The Art Of Intrusion: The Real Stories Behind The Exploits Of Hackers, Intruders And Deceivers

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

This book is the definitive guide on the OSSEC Host-based Intrusion Detection system and frankly, to really use OSSEC you are going to need a definitive guide. Documentation has been available since the start of the OSSEC project but, due to time constraints, no formal book has been created to outline the various features and functions of the OSSEC product. This has left very important and powerful features of the product undocumented...until now! The book you are holding will show you how to install and configure OSSEC on the operating system of your choice and provide detailed examples to help prevent and mitigate attacks on your systems. -- Stephen Northcutt OSSEC determines if a host has been compromised in this manner by taking the equivalent of a picture of the host machine in its original, unaltered state. This "picture" captures the most relevant information about that machine's configuration. OSSEC saves this "picture" and then constantly compares it to the current state of that machine to identify anything that may have changed from the original configuration. Now, many of these changes are necessary, harmless, and authorized, such as a system administrator installing a new software upgrade, patch, or application. But, then there are the not-so-harmless changes, like the installation of a rootkit, trojan horse, or virus. Differentiating between the harmless and the not-so-harmless changes determines whether the system administrator or security professional is managing a secure, efficient network or a compromised network which might be funneling credit card numbers out to phishing gangs or storing massive amounts of pornography creating significant liability for that organization. Separating the wheat from the chaff is by no means an easy task. Hence the need for this book. The book is co-authored by Daniel Cid, who is the founder and lead developer of the freely available OSSEC host-based IDS. As such, readers can be certain they are reading the most accurate, timely, and insightful information on OSSEC. * Nominee for Best Book Bejtlich read in 2008! * http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html • Get Started with OSSEC Get an overview of the features of OSSEC including commonly used terminology, pre-install preparation, and deployment considerations. • Follow Steb-by-Step Installation Instructions Walk through the installation process for the "local , “agent , and "server" install types on some of the most popular operating systems available. • Master Configuration Learn the basic configuration options for your install type and learn how to monitor log files, receive remote messages, configure email notification, and configure alert levels. • Work With Rules Extract key information from logs using decoders and how you can leverage rules to alert you of strange occurrences on your network. • Understand System Integrity Check and Rootkit Detection Monitor binary executable files, system configuration files, and the Microsoft Windows registry. • Configure Active Response Configure the active response actions you want and bind the actions to specific rules and sequence of events. • Use the OSSEC Web User Interface Install, configure, and use the community-developed, open source web interface available for OSSEC. • Play in the OSSEC VMware Environment Sandbox • Dig Deep into Data Log Mining Take the “high art of log analysis to the next level by breaking the dependence on the lists of strings or patterns to look for in the logs.

On computer security

The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response

Hacking- The art Of Exploitation

Hardware Hacking

Salinity and Tides in Alluvial Estuaries

Privacy is Power

The Art of Deception

The Art of Memory Forensics

The book describes an integrated theory that links estuary shape to tidal hydraulics, tidal mixing and salt intrusion. The shape of an alluvial estuary is characterised by exponentially varying width and the absence of bottom slope. This topography is closely related to tidal parameters, hydraulic parameters and parameters that describe 1-dimensional mixing and salt intrusion. Starting from the fundamental equations for conservation of mass and momentum, analytical equations are derived that relate the topography to tidal parameters (tidal excursion, phase lag, tidal damping, tidal amplification), wave celerity, lateral and vertical mixing and salt intrusion. The book presents a review of the state of the art, a comprehensive theoretical background and ample case illustrations from all over the world. It provides tools with which human interference in estuary dynamics can be described and predicted, resulting from, for instance: upstream fresh water abstraction, dredging, climate change or sea-level rise. In describing the interactions between tide, topography, water quality and river discharge, it provides useful information for hydraulic engineers, morphologists, ecologists and people concerned with water quality in alluvial estuaries. Although the book can be used as a text book, it is mainly a monograph aimed at graduate students and researchers. * Provides new integrated theory for tidal hydraulics, tidal mixing and salt intrusion in alluvial estuaries * Presents a consistent set of analytical equations to compute tidal movement, tidal mixing and salt intrusion, derived from the fundamental laws of conservation of mass and momentum * Serves as a practical guide with many illustrations of applications in real estuaries

An investigative reporter evaluates the capacity of the international law-enforcement community to combat cybercrime, offering insight into the personalities of online criminals and what motivates their activities.

Provides instructions for using honeypots to impede, trap, or monitor online attackers, and discusses how honeypots can be used, the roles they can play, and legal issues surrounding their use.

This book constitutes the proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection, RAID 2011, held in Menlo Park, CA, USA in September 2011. The 20 papers presented were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on application security; malware; anomaly detection; Web security and social networks; and sandboxing and embedded environments.

The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

Concepts, Methods and Practices

Seawater Intrusion in Coastal Aquifers

Practical Guide to Penetration Testing

Challenges and Solutions

The Hacker Playbook 2

The Art of Intrusion

Research on violence against women tends to focus on topics such as sexual assault and intimate partner violence, arguably to the detriment of investigating men’s violence and intrusion in women’s everyday lives. The reality and possibility of the routine intrusions women experience from men in public space – from unwanted comments, to flashing, following and frottage – are frequently unaddressed in research, as well as in theoretical and policy-based responses to violence against women. Often at their height during women’s adolescence, such practices are commonly dismissed as trivial, relatively harmless expressions of free speech too subjective to be legislated against. Based on original empirical research, this book is the first of its kind to conduct a feminist phenomenological analysis of the experience for women of men’s stranger intrusions in public spaces. It suggests that intrusion from unknown men is a fundamental factor in how women understand and enact their embodied selfhood. This book is essential reading for academics and students involved in the study of violence against women, feminist philosophy, applied sociology, feminist criminology and gender studies.

This book presents state-of-the-art research on intrusion detection using reinforcement learning, fuzzy and rough set theories, and genetic algorithm. Reinforcement learning is employed to incrementally learn the computer network behavior, while rough and fuzzy sets are utilized to handle the uncertainty involved in the detection of traffic anomaly to secure data resources from possible attack. Genetic algorithms make it possible to optimally select the network traffic parameters to reduce the risk of network intrusion. The book is unique in terms of its content, organization, and writing style. Primarily intended for graduate electrical and computer engineering students, it is also useful for doctoral students pursuing research in intrusion detection and practitioners interested in network security and administration. The book covers a wide range of applications, from general computer security to server, network, and cloud security.

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

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

How to Write Better Essays

Handbook of Research on Intrusion Detection Systems

Recent Advances in Intrusion Detection

The Science of Human Hacking

Hacking the Hacker

Learn From the Experts Who Take Down Hackers

Machine Learning Techniques and Analytics for Cloud Security

"If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the $99 to replace it! Install a new iPod battery yourself without Apple's "help" * An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case * Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players * Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development * Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC * Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point * Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader * Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.

Coastal aquifers serve as major sources for freshwater supply in many countries around the world, especially in arid and semi-arid zones. Many coastal areas are also heavily urbanized, a fact that makes the need for freshwater even more acute. Coastal aquifers are highly sensitive to disturbances. Inappropriate management of a coastal aquifer may lead to its destruction as a source for freshwater much earlier than other aquifers which are not connected to the sea. The reason is the threat of seawater intrusion. In many coastal aquifers, intrusion of seawater has become one of the major constraints imposed on groundwater utilization. As sea water intrusion progresses, existing pumping wells, especially those close to the coast, become saline and have to be abandoned. Also, the area above the intruding seawater wedge is lost as a source of natural replenishment to the aquifer. Despite the importance of this subject, so far there does not exist a book that integrates our present knowledge of seawater intrusion, its occurrences, physical mechanism, chemistry, exploration by geo physical and geochemical techniques, conceptual and mathematical modeling, analytical and numerical solution methods, engineering measures of combating seawater intrusion, management strategies, and experience learned from case studies. By presenting this fairly comprehensive volume on the state-of-the-art of knowledge and ex perience on saltwater intrusion, we hoped to transfer this body of knowledge to the geologists, hydrologists, hydraulic engineers, water resources planners, managers, and governmental policy makers, who are engaged in the sustainable development of coastal fresh ground water resources.

With the immense cost savings and scalability the cloud provides, the rationale for building cloud native applications is no longer in question. The real issue is how. With this practical guide, developers will learn about the most commonly used design patterns for building cloud native applications using APIs, data, events, and streams in both greenfield and brownfield development. You'll learn how to incrementally design, develop, and deploy large and effective cloud native applications that you can manage and maintain at scale with minimal cost, time, and effort. Authors Kasun Indrasiri and Sriskandarajah Suhothayan highlight use cases that effectively demonstrate the challenges you might encounter at each step. Learn the fundamentals of cloud native applications Explore key cloud native communication, connectivity, and composition patterns Learn decentralized data management techniques Use event-driven architecture to build distributed and scalable cloud native applications Explore the most commonly used patterns for API management and consumption Examine some of the tools and technologies you'll need for building cloud native systems

Real-world advice on how to be invisible online from "the FBI's most wanted hacker" (Wired). Be online without leaving a trace. Your every step online is being tracked and stored, and your identity literally stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand. In this explosive yet practical book, Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, teaching you "the art of invisibility" -- online and real-world tactics to protect you and your family, using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Kevin Mitnick knows exactly how vulnerabilities can be exploited and just what to do to prevent that from happening. The world's most famous -- and formerly the US government's most wanted -- computer hacker, he has hacked into some of the country's most powerful and seemingly impenetrable agencies and companies, and at one point was on a three-year run from the FBI. Now Mitnick is reformed and widely regarded as the expert on the subject of computer security. Invisibility isn't just for superheroes; privacy is a power you deserve and need in the age of Big Brother and Big Data. "Who better than Mitnick -- internationally wanted hacker turned Fortune 500 security consultant -- to teach you how to keep your data safe?" --Esquire

Prevention and Detection for the Twenty-First Century

Why and How You Should Take Back Control of Your Data

14th International Symposium, RAID 2011, Menlo Park, CA, USA, September 20-21, 2011, Proceedings

Ghost in the Wires

Controlling the Human Element of Security

Virtual Honeypots

OSSEC Host-Based Intrusion Detection Guide

'Insightful and ingenious . . . Intrusion is both horrific and comic, and deals movingly with the consequences of genetic fixes' - GUARDIAN 'Intrusion is a finely-tuned, in-your-face argument of a novel . . . MacLeod will push your buttons - and make you think' - SFX Imagine a near-future city, say London, where medical science has advanced beyond our own and a single-dose pill has been developed that, taken when pregnant, eradicates many common genetic defects from an unborn child. Hope Morrison, mother of a hyperactive four-year-old, is expecting her second child. She refuses to take The Fix, as the pill is known. This divides her family and friends and puts her and her husband in danger of imprisonment or worse. Is her decision a private matter of individual choice, or is it tantamount to willful neglect of her unborn child? A plausible and original novel with sinister echoes of 1984 and Brave New World. Books by Ken MacLeod: Fall Revolution The Star Fraction The Stone Canal The Cassini Division The Sky Road Engines of Light Cosmonaut Keep Dark Light Engine City Corporation Wars Trilogy Dissidence Insurgence Emergence Novels The Human Front Newton's Wake Learning the World The Execution Channel The Restoration Game Intrusion Descent

This indispensable guide takes students through each step of the essay writing process, enabling them to tackle written assignments with confidence. Students will develop their ability to analyse complex concepts, evaluate and critically engage with arguments, communicate their ideas clearly and concisely and generate more ideas of their own. Chapters are short and succinct and cover topics such as reading purposefully, note-taking, essay writing in exams and avoiding plagiarism. Packed with practical activities and handy hints which students can apply to their own writing, this is an ideal resource for students looking to improve the quality and clarity of their academic writing. This book will be a source of guidance and inspiration for students of all disciplines and levels who need to write essays as part of their course. New to this Edition: - Brand new chapters on topics such as learning from feedback, finding your voice and using the right vocabulary - Expanded companion website featuring videos, interactive exercises, sample essays and lecturer resources - Exclusive web-only chapter on improving your memory

Presenting cutting-edge research, Intrusion Detection in Wireless Ad-Hoc Networks explores the security aspects of the basic categories of wireless ad-hoc networks and related application areas. Focusing on intrusion detection systems (IDSs), it explains how to establish security solutions for the range of wireless networks, including mobile ad-hoc networks, hybrid wireless networks, and sensor networks. This edited volume reviews and analyzes state-of-the-art IDSs for various wireless ad-hoc networks. It includes case studies on honesty-based intrusion detection systems, cluster oriented-based intrusion detection systems, and trust-based intrusion detection systems. Addresses architecture and organization issues Examines the different types of routing attacks for WANs Explains how to ensure Quality of Service in secure routing Considers honesty and trust-based IDS solutions Explores emerging trends in WAN security Describes the blackhole attack detection technique Surveying existing trust-based solutions, the book explores the potential of the CORIDS algorithm to provide trust-based solutions for secure mobile applications. Touching on more advanced topics, including security for smart power grids, securing cloud services, and energy-efficient IDSs, this book provides you with the tools to design and build secure next-generation wireless networking environments.

The dramatic true story of the capture of the world's most wanted cyberthief by brilliant computer expert Tsutomu Shimomura, describes Kevin Mitnick's long computer crime spree, which involved millions of dollars in credit card numbers and corporate trade secrets. Reprint. NYT.

How Hackers Became the New Mafia

The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

The Art of Invisibility

A critical analysis of street harassment

Eh

Intrusion Detection and Correlation

A Novel

These essays explicitly confront a particular crisis in postwar art, seeking to examine the assumptions on which the modern commercial and museum gallery was based.

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.

Kat and Scott Hamilton are dealing with the hardest of losses: the death of their only child. While Scott throws himself back into his law practice in Los Angeles, Kat is hesitant to rejoin the workplace and instead spends her days shell-shocked and confused, unable to focus. When an unwelcome face from Kat's past in England emerges--the beautiful and imposing Sarah Cherrington--Kat's marriage is thrown into a tailspin. Now wealthy beyond anything she could have imagined as a girl, Sarah appears to have everything she could need or want. But Sarah has an agenda and she wants one more thing. Soon Kat and Scott are caught up in her devious games and power plays. Against the backdrops of Southern California and Sussex, in spare and haunting prose, Mary McCluskey propels this domestic drama to its chilling conclusion.

The aim of this book is to integrate machine learning approaches to meet various analytical issues in cloud security. Cloud-security with ML has long-standing challenges that require methodological and theoretical handling. The conventional cryptography approach is less applied in resource constrained devices. To solve these issues, machine learning approach may be effectively used in providing security to the vast growing cloud environment. Machine learning algorithms can also be used to meet various cloud security issues, like effective intrusion detection system, zero knowledge authentication system, measures for passive attacks, protocols design, privacy system design and application and many more. This book also contains case study / projects to implement various security features using machine learning algorithms and analytics. This book will provide a learning paradigm in field of Artificial Intelligence and deep learning community with related datasets to help dive deeper into Machine Learning applications in cloud security.

Intrusion Detection in Wireless Ad-Hoc Networks

Detecting Malware and Threats in Windows, Linux, and Mac Memory

Honeypots

The State of the Art in Intrusion Prevention and Detection

Have Fun while Voiding your Warranty

DarkMarket

My Adventures as the World's Most Wanted Hacker

Real-world advice on how to be invisible online from "the FBI's most-wanted hacker" (Wired) Your every step online is being tracked and stored, and your identity easily stolen. Big companies and big governments want to know and exploit what you do, and privacy is can afford or understand. In this explosive yet practical book, computer-security expert Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, and teaches you "the art of invisibility": online and everyday tactics to protect you a using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Invisibility isn't just for superheroes--privacy is a power you deserve a of Big Brother and Big Data.

Meet the world's top ethical hackers and explore the tools of the trade Hacking the Hacker takes you inside the world of cybersecurity to show you what goes on behind the scenes, and introduces you to the men and women on the front lines of this technological arm of the world's top white hat hackers, security researchers, writers, and leaders, describe what they do and why, with each profile preceded by a no-experience-necessary explanation of the relevant technology. Dorothy Denning discusses advanced persistent threats describes how he helped invent public key encryption, Bill Cheswick talks about firewalls, Dr. Charlie Miller talks about hacking cars, and other cybersecurity experts from around the world detail the threats, their defenses, and the tools and techniques they use to th advanced criminals history has ever seen. Light on jargon and heavy on intrigue, this book is designed to be an introduction to the field; final chapters include a guide for parents of young hackers, as well as the Code of Ethical Hacking to help you start your own jou Cybersecurity is becoming increasingly critical at all levels, from retail businesses all the way up to national security. This book drives to the heart of the field, introducing the people and practices that help keep our world secure. Go deep into the world of white hat ha just how critical cybersecurity is Read the stories of some of the world's most renowned computer security experts Learn how hackers do what they do—no technical expertise necessary Delve into social engineering, cryptography, penetration testing, network attack field, cybersecurity is large and multi-faceted—yet not historically diverse. With a massive demand for qualified professional that is only going to grow, opportunities are endless. Hacking the Hacker shows you why you should give the field a closer look.

Discusses the intrusion detection system and explains how to install, configure, and troubleshoot it.

The Art of IntrusionThe Real Stories Behind the Exploits of Hackers, Intruders and DeceiversJohn Wiley & Sons

Hackers

Heroes of the Computer Revolution - 25th Anniversary Edition

Takedown

The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It

Intrusion Prevention Fundamentals

Tracking Hackers

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

“Practical Intrusion Analysis provides a solid fundamental overview of the art and science of intrusion analysis.” –Nate Miller, Cofounder, Stratum Security The Only Definitive Guide to New State-of-the-Art Techniques in Intrusion Detection and Prevention Recently, powerful innovations in intrusion detection and prevention have evolved in response to emerging threats and changing business environments. However, security practitioners have found little reliable, usable information about these new IDS/IPS technologies. In Practical Intrusion Analysis, one of the field’s leading experts brings together these innovations for the first time and demonstrates how they can be used to analyze attacks, mitigate damage, and track attackers. Ryan Trost reviews the fundamental techniques and business drivers of intrusion detection and prevention by analyzing today’s new vulnerabilities and attack vectors. Next, he presents complete explanations of powerful new IDS/IPS methodologies based on Network Behavioral Analysis (NBA), data visualization, geospatial analysis, and more. Writing for security practitioners and managers at all experience levels, Trost introduces new solutions for virtually every environment. Coverage includes Assessing the strengths and limitations of mainstream monitoring tools and IDS technologies Using Attack Graphs to map paths of network vulnerability and becoming more proactive about preventing intrusions Analyzing network behavior to immediately detect polymorphic worms, zero-day exploits, and botnet DoS attacks Understanding the theory, advantages, and disadvantages of the latest Web Application Firewalls Implementing IDS/IPS systems that protect wireless data traffic Enhancing your intrusion detection efforts by converging with physical security defenses Identifying attackers’ “geographical fingerprints” and using that information to respond more effectively Visualizing data traffic to identify suspicious patterns more quickly Revisiting intrusion detection ROI in light of new threats, compliance risks, and technical alternatives Includes contributions from these leading network security experts: Jeff Forristal, a.k.a. Rain Forest Puppy, senior security professional and creator of libwhisker Seth Fogie, CEO, Airscanner USA; leading-edge mobile security researcher; coauthor of Security Warrior Dr. Sushil Jajodia, Director, Center for Secure Information Systems; founding Editor-in-Chief, Journal of Computer Security Dr. Steven Noel, Associate Director and Senior Research Scientist, Center for Secure Information Systems, George Mason University Alex Kirk, Member, Sourcefire Vulnerability Research Team

Businesses in today’s world are adopting technology-enabled operating models that aim to improve growth, revenue, and identify emerging markets. However, most of these businesses are not suited to defend themselves from the cyber risks that come with these data-driven practices. To further prevent these threats, they need to have a complete understanding of modern network security solutions and the ability to manage, address, and respond to security breaches. The Handbook of Research on Intrusion Detection Systems provides emerging research exploring the theoretical and practical aspects of prominent and effective techniques used to detect and contain breaches within the fields of data science and cybersecurity. Featuring coverage on a broad range of topics such as botnet detection, cryptography, and access control models, this book is ideally designed for security analysts, scientists, researchers, programmers, developers, IT professionals, scholars, students, administrators, and faculty members seeking research on current advancements in network security technology.

An Economist BEST BOOK OF THE YEAR As the data economy grows in power, Carissa Véliz exposes how our privacy is eroded by big tech and governments, why that matters and what we can do about it. The moment you check your phone in the morning you are giving away your data. Before you've even switched off your alarm, a whole host of organisations have been alerted to when you woke up, where you slept, and with whom. As you check the weather, scroll through your 'suggested friends' on Facebook, you continually compromise your privacy. Without your permission, or even your awareness, tech companies are harvesting your information, your location, your likes, your habits, and sharing it amongst themselves. They're not just selling your data. They're selling the power to influence you. Even when you've explicitly asked them not to. And it's not just you. It's all your contacts too. Digital technology is stealing our personal data and with it our power to make free choices. To reclaim that power and democracy, we must protect our privacy. What can we do? So much is at stake. Our phones, our TVs, even our washing machines are spies in our own homes. We need new regulation. We need to pressure policy-makers for red lines on the data economy. And we need to stop sharing and to adopt privacy-friendly alternatives to Google, Facebook and other online platforms. Short, terrifying, practical: Privacy is Power highlights the implications of our laid-back attitude to data and sets out how we can take back control. If you liked The Age of Surveillance Capitalism, you'll love Privacy is Power because it provides a philosophical perspective on the politics of privacy, and it offers a very practical outlook, both for policymakers and ordinary citizens.

The Cuckoo's Egg

Inside the White Cube

The Ideology of the Gallery Space, Expanded Edition

From Botnet Tracking to Intrusion Detection

Intrusion Detection

Tracking a Spy Through the Maze of Computer Espionage

Design Patterns for Cloud Native Applications

Honeypots have demonstrated immense value in Internet security, but physical honeypot deployment can be prohibitively complex, time-consuming, and expensive. Now, there’s a breakthrough solution. Virtual honeypots share many attributes of traditional honeypots, but you can run thousands of them on a single system-making them easier and cheaper to build, deploy, and maintain. In this hands-on, highly accessible book, two leading honeypot pioneers systematically introduce virtual honeypot technology. One step at a time, you’ll learn exactly how to implement, configure, use, and maintain virtual honeypots in your own environment, even if you’ve never deployed a honeypot before. You’ll learn through examples, including Honeyd, the acclaimed virtual honeypot created by coauthor Niels Provos. The authors also present multiple real-world applications for virtual honeypots, including network decoy, worm detection, spam prevention, and network simulation. After reading this book, you will be able to Compare high-interaction honeypots that provide real systems and services and the low-interaction honeypots that emulate them Install and configure Honeyd to simulate multiple operating systems, services, and network environments Use virtual honeypots to capture worms, bots, and other malware Create high-performance "hybrid" honeypots that draw on technologies from both low- and high-interaction honeypots Implement client honeypots that actively seek out dangerous Internet locations Understand how attackers identify and circumvent honeypots Analyze the botnets your honeypot identifies, and the malware it captures Preview the future evolution of both virtual and physical honeypots

Details how intrusion detection works in network security with comparisons to traditional methods such as firewalls and cryptography Analyzes the challenges in interpreting and correlating Intrusion Detection alerts

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.

Practical Intrusion Analysis

The Art of Human Hacking

Intrusion Detection with Snort

Men's Intrusion, Women's Embodiment

A Data Mining Approach

Intrusion

Social Engineering

The State of the Art in Intrusion Prevention and Detection analyzes the latest trends and issues surrounding intrusion detection systems in computer networks, especially in communications networks. Its broad scope of coverage includes wired, wireless, and mobile networks; next-generation converged networks; and intrusion in social networks. Presenting cutting-edge research, the book presents novel schemes for intrusion detection and prevention. It discusses tracing back mobile attackers, secure routing with intrusion prevention, anomaly detection, and AI-based techniques. It also includes information on physical intrusion in wired and wireless networks and agent-based intrusion surveillance, detection, and prevention. The book contains 19 chapters written by experts from 12 different countries that provide a truly global perspective. The text begins by examining traffic analysis and management for intrusion detection systems. It explores honeypots, honeynets, network traffic analysis, and the basics of outlier detection. It talks about different kinds of IDSs for different infrastructures and considers new and emerging technologies such as smart grids, cyber physical systems, cloud computing, and hardware techniques for high performance intrusion detection. The book covers artificial intelligence-related intrusion detection techniques and explores intrusion tackling mechanisms for various wireless systems and networks, including wireless sensor networks, WiFi, and wireless automation systems. Containing some chapters written in a tutorial style, this book is an ideal reference for graduate students, professionals, and researchers working in the field of computer and network security.

In this "intriguing, insightful and extremely educational" novel, the world's most famous hacker teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data (Frank W. Abagnale). Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and no matter how fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. As the FBI's net finally began to tighten, Mitnick went on the run, engaging in an increasingly sophisticated game of hide-and-seek that escalated through false identities, a host of cities, and plenty of close shaves, to an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escapes -- and a portrait of a visionary who forced the authorities to rethink the way they pursued him, and forced companies to rethink the way they protect their most sensitive information. "Mitnick manages to make breaking computer code sound as action-packed as robbing a bank." -- NPR

Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker’s repertoire—why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the “system” in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer’s bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don’t work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer’s playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.