon in order to nullify the malware. Style and approach An easy to follow, hands-on guide with descriptions and screenshots that will help you execute effective malicious software investigations and conjure up solutions creatively and confidently.

Rootkits, Spyware/Adware, Keyloggers and Backdoors: Detection and Neutralization

БХВ-Петербург Covering the wide range of technologies implemented by contemporary malware programs such as rootkits, keyloggers, spyware, adware, back doors, and network and mail worms, this practical guide for system administrators and experienced users covers approaches to computer investigation and how to locate and destroy malicious programs without using antiviral software. Examples such as protocol fragments, operating principles of contemporary malicious programs, and an overview of specialized software for finding and neutralizing malware are presented, and the accompanying CD-ROM includes programs for system analysis and an antiviral utility intended for investigating the system and detecting rootkits and keyloggers.

Learning Malware Analysis

Explore the concepts, tools, and techniques to analyze and investigate Windows malware

Packt Publishing Ltd 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.

Malware, Rootkits & Botnets A Beginner's Guide

McGraw Hill Professional Security Smarts for the Self-Guided IT Professional Learn how to improve the security posture of your organization and defend against some of the most pervasive network attacks. Malware, Rootkits & Botnets: A Beginner's Guide explains the nature, sophistication, and danger of these risks and offers best practices for thwarting them. After reviewing the current threat landscape, the book describes the entire threat lifecycle, explaining how cybercriminals create, deploy, and manage the malware, rootkits, and botnets under their control. You'll learn proven techniques for identifying and mitigating these malicious attacks. Templates, checklists, and examples give you the hands-on help you need to get started protecting your network right away. Malware, Rootkits & Botnets: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work

Professional Assembly Language

John Wiley & Sons Unlike high-level languages such as Java and C++, assembly language is much closer to the machine code that actually runs computers; it's used to create programs or modules that are very fast and efficient, as well as in hacking exploits and reverse engineering Covering assembly language in the Pentium microprocessor environment, this code-intensive guide shows programmers how to create stand-alone assembly language programs as well as how to incorporate assembly language libraries or routines into existing high-level applications Demonstrates how to manipulate data, incorporate advanced functions and libraries, and maximize application performance Examples use C as a high-level language, Linux as the development environment, and GNU tools for assembling, compiling, linking, and debugging

Behold a Pale Farce

Cyberwar, Threat Inflation, & the Malware Industrial Complex

Trine Day This book presents a data-driven message that exposes the cyberwar media campaign being directed by the Pentagon and its patronage networks. By demonstrating that the American public is being coerced by a threat that has been blown out of proportion—much like the run-up to the Gulf War or the global war on terror—this book discusses how the notion of cyberwar instills a crisis mentality that discourages formal risk assessment, making the public anxious and hence susceptible to ill-conceived solutions. With content that challenges conventional notions regarding cyber security, Behold a Pale Farce covers topics—including cybercrime; modern espionage; mass-surveillance systems; and the threats facing infrastructure targets such as the Federal Reserve, the stock exchange, and telecommunications—in a way that provides objective analysis rather than advocacy. This book is a must-read for anyone concerned with the recent emergence of Orwellian tools of mass interception that have developed under the guise of national security.

A Guide to Kernel Exploitation

Attacking the Core

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

Dr. Dropo's Juggling Buffoonery

Piccadilly Books, Ltd. People who want to develop an act for birthday parties or street corners will find this book a blessing. Easy-to-follow directions on how to juggle, manipulate cigar boxes, do balancing tricks, and become an hilariously funny juggler. Contains 25 complete comic juggling routines. Simple enough for beginners, funny enough for professionals.

Windows Internals, Part 1

System architecture, processes, threads, memory management, and more

Microsoft 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 Internals, Part 2

Microsoft Press Drill down into Windows architecture and internals, discover how core Windows components work behind the scenes, and master information you can continually apply to improve architecture, development, system administration, and support. Led by three renowned Windows internals experts, this classic guide is now fully updated for Windows 10 and 8.x. As always, it combines unparalleled insider perspectives on how Windows behaves "under the hood" with hands-on experiments that let you experience these hidden behaviors firsthand. Part 2 examines these and other key Windows 10 OS components and capabilities: Startup and shutdown The Windows Registry Windows management mechanisms WMI System mechanisms ALPC ETW Cache Manager Windows file systems The hypervisor and virtualization UWP Activation Revised throughout, this edition also contains three entirely new chapters: Virtualization technologies Management diagnostics and tracing Caching and file system support

Cube Farm

Apress * Entertainment value (broader market than pure technical). * Provides "lessons learned" section at end of each chapter. * Offers instruction in corporate self-defense. * Explains business software in simple terms. * Allows reader to peek behind the curtain.

The 4 Cornerstones of Your Success

Building a Life Beyond Your Imagination

This profound yet simple book allows readers to get the total picture on how to live beyond mere imagination and bring about the true essence of "the good life". The 4 cornerstones takes the 4 most important areas of your life; faith, family, fitness, and finance and combines it together for your ultimate success! Never before has an author been able to take these unique areas and combine them into one simplified master piece towards your complete prosperity, as Drew Parker does. Purchase your copy today at www.shop.visualizedwealth.com. Available on paperback & e-book.

On the Corner of Heartache & Love

Createspace Independent Publishing Platform After three years, Maren Summers is elated to finally have her dream wedding to her dream man, Kevin Bryant. In her sights is the promotion to weddings she's worked so hard for at the newspaper. Happily ever after is within her grasp... Until Kevin jilts her at the altar, elopes with another woman, and becomes her boss. Devastated by the twisted turn of events Maren moves in with her best friend and notices the not-so-homeless guy on the corner, Zane Whitfield. As his heart-wrenching tale unfolds-his vow to wait a year on the corner for his lost love-Maren sees his compassionate human-interest story as her ticket away from Kevin, weddings, and her heartache. But as the New Year approaches, is Maren headed for heartache again when Zane's lost love returns or has time changed more than one heart?

The Bonadventure: A Random Journal of an Atlantic Holiday

Good Press "The Bonadventure: A Random Journal of an Atlantic Holiday" by Edmund Blunden. Published by Good Press. Good Press publishes a wide range of titles that encompasses every genre. From well-known classics & literary fiction and non-fiction to forgotten−or yet undiscovered gems−of world literature, we issue the books that need to be read. Each Good Press edition has been meticulously edited and formatted to boost readability for all e-readers and devices. Our goal is to produce eBooks that are user-friendly and accessible to everyone in a high-quality digital format.

Spatial Analysis, GIS and Remote Sensing

Applications in the Health Sciences

CRC Press This new book explores the rapidly expanding applications of spatial analysis, GIS and remote sensing in the health sciences, and medical geography.

The Cuckoo's Egg

Tracking a Spy Through the Maze of Computer Espionage

Simon and Schuster The first true account of computer espionage tells of a year-long single-handed hunt for a computer thief who sold information from American computer files to Soviet intelligence agents

Truth Is Not Always True

Createspace Independent Publishing Platform When Joe sees his late wife on a street corner, he believes he's either seen a ghost, or is insane. Jen and he were indescribably in love, but she was tragically killed a year earlier, and he's since remarried.Jen wasn't killed. The report of her death was an appalling mistake. Shattered and almost destroyed in finding him married to someone else, she struggles to find sanity and a new life. A story of love and strife that poses many questions.

Fix It Now

Rediscover the Constitution and Get America Out of Its Fiscal Death Spiral

Createspace Independent Pub A reader-friendly explanation of the need to restore limited government and other American founding values.

Offshoring IT

The Good, the Bad, and the Ugly

Apress * Offers a Well-Rounded Discussion Based on Opposing Views. * Discusses the Obstacles that Confront Offshore Employers, such as the foreign nation's: * Infrastructure (availability of electricity, transportation, water, food, etc). * Political stability. * Distance from the U.S. * Mortality rate. * Health care. * Presents an Exhaustive Survey of Companies Going Offshore. * Offers a Realistic Look at Potential Endgame Scenarios.

Hacking Multifactor Authentication

John Wiley & Sons Protect your organization from scandalously easy-to-hack MFA security “solutions” Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That’s right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You’ll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book. Learn how different types of multifactor authentication work behind the scenes See how easy it is to hack MFA security solutions—no matter how secure they seem Identify the strengths and weaknesses in your (or your customers’) existing MFA security and how to mitigate Author Roger Grimes is an internationally known security expert whose work on hacking MFA has generated significant buzz in the security world. Read this book to learn what decisions and preparations your organization needs to take to prevent losses from MFA hacking.

The Making of the English Working Class

Penguin UK A book that revolutionised our understanding of English social history. E. P. Thompson shows how the English working class emerged through the degradations of the industrial revolution to create a culture and political consciousness of enormous vitality.

Red Team

Strigoi

Createspace Independent Publishing Platform Those monsters that kept you up at night as a child, the ones that made you pull the covers up to your chin while you stared into the dark corners and saw shadows move. Or pulled the blankets over your head and imagined creatures inching across your bedroom. Well, they're real. The Organization, as it's called, is tasked with keeping the nightmares of myth and legend from invading the public eye. The group must be kept a secret along with the fact that the creatures exist. As civilization expands its boundaries, that undertaking becomes more difficult. A very few are selected to stand on the lines between humankind and the horrors lurking in the dark recesses of the world. Follow Jack Walker and Red Team as they're pulled into the shadows to combat creatures that once kept them awake at night.

The Uninhabitable Earth

A Story of the Future

Penguin UK **SUNDAY TIMES AND THE NEW YORK TIMES BESTSELLER** 'An epoch-defining book' Matt Haig 'If you read just one work of non-fiction this year, it should probably be this' David Sexton, Evening Standard Selected as a Book of the Year 2019 by the Sunday Times, Spectator and New Statesman A Waterstones Paperback of the Year and shortlisted for the Foyles Book of the Year 2019 Longlisted for the PEN / E.O. Wilson Literary Science Writing Award It is worse, much worse, than you think. The slowness of climate change is a fairy tale, perhaps as pernicious as the one that says it isn't happening at all, and if your anxiety about it is dominated by fears of sea-level rise, you are barely scratching the surface of what terrors are possible, even within the lifetime of a teenager today. Over the past decades, the term "Anthropocene" has climbed into the popular imagination - a name given to the geologic era we live in now, one defined by human intervention in the life of the planet. But however sanguine you might be about the proposition that we have ravaged the natural world, which we surely have, it is another thing entirely to consider the possibility that we have only provoked it, engineering first in ignorance and then in denial a climate system that will now go to war with us for many centuries, perhaps until it destroys us. In the meantime, it will remake us, transforming every aspect of the way we live-the planet no longer nurturing a dream of abundance, but a living nightmare.

An Essay on the Principle of Population

Cosimo, Inc. Around 1796, Mr. Malthus, an English gentleman, had finished reading a book that confidently predicted human life would continue to grow richer, more comfortable and more secure, and that nothing could stop the march of progress. He discussed this theme with his son, Thomas, and Thomas ardently disagreed with both his father and the book he had been reading, along with the entire idea of unending human progress. Mr. Malthus suggested that he write down his objections so that they could discuss them point-by-point. Not long after, Thomas returned with a rather long essay. His father was so impressed that he urged his son to have it published. And so, in 1798, appeared An Essay on Population, by British political economist and demographer THOMAS ROBERT MALTHUS (1766-1834). Though it was attacked at the time and ridiculed for many years afterward, it has remained one of the most influential works in the English language on the general checks and balances of the world's population and its necessary control. This is a replica of the 1826 sixth edition. Volume 1 includes: Book I: "Of the Checks to the Population in the Less Civilised Parts of the World and in Past Times" and Book II: "Of the Checks to the Population in the Different States of Modern Europe."

The Wrong Side of Space

Lt. Commander Heskan and Komandor Lombardi have only one thing in common - the will to survive. Bitter rivals for over a century, the Brevic Republic and the Hollaran Commonwealth are at war. Cultures that shared a common Terran ancestry have been isolated for decades. Now, Heskan's escort ships must protect Lombardi's heavy cruisers as they are forced to run together into unexplored space from a devastating threat. Each commander faces dissension in the ranks, even as they try to unite their fleets and find some way to escape the fate of so many of their fallen comrades. For the duration of the tenuous truce, there is a singular objective... make it home.Yet there can be only one destination at the end of their journey, and only half of the fleet will be safe, if they reach the Republic or Commonwealth at all. If the warring governments cannot be trusted to secure safe passage of the allied crews, how can the two commanders trust each other?This is Book 3 in the This Corner of the Universe series, continuing the story of the original crew of BRS Anelace and her captain.

Three Thousand Years of Chinese Painting

Yale University Press Written by a team of eminent international scholars, this book is the first to recount the history of Chinese painting over a span of some 3000 years.

Sustainable Development and Renovation in Architecture, Urbanism and Engineering

Springer This book provides an overview of the environmental problems that arise from construction activity, focusing on refurbishment as an alternative to the current crisis in the construction sector, as well as on measures designed to minimize the effects on the environment. Furthermore, it offers professionals insights into alternative eco-efficient solutions using new materials to minimize environmental impacts and offers solutions that they can incorporate into their own designs and buildings. It also demonstrates best practices in the cooperation between various universities in Andalusia in Spain and Latin America and many public and private companies and organizations. This book serves as a valuable reference resource for professionals and researchers and provides an overview on the status of investigations to find solutions to improve sustainable development in terms of materials, systems, facilities, neighborhoods, buildings, and awareness of the society involved.