Intelligence Driven Incident Response Outwitting The Adversary

Getting the books **Intelligence Driven Incident Response Outwitting The Adversary** now is not type of challenging means. You could not abandoned going once books heap or library or borrowing from your associates to way in them. This is an agreed simple means to specifically get lead by on-line. This online message Intelligence Driven Incident Response Outwitting The Adversary can be one of the options to accompany you next having additional time.

It will not waste your time. agree to me, the e-book will unquestionably broadcast you supplementary issue to read. Just invest tiny times to entrance this on-line notice **Intelligence Driven Incident Response Outwitting The Adversary** as well as review them wherever you are now.

Cyberpunk 2077 - Piggyback 2020-04-16

The Complete Official Guide to Cyberpunk 2077 is a massive book covering everything in the game. With details on every last challenge and feature, the guide offers streamlined progression through the entire adventure, as well as a commanding expertise on all key systems. 100% authoritative: all branching paths, all side quests, all rewards, and all endings fully mapped out; also includes optional challenges, mini-games, unlockables, secrets, and more. Foolproof explanations: every mission, every game mechanic, every meaningful choice covered with accessible solutions. Hi-res maps of Night City: each annotated with locations of collectibles and points of interest. Reference & Analysis Chapter: in-depth coverage of all major game systems, including character progression, abilities, perks, Street Cred, Trophies/Achievements, among others. At-a-glance Walkthroughs: annotated screenshots and sequential steps show optimal ways through every mission. Expert Combat Strategies: practical, reproducible tactics to crush all enemies and bosses. Comprehensive references: all-inclusive appraisals of all items and weapons – including statistics and unlock conditions. Spoiler-sensitive: carefully designed to avoid spoilers, ensuring you can read without ever ruining your appreciation of the story. Instant searches: print navigation systems and an extensive index give you immediate access to the information you need. Concept art: direct from the development team and beautifully laid out

Invisible City - Julia Dahl 2014-05-06

A finalist for the Edgar and Mary Higgins Clark Awards, in her riveting debut Invisible City, journalist Julia Dahl introduces a compelling new character in search of the truth about a murder and an understanding of her own heritage. Just months after Rebekah Roberts was born, her mother, an Hasidic Jew from Brooklyn, abandoned her Christian boyfriend and newborn baby to return to her religion. Neither Rebekah nor her father have heard from her since. Now a recent college graduate, Rebekah has moved to New York City to follow her dream of becoming a big-city reporter. But she's also drawn to the idea of being closer to her mother, who might still be living in the Hasidic community in Brooklyn. Then Rebekah is called to cover the story of a murdered Hasidic woman. Rebekah's shocked to learn that, because of the NYPD's habit of kowtowing to the powerful ultra-Orthodox community, not only will the woman be buried without an autopsy, her killer may get away with murder. Rebekah can't let the story end there. But getting to the truth won't be easy—even as she immerses herself in the cloistered world where her mother grew up, it's clear that she's not welcome, and everyone she meets has a secret to keep from an outsider.

CUCKOO'S EGG - Clifford Stoll 2012-05-23

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

The Art of Intrusion - Kevin D. Mitnick 2009-03-17

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-andthen told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

Threat Modeling - Adam Shostack 2014-02-12

The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

Defensive Security Handbook - Lee Brotherston 2017-04-03
Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don’t have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring

Cyber Security Policy Guidebook - Jennifer L. Bayuk 2012-04-24
Drawing upon a wealth of experience from academia, industry, and government service, Cyber Security Policy Guidebook details and dissects, in simple language, current organizational cyber security policy issues on a global scale—taking great care to educate readers on the history and current approaches to the security of cyberspace. It includes thorough descriptions—as well as the pros and cons—of a plethora of issues, and documents policy alternatives for the sake of clarity with respect to policy alone. The Guidebook also delves into organizational implementation issues, and equips readers with descriptions of the positive and negative impact of specific policy choices. Inside are detailed chapters that: Explain what is meant by cyber security and cyber security policy Discuss the process by which cyber security policy goals are set Educate the reader on decision-making processes related to cyber security Describe a new framework and taxonomy for explaining cyber security policy issues Show how the U.S. government is dealing with cyber security policy issues With a glossary that puts cyber security language in layman's terms—and diagrams that help explain complex topics—Cyber Security Policy Guidebook gives students, scholars, and technical decision-makers the necessary knowledge to make informed decisions on cyber security policy.

Crafting the InfoSec Playbook - Jeff Bollinger 2015-05-07
Any good attacker will tell you that expensive security monitoring and prevention tools aren’t enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You’ll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone. Written by members of Cisco’s Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture. Learn incident response fundamentals—and the importance of getting back to basics Understand threats you face and what you should be protecting Collect, mine, organize, and analyze as many relevant data sources as possible Build your own playbook of repeatable methods for security monitoring and response Learn how to put your plan into action and keep it running smoothly Select the right monitoring and detection tools for your environment Develop queries to help you sort through data and create valuable reports Know what actions to take during the incident response phase

The Cultural Cold War - Frances Stonor Saunders 2013-11-05
During the Cold War, freedom of expression was vaunted as liberal democracy’s most cherished possession—but such freedom was put in

service of a hidden agenda. In The Cultural Cold War, Frances Stonor Saunders reveals the extraordinary efforts of a secret campaign in which some of the most vocal exponents of intellectual freedom in the West were working for or subsidized by the CIA—whether they knew it or not. Called "the most comprehensive account yet of the [CIA's] activities between 1947 and 1967" by the New York Times, the book presents shocking evidence of the CIA's undercover program of cultural interventions in Western Europe and at home, drawing together declassified documents and exclusive interviews to expose the CIA's astonishing campaign to deploy the likes of Hannah Arendt, Isaiah Berlin, Leonard Bernstein, Robert Lowell, George Orwell, and Jackson Pollock as weapons in the Cold War. Translated into ten languages, this classic work—now with a new preface by the author—is "a real contribution to popular understanding of the postwar period" (The Wall Street Journal), and its story of covert cultural efforts to win hearts and minds continues to be relevant today.

Intelligence-Driven Incident Response - Scott J Roberts 2017-08-21

Using a well-conceived incident response plan in the aftermath of an online security breach enables your team to identify attackers and learn how they operate. But, only when you approach incident response with a cyber threat intelligence mindset will you truly understand the value of that information. With this practical guide, you'll learn the fundamentals of intelligence analysis, as well as the best ways to incorporate these techniques into your incident response process. Each method reinforces the other: threat intelligence supports and augments incident response, while incident response generates useful threat intelligence. This book helps incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts understand, implement, and benefit from this relationship. In three parts, this in-depth book includes: The fundamentals: get an introduction to cyber threat intelligence, the intelligence process, the incident-response process, and how they all work together Practical application: walk through the intelligence-driven incident response (IDIR) process using the F3EAD process—Find, Fix Finish, Exploit, Analyze, and Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building

Malware Data Science - Joshua Saxe 2018-09-25

Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a "big data" problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you'll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Saxe introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You'll learn how to: - Analyze malware using static analysis - Observe malware behavior using dynamic analysis - Identify adversary groups through shared code analysis - Catch 0-day vulnerabilities by building your own machine learning detector - Measure malware detector accuracy - Identify malware campaigns, trends, and relationships through data visualization Whether you're a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.

Intelligence Analysis: How to Think in Complex Environments - Wayne Michael Hall 2009-12-22

This book offers a vast conceptual and theoretical exploration of the ways intelligence analysis must change in order to succeed against today's most dangerous combatants and most complex irregular theatres of conflict. • Includes quotations from a wide range of acclaimed thinkers • Offers an extensive bibliography of works cited and resources for further reading • Presents a comprehensive index

Insider Attack and Cyber Security - Salvatore J. Stolfo 2008-08-29

This book defines the nature and scope of insider problems as viewed by the financial industry. This edited volume is based on the first workshop on Insider Attack and Cyber Security, IACS 2007. The workshop was a joint effort from the Information Security Departments of Columbia University and Dartmouth College. The book sets an agenda for an ongoing research initiative to solve one of the most vexing problems encountered in security, and a range of topics from critical IT infrastructure to insider threats. In some ways, the insider problem is the ultimate security problem.

Blue Team Handbook - Don Murdoch 2014-08-03

Updated, Expanded, and released to print on 10/5/14! Complete details below! Two new sections, five protocol header illustrations, improved formatting, and other corrections. The Blue Team Handbook is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics. The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way. Version 2.0 updates: - *** A new section on Database incident response was added. - *** A new section on Chain of Custody was added. - *** Matt Baxter's superbly formatted protocol headers were added! - Table headers bolded. - Table format slightly revised throughout book to improve left column readability. - Several sentences updated and expanded for readability and completeness. - A few spelling errors were corrected. - Several sites added to the Web References section. - Illustrations reformatted for better fit on the page. - An index was added. - Attribution for some content made more clear (footnotes, expanded source citing) - Content expanded a total of 20 pages

The Origin of Consciousness in the Breakdown of the Bicameral Mind - Julian Jaynes 2000-08-15

National Book Award Finalist: “This man’s ideas may be the most influential, not to say controversial, of the second half of the twentieth century.”—Columbus Dispatch At the heart of this classic, seminal book is Julian Jaynes's still-controversial thesis that human consciousness did not begin far back in animal evolution but instead is a learned process that came about only three thousand years ago and is still developing. The implications of this revolutionary scientific paradigm extend into virtually every aspect of our psychology, our history and culture, our religion—and indeed our future. “Don’t be put off by the academic title of Julian Jaynes’s The Origin of Consciousness in the Breakdown of the Bicameral Mind. Its prose is always lucid and often lyrical…he unfolds his case with the utmost intellectual rigor.”—The New York Times “When Julian Jaynes . . . speculates that until late in the twentieth millennium BC men had no consciousness but were automatically obeying the voices of the gods, we are astounded but compelled to follow this remarkable thesis.”—John Updike, The New Yorker “He is as startling as Freud was in The Interpretation of Dreams, and Jaynes is equally as adept at forcing a new view of known human behavior.”—American Journal of Psychiatry

Practical Threat Intelligence and Data-Driven Threat Hunting - Valentina Costa-Gazcon 2021-02-12

Get to grips with cyber threat intelligence and data-driven threat hunting while exploring expert tips and techniques Key FeaturesSet up an environment to centralize all data in an Elasticsearch, Logstash, and Kibana (ELK) server that enables threat huntingCarry out atomic hunts to start the threat hunting process and understand the environmentPerform advanced hunting using MITRE ATT&CK Evals emulations and Mordor datasetsBook Description Threat hunting (TH) provides cybersecurity analysts and enterprises with the opportunity to proactively defend themselves by getting ahead of threats before they can cause major damage to their business. This book is not only an introduction for those who don't know much about the cyber threat intelligence (CTI) and TH world, but also a guide for those with more advanced knowledge of other cybersecurity fields who are looking to implement a TH program from scratch. You will start by exploring what threat intelligence is and how it can be used to detect and prevent cyber threats. As you progress, you'll learn how to collect data, along with understanding it by developing data models. The book will also show you how to set up an environment for TH using open source tools. Later, you will focus on how to plan a hunt with practical examples, before going on to explore the MITRE ATT&CK framework. By the end of this book, you'll have the skills you need to be able to carry out effective hunts in your own environment. What you will learnUnderstand what CTI is, its key concepts, and how it is useful for preventing threats and protecting your organizationExplore the different stages of the TH processModel the data collected and understand how to document the findingsSimulate threat actor activity in a lab environmentUse the information collected to detect breaches and validate the results of your queriesUse documentation and strategies to communicate processes to senior management and the wider businessWho this book is for If you are looking to start out in the cyber intelligence and threat hunting domains and want to know more about how to implement a threat hunting division with open-source tools, then this cyber threat intelligence book is for you.

Essential Cybersecurity Science - Josiah Dykstra 2015-12-08

If you’re involved in cybersecurity as a software developer, forensic investigator, or network administrator, this practical guide shows you how to apply the scientific method when assessing techniques for protecting your information systems. You’ll learn how to conduct scientific experiments on everyday tools and procedures, whether you’re evaluating corporate security systems, testing your own security product, or looking for bugs in a mobile game. Once author Josiah Dykstra gets you up to speed on the scientific method, he helps you focus on standalone, domain-specific topics, such as cryptography, malware analysis, and system security engineering. The latter chapters include practical case studies that demonstrate how to use available tools to conduct domain-specific scientific experiments. Learn the steps necessary to conduct scientific experiments in cybersecurity Explore fuzzing to test how your software handles various inputs Measure the performance of the Snort intrusion detection system Locate malicious “needles in a haystack” in your network and IT environment Evaluate cryptography design and application in IoT products Conduct an experiment to identify relationships between similar malware binaries Understand system-level security requirements for enterprise networks and web services

Industry of Anonymity - Jonathan Lusthaus 2018-10-16

Jonathan Lusthaus lifts the veil on cybercriminals in the most extensive account yet of the lives they lead and the vast international industry they have created. Having traveled to hotspots around the world to meet with hundreds of law enforcement agents, security gurus, hackers, and criminals, he charts how this industry based on anonymity works.

Risk Centric Threat Modeling - Tony UcedaVelez 2015-05-26

This book introduces the Process for Attack Simulation & Threat Analysis (PASTA) threat modeling methodology. It provides an introduction to various types of application threat modeling and introduces a risk-centric methodology aimed at applying security countermeasures that are commensurate to the possible impact that could be sustained from defined threat models, vulnerabilities, weaknesses, and attack patterns. This book describes how to apply application threat modeling as an advanced preventive form of security. The authors discuss the methodologies, tools, and case studies of successful application threat modeling techniques. Chapter 1 provides an overview of threat modeling, while Chapter 2 describes the objectives and benefits of threat modeling. Chapter 3 focuses on existing threat modeling approaches, and Chapter 4 discusses integrating threat modeling within the different types of Software Development Lifecycles (SDLCs). Threat modeling and risk management is the focus of Chapter 5. Chapter 6 and Chapter 7 examine Process for Attack Simulation and Threat Analysis (PASTA). Finally, Chapter 8 shows how to use the PASTA risk-centric threat modeling process to analyze the risks of specific threat agents targeting web applications. This chapter focuses specifically on the web application assets that include customer’s confidential data and business critical functionality that the web application provides. • Provides a detailed walkthrough of the PASTA methodology alongside software development activities, normally conducted via a standard SDLC process • Offers precise steps to take when combating threats to businesses • Examines real-life data breach incidents and lessons for risk management Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis is a resource for software developers, architects, technical risk managers, and seasoned security professionals.

Life of Pi - Yann Martel 2022-01-27

"Life of Pi will make you believe in the power of theatre" (Times). After a cargo ship sinks in the middle of the vast Pacific Ocean, there are five survivors stranded on a lifeboat - a hyena, a zebra, an orangutan, a Royal Bengal tiger, and a sixteen year-old boy named Pi. Time is against them, nature is harsh, who will survive? Based on one of the most extraordinary and best-loved works of fiction - winner of the Man Booker Prize, selling over fifteen million copies worldwide - and featuring breath-taking puppetry and state-of-the-art visuals, Life of Pi is a universally acclaimed, smash hit adaptation of an epic journey of endurance and hope. Adapted by acclaimed playwright Lolita Chakrabarti, this edition was published to coincide with the West End premiere in November 2021.

Applied Incident Response - Steve Anson 2020-01-29

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls

Real digital forensics -

Applied Network Security Monitoring - Chris Sanders 2013-11-26

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM. Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster. The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data. If you've never performed NSM analysis, Applied Network Security Monitoring will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job. Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples Companion website includes up-to-date blogs from the authors about the latest developments in NSM

Cyber Warfare – Truth, Tactics, and Strategies - Dr. Chase

Cunningham 2020-02-25

Insights into the true history of cyber warfare, and the strategies, tactics, and cybersecurity tools that can be used to better defend yourself and your organization against cyber threat. Key FeaturesDefine and determine a cyber-defence strategy based on current and past real-life examplesUnderstand how future technologies will impact cyber warfare campaigns and societyFuture-ready yourself and your business against any cyber threatBook Description The era of cyber warfare is now upon us. What we do now and how we determine what we will do in the future is the difference between whether our businesses live or die and whether our digital self survives the digital battlefield. Cyber Warfare – Truth, Tactics, and Strategies takes you on a journey through the myriad of cyber attacks and threats that are present in a world powered by AI, big data, autonomous vehicles, drones video, and social media. Dr. Chase Cunningham uses his military background to provide you with a unique perspective on cyber security and warfare. Moving away from a reactive stance to one that is forward-looking, he aims to prepare people and organizations to better defend themselves in a world where there are no borders or perimeters. He demonstrates how the cyber landscape is growing infinitely more complex and is continuously evolving at the speed of light. The book not only covers cyber warfare, but it also looks at the political, cultural, and geographical influences that pertain to these attack methods and helps you understand the motivation and impacts that are likely in each scenario. Cyber Warfare – Truth, Tactics, and Strategies is as real-life and up-to-date as cyber can possibly be, with examples of actual attacks and defense techniques, tools. and strategies presented for you to learn how to think about defending your own systems and data. What you will learnHacking at scale – how machine learning (ML) and artificial intelligence (AI) skew the battlefieldDefending a boundaryless enterpriseUsing video and audio as weapons of influenceUncovering DeepFakes and their associated attack vectorsUsing voice augmentation for exploitationDefending when there is no perimeterResponding tactically to counter-campaign-based attacksWho this book is for This book is for any engineer, leader, or professional with either a responsibility for cyber security within their organizations, or an interest in working in this ever-growing field.

Intelligence-driven Incident Response - Scott J. Roberts 2016-08-25

Threat intelligence—understanding the who, why, and how of attacks—is most valuable when applied directly to an organization's incident response capability for hunting and investigation. Threat intelligence has become more common and important in recent years. However, many professionals want a better understanding of how to apply this intelligence within their operations and organizations. This book explains the fundamentals of intelligence analysis and the best ways to apply it to your incident response function.

The Secret Team - L. Fletcher Prouty 2011-04-01

With a new foreword by Jesse Ventura: A government insider's shocking exposé of crimes committed by America's intelligence agencies during the Cold War. L. Fletcher Prouty—decorated Air Force officer, former chief of special operations for the Joint Chiefs of Staff under President John F. Kennedy, and the inspiration for “Mr. X” in Oliver Stone's Academy Award-winning film JFK—first published The Secret Team in the 1970s. But virtually all copies of the book disappeared upon distribution, purchased en masse by shady private buyers. Certainly Prouty's amazing allegations—that the U-2 Crisis of 1960 was fixed to sabotage Eisenhower-Khrushchev talks, and that President Kennedy was assassinated to keep the United States, and its defense budget, in Vietnam—cannot have pleased the CIA. Though suppressed (until now), The Secret Team was an important influence for countless works on US government conspiracies, and it raises the same crucial question today that it did on its first appearance: who, in fact, is in control of the United States and the world?

I Know Why the Caged Bird Sings - Maya Angelou 2010-07-21

Here is a book as joyous and painful, as mysterious and memorable, as childhood itself. I Know Why the Caged Bird Sings captures the longing of lonely children, the brute insult of bigotry, and the wonder of words that can make the world right. Maya Angelou's debut memoir is a modern American classic beloved worldwide. Sent by their mother to live with their devout, self-sufficient grandmother in a small Southern town, Maya and her brother, Bailey, endure the ache of abandonment and the prejudice of the local “powhitetrash.” At eight years old and back at her mother’s side in St. Louis, Maya is attacked by a man many times her age—and has to live with the consequences for a lifetime. Years later, in San Francisco, Maya learns that love for herself, the kindness of others, her own strong spirit, and the ideas of great authors (“I met and fell in love with William Shakespeare”) will allow her to be free instead of imprisoned. Poetic and powerful, I Know Why the Caged Bird Sings will touch hearts and change minds for as long as people read. “I Know Why the Caged Bird Sings liberates the reader into life simply because Maya Angelou confronts her own life with such a moving wonder, such a luminous dignity.”—James Baldwin From the Paperback edition.

Security, Privacy, and Digital Forensics in the Cloud - Lei Chen 2019-02-05

In a unique and systematic way, this book discusses the security and privacy aspects of the cloud, and the relevant cloud forensics. Cloud computing is an emerging yet revolutionary technology that has been changing the way people live and work. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue. Written by some of the top experts in the field, this book specifically discusses security and privacy of the cloud, as well as the digital forensics of cloud data, applications, and services. The first half of the book enables readers to have a comprehensive understanding and background of cloud security, which will help them through the digital investigation guidance and recommendations found in the second half of the book. Part One of Security, Privacy and Digital Forensics in the Cloud covers cloud infrastructure security; confidentiality of data; access control in cloud IaaS; cloud security and privacy management; hacking and countermeasures; risk management and disaster recovery; auditing and compliance; and security as a service (SaaS). Part Two addresses cloud forensics – model, challenges, and approaches; cyberterrorism in the cloud; digital forensic process and model in the cloud; data acquisition; digital evidence management, presentation, and court preparation; analysis of digital evidence; and forensics as a service (FaaS). Thoroughly covers both security and privacy of cloud and digital forensics Contributions by top researchers from the U.S., the European and other countries, and professionals active in the field of information and network security, digital and computer forensics, and cloud and big data Of interest to those focused upon security and implementation, and incident management Logical, well-structured, and organized to facilitate comprehension Security, Privacy and Digital Forensics in the Cloud is an ideal book for advanced undergraduate and master's-level students in information systems, information technology, computer and network forensics, as well as computer science. It can also serve as a good reference book for security professionals, digital forensics practitioners and cloud service providers.

Cyber Dragon: Inside China's Information Warfare and Cyber Operations - Dean Cheng 2016-11-14

This book provides a framework for assessing China's extensive cyber espionage efforts and multi-decade modernization of its military, not only identifying the "what" but also addressing the "why" behind China's focus on establishing information dominance as a key component of its military efforts. • Provides a detailed overview and thorough analysis of Chinese cyber activities • Makes extensive use of Chinese-language materials, much of which has not been utilized in the existing Western literature on the subject • Enables a better understanding of Chinese computer espionage by placing it in the context of broader Chinese information warfare activities • Analyzes Chinese military modernization efforts, providing a context for the ongoing expansion in China's military spending and reorganization • Offers readers policy-relevant insight into Chinese military thinking while maintaining academic-level rigor in analysis and source selection

Penetration Testing Azure for Ethical Hackers - David Okeyode 2021-11-25

Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key FeaturesUnderstand the different Azure attack techniques and methodologies used by hackersFind out how you can ensure end-to-end cybersecurity in the Azure ecosystemDiscover various tools and techniques to perform successful penetration tests on your Azure infrastructureBook Description “If you're looking for this book, you need it.” — 5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities, along with extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful penetration tests on your own Azure infrastructure. What you will learnIdentify how administrators misconfigure Azure services, leaving them open to exploitationUnderstand how to detect cloud infrastructure, service, and application misconfigurationsExplore processes and techniques for exploiting common Azure security issuesUse on-premises networks to pivot and escalate access within AzureDiagnose gaps and weaknesses in Azure security implementationsUnderstand how attackers can escalate privileges in Azure ADWho this book is for This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures (TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform (including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

Mein Kampf - Adolf Hitler 2021-03-19

‘MEIN KAMPF’ is the autobiography of Adolf Hitler gives detailed insight into the mission and vision of Adolf Hitler that shook the world. This book is the merger of two volumes. The first volume of MEIN KAMPF’ was written while the author was imprisioned in a Bavarian fortress. The book deals with events which brought the author into this blight. It was the hour of Germany’s deepest humiliation, when Napolean has dismembered the old German Empire and French soldiers occupied almost the whole of Germony. The books narrates how Hitler was arrested with several of his comrades and imprisoned in the fortress of Landsberg on the river Lech. During this period only the author wrote the first volume of MEIN KAMPF. The Second volume of MEIN KAMPF was written after release of Hitler from prison and it was published after the French had left the Ruhr, the tramp of the invading armies still echoed in German ears and the terrible ravages had plunged the country into a state of social and economic Chaos. The beauty of the book is, MEIN KAMPF is an historical document which bears the emprint of its own time. Moreover, Hitler has declared that his acts and ‘public statements’ constitute a partial revision of his book and are to be taken as such. Also, the author has translated Hitler’s ideal, the Volkischer Staat, as the People’s State. The author has tried his best making German Vocabulary easy to understand. You will never be satisfied until go through the whole book. A must read book, which is one of the most widely circulated and read books worldwide.

Working with the Law - Raymond Holliwell 1985-01-03

Science has defined a variety of natural laws that explain the physical world and how it changes. One such law states that for every action there is a reaction, and that for every motion there is corresponding counter-motion. Whether it’s visible to the human eye or not, one thing is certain – movement and change will occur as a result. Having studied these principles, author Raymond Holliwell not only understood the universal physical applications, he also understood the spiritual and mental applications as well. By using this law on a spiritual and mental level, Holliwell found that a specific thought could create a desired reaction in his personal and professional life through continual and dedicated practice. As he came to realize the expanded potential of this powerful law, he eventually recognized the ultimate source of the dramatic results – God.

Adversarial Tradecraft in Cybersecurity - Dan Borges 2021-06-14
Master cutting-edge techniques and countermeasures to protect your organization from live hackers. Learn how to harness cyber deception in your operations to gain an edge over the competition. Key FeaturesGain an advantage against live hackers in a competition or real computing environmentUnderstand advanced red team and blue team techniques with code examplesLearn to battle in short-term memory, whether remaining unseen (red teams) or monitoring an attacker's traffic (blue teams)Book Description Little has been written about what to do when live hackers are on your system and running amok. Even experienced hackers tend to choke up when they realize the network defender has caught them and is zoning in on their implants in real time. This book will provide tips and tricks all along the kill chain of an attack, showing where hackers can have the upper hand in a live conflict and how defenders can outsmart them in this adversarial game of computer cat and mouse. This book contains two subsections in each chapter, specifically focusing on the offensive and defensive teams. It begins by introducing you to adversarial operations and principles of computer conflict where you will explore the core principles of deception, humanity, economy, and more about human-on-human conflicts. Additionally, you will understand everything from planning to setting up infrastructure and tooling that both sides should have in place. Throughout this book, you will learn how to gain an advantage over opponents by disappearing from what they can detect. You will further understand how to blend in, uncover other actors' motivations and means, and learn to tamper with them to hinder their ability to detect your presence. Finally, you will learn how to gain an advantage through advanced research and thoughtfully concluding an operation. By the end of this book, you will have achieved a solid understanding of cyberattacks from both an attacker's and a defender's perspective. What you will learnUnderstand how to implement process injection and how to detect itTurn the tables on the offense with active defenseDisappear on the defender's system, by tampering with defensive sensorsUpskill in using deception with your backdoors and countermeasures including honeypotsKick someone else from a computer you are on and gain the upper handAdopt a language agnostic approach to become familiar with techniques that can be applied to both the red and blue teamsPrepare yourself for real-time cybersecurity conflict by using some of the best techniques currently in the industryWho this book is for Pentesters to red teamers, security operations center analysts to incident responders, attackers, defenders, general hackers, advanced computer users, and security engineers will benefit from this book. Participants in purple teaming or adversarial simulations will also learn a lot from its practical examples of processes for gaining an advantage over the opposing team. Basic knowledge of Python, Go, Bash, PowerShell, system administration as well as knowledge of incident response in Linux and prior exposure to any kind of cybersecurity knowledge, penetration testing, and ethical hacking basics will help you follow along.

The Art of Cyber Leadership - Matt Doan 2018-11-16

Cybersecurity Incident Response - Eric C. Thompson 2018-09-20
Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support. Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each

phase of incident response are explored in the book. Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You’ll Learn Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team Who This Book Is For Cybersecurity leaders, executives, consultants, and entry-level professionals responsible for executing the incident response plan when something goes wrong

Gray Hat Python - Justin Seitz 2009-04-15

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Managing Security with Snort & IDS Tools - Kerry J. Cox 2004-08-02

Intrusion detection is not for the faint at heart. But, if you are a network administrator chances are you're under increasing pressure to ensure that mission-critical systems are safe--in fact impenetrable--from malicious code, buffer overflows, stealth port scans, SMB probes, OS fingerprinting attempts, CGI attacks, and other network intruders.Designing a reliable way to detect intruders before they get in is a vital but daunting challenge. Because of this, a plethora of complex, sophisticated, and pricy software solutions are now available. In terms of raw power and features, SNORT, the most commonly used Open Source Intrusion Detection System, (IDS) has begun to eclipse many expensive proprietary IDSes. In terms of documentation or ease of use, however, SNORT can seem overwhelming. Which output plugin to use? How do you to email alerts to yourself? Most importantly, how do you sort through the immense amount of information Snort makes available to you?Many intrusion detection books are long on theory but short on specifics and practical examples. Not Managing Security with Snort and IDS Tools. This new book is a thorough, exceptionally practical guide to managing network security using Snort 2.1 (the latest release) and dozens of other high-quality open source other open source intrusion detection programs.Managing Security with Snort and IDS Tools covers reliable methods for detecting network intruders, from using simple packet sniffers to more sophisticated IDS (Intrusion Detection Systems) applications and the GUI interfaces for managing them. A comprehensive but concise guide for monitoring illegal entry attempts, this invaluable new book explains how to shut down and secure workstations, servers, firewalls, routers, sensors and other network devices.Step-by-step instructions are provided to quickly get up and running with Snort. Each chapter includes links for the programs discussed, and additional links at the end of the book give administrators access to numerous web sites for additional information and instructional material that will satisfy even the most serious security enthusiasts.Managing Security with Snort and IDS Tools maps out a proactive--and effective--approach to keeping your systems safe from attack.

Digital Forensics and Incident Response - Gerard Johansen 2020-01-29

Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key

Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

The Risk Business - Levi Gundert 2020-02-24

Practical Cyber Intelligence - Wilson Bautista 2018-03-29

Your one stop solution to implement a Cyber Defense Intelligence program in to your organisation. Key Features Intelligence processes and procedures for response mechanisms Master F3EAD to drive processes based on intelligence Threat modeling and intelligent frameworks Case studies and how to go about building intelligent teams Book Description Cyber intelligence is the missing link between your cyber defense operation teams, threat intelligence, and IT operations to provide your organization with a full spectrum of defensive capabilities. This book kicks off with the need for cyber intelligence and why it is required in terms of a defensive framework. Moving forward, the book provides a practical explanation of the F3EAD protocol with the help of examples. Furthermore, we learn how to go about threat models and intelligence products/frameworks and apply them to real-life scenarios. Based on the discussion with the prospective author I would also love to explore the induction of a tool to enhance the marketing feature and functionality of the book. By the end of this book, you will be able to boot up an intelligence program in your organization based on the operation and tactical/strategic spheres of Cyber defense intelligence. What you will learn Learn about the Observe-Orient-Decide-Act (OODA) loop and it's applicability to security Understand tactical view of Active defense concepts and their application in today's threat landscape Get acquainted with an operational view of the F3EAD process to drive decision making within an organization Create a Framework and Capability Maturity Model that integrates inputs and outputs from key functions in an information security organization Understand the idea of communicating with the Potential for Exploitability based on cyber intelligence Who this book is for This book targets incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts; experience in, or knowledge of, security operations, incident responses or investigations is desirable so you can make the most of the subjects presented.