Investigator S Guide To Steganography

Divided into two major parts, Enhancing Computer Security with Smart Technology introduces the problems of computer security to researchers with a machine learning background, then introduces machine learning concepts to computer security professionals. Realizing the massive scope of these subjects, the author concentrates on problems related to the detection of intrusions through the application of machine learning methods and on the practical algorithmic aspects of machine learning and its role in security. A collection of tutorials that draw from a broad spectrum of viewpoints and experience, this volume is made up of chapters written by specialists in each subject field. It is accessible to any professional with a basic background in computer science. Following an introduction to the issue of cyber-security and cyber-trust, the book offers a broad survey of the state-of-the-art in firewall technology and of the importance of Web application security. The remainder of the book focuses on the use of machine learning methods and tools and their performance.

HIPAA is very complex. So are the privacy and security initiatives that must occur to reach and maintain HIPAA compliance. Organizations need a quick, concise reference in order to meet HIPAA requirements and maintain ongoing compliance. The Practical Guide to HIPAA Privacy and Security Compliance is a one-stop resource for real-world HIPAA.

“This book contains some of the most up-to-date information available anywhere on a wide variety of topics related to Techno Security. As you read the book, you will notice that the authors took the approach of identifying some of the risks, threats, and vulnerabilities and then discussing the countermeasures to address them. Some of the topics and thoughts discussed
here are as new as tomorrow’s headlines, whereas others have been around for decades without being properly addressed. I hope you enjoy this book as much as we have enjoyed working with the various authors and friends during its development. —Donald Withers, CEO and Cofounder of TheTrainingCo. • Jack Wiles, on Social Engineering offers up a potpourri of tips, tricks, vulnerabilities, and lessons learned from 30-plus years of experience in the worlds of both physical and technical security. • Russ Rogers on the Basics of Penetration Testing illustrates the standard methodology for penetration testing: information gathering, network enumeration, vulnerability identification, vulnerability exploitation, privilege escalation, expansion of reach, future access, and information compromise. • Johnny Long on No Tech Hacking shows how to hack without touching a computer using tailgating, lock bumping, shoulder surfing, and dumpster diving. • Phil Drake on Personal, Workforce, and Family Preparedness covers the basics of creating a plan for you and your family, identifying and obtaining the supplies you will need in an emergency. • Kevin O’Shea on Seizure of Digital Information discusses collecting hardware and information from the scene. • Amber Schroader on Cell Phone Forensics writes on new methods and guidelines for digital forensics. • Dennis O’Brien on RFID: An Introduction, Security Issues, and Concerns discusses how this well-intended technology has been eroded and used for fringe implementations. • Ron Green on Open Source Intelligence details how a good Open Source Intelligence program can help you create leverage in negotiations, enable smart decisions regarding the selection of goods and services, and help avoid pitfalls and hazards. • Raymond Blackwood on Wireless Awareness: Increasing the Sophistication of Wireless Users maintains it is the technologist’s responsibility to educate, communicate, and support users despite their lack of interest in understanding how
it works. • Greg Kipper on What is Steganography? provides a solid understanding of the basics of steganography, what it can and can’t do, and arms you with the information you need to set your career path. • Eric Cole on Insider Threat discusses why the insider threat is worse than the external threat and the effects of insider threats on a company. Internationally known experts in information security share their wisdom Free pass to Techno Security Conference for everyone who purchases a book—$1,200 value Today, the scope of image processing and recognition has broadened due to the gap in scientific visualization. Thus, new imaging techniques have developed, and it is imperative to study this progression for optimal utilization. Advanced Image Processing Techniques and Applications is an essential reference publication for the latest research on digital image processing advancements. Featuring expansive coverage on a broad range of topics and perspectives, such as image and video steganography, pattern recognition, and artificial vision, this publication is ideally designed for scientists, professionals, researchers, and academicians seeking current research on solutions for new challenges in image processing. Since 1993, the Information Security Management Handbook has served not only as an everyday reference for information security practitioners but also as an important document for conducting the intense review necessary to prepare for the Certified Information System Security Professional (CISSP) examination. Now completely revised and updated and in its fifth edition, the handbook maps the ten domains of the Information Security Common Body of Knowledge and provides a complete understanding of all the items in it. This is a ...must have... book, both for preparing for the CISSP exam and as a comprehensive, up-to-date reference.
Since 1993, the Information Security Management Handbook has served not only as an everyday reference for information security practitioners but also as an important document for conducting the intense review necessary to prepare for the Certified Information System Security Professional (CISSP) examination. Now completely revised and updated and investigating Guide to Steganography CRC Press

Information Security Policies and Procedures: A Practitioner’s Reference, Second Edition illustrates how policies and procedures support the efficient running of an organization. This book is divided into two parts, an overview of security policies and procedures, and an information security reference guide. This volume points out how securi

A successor to the popular Artech House title Information Hiding Techniques for Steganography and Digital Watermarking, this comprehensive and up-to-date new resource gives the reader a thorough review of steganography, digital watermarking and media fingerprinting with possible applications to modern communication, and a survey of methods used to hide information in modern media. This book explores Steganography, as a means by which two or more parties may communicate using invisible or subliminal communication. "Steganalysis" is described as methods which can be used to break steganographic communication. This comprehensive resource also includes an introduction to watermarking and its methods, a means of hiding copyright data in images and discusses components of commercial multimedia applications that
are subject to illegal use. This book demonstrates a working knowledge of
watermarking’s pros and cons, and the legal implications of watermarking and
copyright issues on the Internet.
With the recent Electronic Signatures in Global and National Commerce Act,
public key cryptography, digital signatures, and digital certificates are finally
emerging as a ubiquitous part of the Information Technology landscape. Although
these technologies have been around for over twenty years, this legislative move
will surely boost e-commerce act
The risk management process supports executive decision-making, allowing
managers and owners to perform their fiduciary responsibility of protecting the
assets of their enterprises. This crucial process should not be a long, drawn-out
affair. To be effective, it must be done quickly and efficiently. Information Security
Risk Analysis, Second Edition enables CIOs, CSOs, and MIS managers to
understand when, why, and how risk assessments and analyses can be
conducted effectively. This book discusses the principle of risk management and
its three key elements: risk analysis, risk assessment, and vulnerability
assessment. It examines the differences between quantitative and qualitative risk
assessment, and details how various types of qualitative risk assessment can be
applied to the assessment process. The text offers a thorough discussion of
recent changes to FRAAP and the need to develop a pre-screening method for risk assessment and business impact analysis.

Network security is concerned with creating a secure inter-connected network that is designed so that on the one hand, users cannot perform actions that they are not allowed to perform, but on the other hand, can perform the actions that they are allowed to. Network security not only involves specifying and implementing a security policy that describes access control, but also implementing an Intrusion Detection System as a tool for detecting attempted attacks or intrusions by crackers or automated attack tools and identifying security breaches such as incoming shellcode, viruses, worms, malware and trojan horses transmitted via a computer system or network. Today’s computer infrastructure is exposed to several kinds of security threats ranging from virus attacks, unauthorised data access, sniffing and password cracking.

Understanding network vulnerabilities in order to protect networks from external and internal threats is vital to the world’s economy and should be given the highest priority. Computer and network security involves many important and complicated issues and this gathering of scientists will help not only in raising awareness but also in teaching participants the state-of-the-art of security techniques. Topics in network security, information security and coding are
discussed in this volume.
The need for information security management has never been greater. With constantly changing technology, external intrusions, and internal thefts of data, information security officers face threats at every turn. The Information Security Management Handbook on CD-ROM, 2006 Edition is now available. Containing the complete contents of the Information Security Management Handbook, this is a resource that is portable, linked and searchable by keyword. In addition to an electronic version of the most comprehensive resource for information security management, this CD-ROM contains an extra volume's worth of information that is not found anywhere else, including chapters from other security and networking books that have never appeared in the print editions. Exportable text and hard copies are available at the click of a mouse. The Handbook's numerous authors present the ten domains of the Information Security Common Body of Knowledge (CBK) ®. The CD-ROM serves as an everyday reference for information security practitioners and an important tool for any one preparing for the Certified Information System Security Professional (CISSP) ® examination. New content to this Edition: Sensitive/Critical Data Access Controls Role-Based Access Control Smartcards A Guide to Evaluating Tokens Identity Management-Benefits and Challenges An Examination of Firewall Architectures The Five "W's"
Effective security rules and procedures do not exist for their own sake—they are put in place to protect critical assets, thereby supporting overall business objectives. Recognizing security as a business enabler is the first step in building a successful program. Information Security Fundamentals allows future security professionals to gain a solid understanding of the foundations of the field and the entire range of issues that practitioners must address. This book enables students to understand the key elements that comprise a successful information security program and eventually apply these concepts to their own efforts. The book examines the elements of computer security, employee roles and responsibilities, and common threats. It examines the need for management controls, policies and procedures, and risk analysis, and also presents a comprehensive list of tasks and objectives that make up a typical information protection program. The volume discusses organizationwide policies and their
documentation, and legal and business requirements. It explains policy format, focusing on global, topic-specific, and application-specific policies. Following a review of asset classification, the book explores access control, the components of physical security, and the foundations and processes of risk analysis and risk management. Information Security Fundamentals concludes by describing business continuity planning, including preventive controls, recovery strategies, and ways to conduct a business impact analysis.

A comprehensive security patch management process is one of the fundamental security requirements for any IT-dependent organization. Fully defining this process ensures that patches are deployed in an organized, staged manner, resulting in little or no slowdowns or downtime to network infrastructure. Until now, there were no technical books for com

Investigators within the law enforcement and cyber forensics communities are generally aware of the concept of steganography, but their levels of expertise vary dramatically depending upon the incidents and cases that they have been exposed to. Now there is a book that balances the playing field in terms of awareness, and serves as a valuable reference source for the tools and techniques of steganography. The Investigator's Guide to Steganography provides a comprehensive look at this unique form of hidden communication from its earliest beginnings to its most modern uses. The book begins
by exploring the past, providing valuable insight into how this method of communication began and evolved from ancient times to the present day. It continues with an in-depth look at the workings of digital steganography and watermarking methods, available tools on the Internet, and a review of companies who are providing cutting edge steganography and watermarking services. The third section builds on the first two by outlining and discussing real world uses of steganography from the business and entertainment to national security and terrorism. The book concludes by reviewing steganography detection methods and what can be expected in the future. It is an informative and entertaining resource that effectively communicates a general understanding of this complex field.

Managing an Information Security and Privacy Awareness and Training Program provides a starting point and an all-in-one resource for infosec and privacy education practitioners who are building programs for their organizations. The author applies knowledge obtained through her work in education, creating a comprehensive resource of nearly everything involved with managing an infosec and privacy training course. This book includes examples and tools from a wide range of businesses, enabling readers to select effective components that will be beneficial to their enterprises. The text progresses from the inception of an education program through development, implementation, delivery, and evaluation.

Among the features that make Noiseless Steganography: The Key to Covert
Communications a first of its kind: The first to comprehensively cover Linguistic Steganography The first to comprehensively cover Graph Steganography The first to comprehensively cover Game Steganography Although the goal of steganography is to prevent adversaries from suspecting the existence of covert communications, most books on the subject present outdated steganography approaches that are detectable by human and/or machine examinations. These approaches often fail because they camouflage data as a detectable noise by altering digital images, audio files, text, etc. However, such alteration raises suspicion and makes the message discernible by detecting its noise. Addressing such shortcomings, Noiseless Steganography: The Key to Covert Communications introduces a novel Noiseless Steganography Paradigm (Nostega). Rather than hiding data in noise or producing noise, Nostega camouflages messages as well as their transmission in the form of unquestionable data in the generated steganographic cover. The book explains how to use Nostega to determine suitable domains capable of generating unsuspicious steganographic cover in which messages are embedded in the form of innocent data that is compatible with the chosen domain. It presents a number of Nostega-based methodologies, including but not limited to: A novel cover type that enables data to be hidden in plotted graphs A novel methodology that pursues popular games such as chess, checkers, crosswords, and dominoes to conceal messages Comprehensive coverage of linguistic steganography Several novel linguistic steganography methodologies based on Natural
Language Processing and Computational Linguistic techniques such as: Education-Centric-Based, Summarization-Based, Natural Language Generation Based, Random-Series-Based, Email Headers Based, Automatic Joke Generation Based, List-Based, and Automatic Notes Generation Based. The first book to provide comprehensive coverage of Linguistic Steganography, Graph Steganography, and Game Steganography, it discusses the implementation and steganalysis validation of ten Nostega-based methodologies. It describes how to establish covert channels by employing the selected domain to serve as justification for the interaction and delivery of the cover among the communicating parties. Instead of using contemporary steganography approaches to camouflage your data as noise that is assumed to look innocent, the text provides you with the tools to prevent your adversaries from suspecting the existence of covert communications altogether.

Building and Implementing a Security Certification and Accreditation Program: Official (ISC)² Guide to the CAP CBK demonstrates the practicality and effectiveness of certification and accreditation (C&A) as a risk management methodology for IT systems in both public and private organizations. It provides security professiona

Virtualization and Forensics: A Digital Forensic Investigators Guide to Virtual Environments offers an in-depth view into the world of virtualized environments and the implications they have on forensic investigations. Named a 2011 Best Digital Forensics Book by InfoSec Reviews, this guide gives you the end-to-end knowledge needed to
identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun. It covers technological advances in virtualization tools, methods, and issues in digital forensic investigations, and explores trends and emerging technologies surrounding virtualization technology. This book consists of three parts. Part I explains the process of virtualization and the different types of virtualized environments. Part II details how virtualization interacts with the basic forensic process, describing the methods used to find virtualization artifacts in dead and live environments as well as identifying the virtual activities that affect the examination process. Part III addresses advanced virtualization issues, such as the challenges of virtualized environments, cloud computing, and the future of virtualization. This book will be a valuable resource for forensic investigators (corporate and law enforcement) and incident response professionals. Named a 2011 Best Digital Forensics Book by InfoSec Reviews Gives you the end-to-end knowledge needed to identify server, desktop, and portable virtual environments, including: VMware, Parallels, Microsoft, and Sun Covers technological advances in virtualization tools, methods, and issues in digital forensic investigations Explores trends and emerging technologies surrounding virtualization technology
Steganography is the art and science of hiding information in inconspicuous cover data so that even the existence of a secret message is kept confidential, and steganalysis is the task of detecting secret messages in covers. This research monograph focuses on the role of cover signals, the distinguishing feature that requires us to treat steganography and steganalysis differently from other secrecy techniques. The main theoretical contribution of the book is a proposal to structure approaches to provably secure steganography according to their implied assumptions on the limits of the adversary and on the nature of covers. A further contribution is the emphasis on dealing with heterogeneity in cover distributions, crucial for security analyses. The author's work complements earlier approaches based on information, complexity, probability and signal processing theory, and he presents numerous practical implications. The scientific advances are supported by a survey of the classical steganography literature; a new proposal for a unified terminology and notation that is maintained throughout the book; a critical discussion of the results achieved and their limitations; and an assessment of the possibility of transferring elements of this research's empirical perspective to other domains in information security. The book is suitable for researchers working in cryptography and information security, practitioners in the corporate and national security domains, and graduate students specializing in multimedia security and data hiding.
Information Security Architecture, Second Edition incorporates the knowledge developed during the past decade that has pushed the information security life cycle from infancy to a more mature, understandable, and manageable state. It simplifies security by providing clear and organized methods and by guiding you to the most effective resources available.

This book comprises select proceedings of the annual convention of the Computer Society of India. Divided into 10 topical volumes, the proceedings present papers on state-of-the-art research, surveys, and succinct reviews. The volume covers diverse topics ranging from information security to cryptography and from encryption to intrusion detection. This book focuses on Cyber Security. It aims at informing the readers about the technology in general and the internet in particular. The book uncovers the various nuances of information security, cyber security and its various dimensions. This book also covers latest security trends, ways to combat cyber threats including the detection and mitigation of security threats and risks. The contents of this book will prove useful to professionals and researchers alike.

Many excellent hardware and software products exist to protect our data communications systems, but security threats dictate that they must be further enhanced. Many laws implemented during the past 15 years have provided law...
enforcement with more teeth to take a bite out of cyber crime, but there is still a need for individuals who know how to investigate computer network security incidents. Organizations demand experts with both investigative talents and a technical knowledge of how cyberspace really works. Cyber Crime Investigator's Field Guide, Second Edition provides the investigative framework that needs to be followed, along with information about how cyberspace works and the tools that reveal the who, what, when, where, why, and how in the investigation of cyber crime. This volume offers a valuable Q&A by subject area, an extensive overview of recommended reference materials, and a detailed case study. Appendices highlight attack signatures, UNIX/Linux commands, Cisco PIX commands, port numbers targeted by trojan horses, and more.

The modern dependence upon information technology and the corresponding information security regulations and requirements force companies to evaluate the security of their core business processes, mission critical data, and supporting IT environment. Combine this with a slowdown in IT spending resulting in justifications of every purchase, and security professionals are forced to scramble to find comprehensive and effective ways to assess their environment in order to discover and prioritize vulnerabilities, and to develop cost-effective solutions that show benefit to the business. A Practical Guide to
Security Assessments is a process-focused approach that presents a structured methodology for conducting assessments. The key element of the methodology is an understanding of business goals and processes, and how security measures are aligned with business risks. The guide also emphasizes that resulting security recommendations should be cost-effective and commensurate with the security risk. The methodology described serves as a foundation for building and maintaining an information security program. In addition to the methodology, the book includes an Appendix that contains questionnaires that can be modified and used to conduct security assessments. This guide is for security professionals who can immediately apply the methodology on the job, and also benefits management who can use the methodology to better understand information security and identify areas for improvement.

This six volume set LNCS 11063 – 11068 constitutes the thoroughly refereed conference proceedings of the 4th International Conference on Cloud Computing and Security, ICCCS 2018, held in Haikou, China, in June 2018. The 386 full papers of these six volumes were carefully reviewed and selected from 1743 submissions. The papers cover ideas and achievements in the theory and practice of all areas of inventive systems which includes control, artificial intelligence, automation systems, computing systems, electrical and informative
systems. The six volumes are arranged according to the subject areas as follows: cloud computing, cloud security, encryption, information hiding, IoT security, multimedia forensics.

Communications represent a strategic sector for privacy protection and for personal, company, national and international security. The interception, damage or lost of information during communication can generate material and non material economic damages from both a personal and collective point of view. The purpose of this book is to give the reader information relating to all aspects of communications security, beginning at the base ideas and building to reach the most advanced and updated concepts. The book will be of interest to integrated system designers, telecommunication designers, system engineers, system analysts, security managers, technicians, intelligence personnel, security personnel, police, army, private investigators, scientists, graduate and postgraduate students and anyone that needs to communicate in a secure way. Assessing and Managing Security Risk in IT Systems: A Structured Methodology builds upon the original McCumber Cube model to offer proven processes that do not change, even as technology evolves. This book enables you to assess the security attributes of any information system and implement vastly improved security environments. Part I delivers an overview of information systems.
security, providing historical perspectives and explaining how to determine the value of information. This section offers the basic underpinnings of information security and concludes with an overview of the risk management process. Part II describes the McCumber Cube, providing the original paper from 1991 and detailing ways to accurately map information flow in computer and telecom systems. It also explains how to apply the methodology to individual system components and subsystems. Part III serves as a resource for analysts and security practitioners who want access to more detailed information on technical vulnerabilities and risk assessment analytics. McCumber details how information extracted from this resource can be applied to his assessment processes. The Wireless Security Handbook provides a well-rounded overview of wireless network security. It examines wireless from multiple perspectives, including those of an auditor, security architect, and hacker. This wide scope benefits anyone who has to administer, secure, hack, or conduct business on a wireless network. This text tackles wirele

Every day millions of people capture, store, transmit, and manipulate digital data. Unfortunately free access digital multimedia communication also provides virtually unprecedented opportunities to pirate copyrighted material. Providing the theoretical background needed to develop and implement advanced techniques
and algorithms, Digital Watermarking and Steganography: Demonstrates how to
develop and implement methods to guarantee the authenticity of digital media
Explains the categorization of digital watermarking techniques based on
characteristics as well as applications Presents cutting-edge techniques such as
the GA-based breaking algorithm on the frequency-domain steganalytic system
The popularity of digital media continues to soar. The theoretical foundation
presented within this valuable reference will facilitate the creation on new
techniques and algorithms to combat present and potential threats against
information security.
This timely textbook presents a comprehensive guide to the core topics in
cybersecurity, covering issues of security that extend beyond traditional computer
networks to the ubiquitous mobile communications and online social networks that have
become part of our daily lives. In the context of our growing dependence on an ever-
changing digital ecosystem, this book stresses the importance of security awareness,
whether in our homes, our businesses, or our public spaces. This fully updated new
edition features new material on the security issues raised by blockchain technology,
and its use in logistics, digital ledgers, payments systems, and digital contracts. Topics
and features: Explores the full range of security risks and vulnerabilities in all connected
digital systems Inspires debate over future developments and improvements necessary
to enhance the security of personal, public, and private enterprise systems Raises thought-provoking questions regarding legislative, legal, social, technical, and ethical challenges, such as the tension between privacy and security Describes the fundamentals of traditional computer network security, and common threats to security Reviews the current landscape of tools, algorithms, and professional best practices in use to maintain security of digital systems Discusses the security issues introduced by the latest generation of network technologies, including mobile systems, cloud computing, and blockchain Presents exercises of varying levels of difficulty at the end of each chapter, and concludes with a diverse selection of practical projects Offers supplementary material for students and instructors at an associated website, including slides, additional projects, and syllabus suggestions This important textbook/reference is an invaluable resource for students of computer science, engineering, and information management, as well as for practitioners working in data- and information-intensive industries.


The Official (ISC)2 Guide to the CISSP-ISSEP CBK provides an inclusive analysis of all
of the topics covered on the newly created CISSP-ISSEP Common Body of Knowledge. The first fully comprehensive guide to the CISSP-ISSEP CBK, this book promotes understanding of the four ISSEP domains: Information Systems Security Engineering (ISSE); Certification.

The investigative experience offers many challenges in reconstructing past events and in discovering the persons, entities, and organizations involved in a crime or a civil wrong. The discussion begins with explaining the nature of cold cases and the major problems associated with these investigations. A cold case investigation progresses from the internal (the case's center), proximal (contact evidence), distal (immediate vicinity) to the limbic (the world at large) realms of information. The text stresses the importance of gathering basic identifiers about the victim, suspect, product, or object that constitutes the case's center of the case. Fifteen keys exist that act as collection points for evidence, and these keys are discussed, including the role they play in the evolution of an investigation. The following topics are featured: identifying the differences between physical evidence, traceable evidence, and information resources; the differences between the goals in criminal cases and in civil investigations; working with the medical examiner; the importance of visiting the locus or crime scene even after a considerable period of time has elapsed; the basics of computer forensics and tips on cyberprofiling; technical assistance and how to locate expert help; tools for uncovering witnesses; locating hidden information archives relevant to a
particular case; financial evidence; managing a case; and response when using a combination of traditional and forensic techniques, which constitutes a modern synthesis of investigative methods. Despite analytical methods, it is necessary to understand when to stop an investigation. The text covers this issue and makes recommendations regarding the writing of reports on a case. The Appendix contains a Master Checklist that provides a wealth of information and expertise. This book will be a valuable resource for police investigators, private investigators, and governmental/regulatory investigators.

Video monitoring has become a vital aspect within the global society as it helps prevent crime, promote safety, and track daily activities such as traffic. As technology in the area continues to improve, it is necessary to evaluate how video is being processed to improve the quality of images. Applied Video Processing in Surveillance and Monitoring Systems investigates emergent techniques in video and image processing by evaluating such topics as segmentation, noise elimination, encryption, and classification. Featuring real-time applications, empirical research, and vital frameworks within the field, this publication is a critical reference source for researchers, professionals, engineers, academicians, advanced-level students, and technology developers.

Whether you are a professional licensed investigator or have been tasked by your employer to conduct an internal investigation, Investigations in the Workplace gives you
a powerful mechanism for engineering the most successful workplace investigations possible. Corporate investigator Eugene Ferraro, CPP, CFE has drawn upon his twenty-four years of practical experience to craft a book that dispels the myths and troublesome theories promulgated by the uninitiated. He provides the back-story behind the methodology, rationale, and gritty practices that have made his workplace investigations soar. But most importantly, he shares this knowledge with you. The book is designed for easy reading and use. Although every page is filled with useful information, you do not need to read the book cover to cover. The exhaustive table of contents, innumerable references, and expansive index allow you to quickly find the immediate information you need. The Applied Strategies chapter shows you how to conduct a particular type of investigation and the action steps involved. To help capture salient points and simplify the learning process, the text is sprinkled with brief Tips and Traps that provide quick and easy lessons on how to make the best use of the information in a particular section. Few workplace activities invoke so much risk and at the same time, so much opportunity, as workplace investigations. A combination of skill, experience, and luck: successful workplace investigations are complex undertakings. An improperly conducted workplace investigation can be expensive and ruin the careers of everyone who touches it. Exploring modern investigative technique and strategies, this book gives you new solutions you need and provides the keys to master even the most complex workplace investigation.
It was an honor and a privilege to chair the 24th IFIP International Information Security Conference (SEC 2009), a 24-year-old event that has become a tradition for formation security professionals around the world. SEC 2009 was organized by the Technical Committee 11 (TC-11) of IFIP, and took place in Pafos, Cyprus, during May 18–20, 2009. It is an indication of good fortune for a Chair to serve a conference that takes place in a country with the natural beauty of Cyprus, an island where the hospitality and friendliness of the people have been going together, hand-in-hand, with its long history. This volume contains the papers selected for presentation at SEC 2009. In response to the call for papers, 176 papers were submitted to the conference. All of them were evaluated on the basis of their novelty and technical quality, and reviewed by at least two members of the conference Program Committee. Of the papers submitted, 39 were selected for presentation at the conference; the acceptance rate was as low as 22%, thus making the conference a highly competitive forum. It is the commitment of several people that makes international conferences possible. That also holds true for SEC 2009. The list of people who volunteered their time and energy to help is really long. There are many books that detail tools and techniques of penetration testing, but none of these effectively communicate how the information gathered from tests should be analyzed and implemented. Until recently, there was very little strategic information available to explain the value of ethical hacking and how tests should be performed in order to provide a company with insight beyond a mere listing of security vulnerabilities.
Now there is a resource that illustrates how an organization can gain as much value from an ethical hack as possible. The Ethical Hack: A Framework for Business Value Penetration Testing explains the methodologies, framework, and "unwritten conventions" that ethical hacks should employ to provide the maximum value to organizations that want to harden their security. This book is unique in that it goes beyond the technical aspects of penetration testing to address the processes and rules of engagement required for successful tests. It examines testing from a strategic perspective, shedding light on how testing ramifications affect an entire organization. Security practitioners can use this resource to reduce their exposure and deliver a focused, valuable service to customers. Organizations will learn how to align the information about tools, techniques, and vulnerabilities that they gathered from testing with their overall business objectives.

Copyright: 361be3adc859dac8cb6b2acfd4f4eb36