Botnets The Killer Web App

This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2012, held in October 2012 in Lafayette, Indiana, USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybercrime investigations.

BotnetsThe Killer Web ApplicationsElsevier

This comprehensive, four-volume reference set on the subject of criminal psychology includes contributions from top scholars and practitioners in the field, explaining new and emerging theory and research in the study of the criminal mind and criminal behavior.

One of the biggest buzzwords in the IT industry for the past few years, virtualization has matured into a practical requirement for many best-practice business scenarios, becoming an invaluable tool for security professionals at companies of every size. In addition to saving time and other resources, virtualization affords unprecedented means for intrusion and malware detection, prevention, recovery, and analysis. Taking a practical approach in a growing market underserved by books, this hands-on title is the first to combine in one place the most important and sought-after uses of virtualization for enhanced security, including sandboxing, disaster recovery and high availability, forensic analysis, and honeypotting. Already gaining buzz and traction in actual usage at an impressive rate, Gartner research indicates that virtualization will be the most significant trend in IT infrastructure and operations over the next four years. A recent report by IT research firm IDC predicts the virtualization services market will grow from $5.5 billion in 2006 to $11.7 billion in 2011. With this growth in adoption, becoming increasingly common even for small and midsize businesses, security is becoming a much more serious concern, both in terms of how to secure virtualization and how virtualization can serve critical security objectives. Titles exist and are on the way to fill the need for securing virtualization, but security professionals do not yet have a book outlining the many security applications of virtualization that will become increasingly important in their job requirements. This book is the first to fill that need, covering tactics such as isolating a virtual environment on the desktop for application testing, creating virtualized storage solutions for immediate disaster recovery and high availability across a network, migrating physical systems to virtual systems for analysis, and creating complete virtual systems to entice hackers and expose potential threats to actual production systems. About the Technologies A sandbox is an isolated environment created to run and test applications that might be a security risk. Recovering a compromised system is as easy as restarting the virtual machine to revert to the point before failure. Employing virtualization on actual production systems, rather than just test environments, yields similar benefits for disaster recovery and high availability. While traditional disaster recovery methods require time-consuming reinstallation of the operating system and applications before restoring data, backing up to a virtual machine makes the recovery process much easier, faster, and efficient. The virtual machine can be restored to same physical machine or an entirely different machine if the original machine has experienced irreparable hardware failure. Decreased downtime translates into higher availability of the system and increased

productivity in the enterprise. Virtualization has been used for years in the field of forensic analysis, but new tools, techniques, and automation capabilities are making it an increasingly important tool. By means of virtualization, an investigator can create an exact working copy of a physical computer on another machine, including hidden or encrypted partitions, without altering any data, allowing complete access for analysis. The investigator can also take a live ?snapshot? to review or freeze the target computer at any point in time, before an attacker has a chance to cover his tracks or inflict further damage.

Network forensics is an evolution of typical digital forensics, in which evidence is gathered from network traffic in near real time. This book will help security and forensics professionals as well as network administrators build a solid foundation of processes and controls to identify incidents and gather evidence from the network.

Forensic scientists and investigators are some of the fastest growing jobs in the United States with over 70,000 individuals employed in 2008. Specifically in the area of cybercrime and digital forensics, the federal government is conducting a talent search for 10,000 qualified specialists. Almost every technology company has developed or is developing a cloud computing strategy. To cut costs, many companies are moving toward network-based applications like SalesForce.com, PeopleSoft, and HR Direct. Every day, we are moving companies' proprietary data into a cloud, which can be hosted anywhere in the world. These companies need to understand how to identify where their data is going and what they are sending. Key network forensics skills and tools are discussed-for example, capturing network traffic, using Snort for network-based forensics, using NetWitness Investigator for network traffic analysis, and deciphering TCP/IP. The current and future states of network forensics analysis tools are addressed. The admissibility of network-based traffic is covered as well as the typical life cycle of a network forensics investigation.

Identity theft has been steadily rising in recent years, and credit card data is one of the number one targets for identity theft. With a few pieces of key information. Organized crime has made malware development and computer networking attacks more professional and better defenses are necessary to protect against attack. The credit card industry established the PCI Data Security standards to provide a baseline expectancy for how vendors, or any entity that handles credit card transactions or data, should protect data to ensure it is not stolen or compromised. This book will provide the information that you need to understand the PCI Data Security standards and how to effectively implement security on the network infrastructure in order to be compliant with the credit card industry guidelines and protect sensitive and personally identifiable information. PCI Data Security standards apply to every company globally that processes or transmits credit card transaction data Information to develop and implement an effective security strategy to keep infrastructures compliant Well known authors have extensive information security backgrounds

Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone. Examining code in past, current, and future risks, protect your banking, auctioning, and other activities performed on mobile devices. * Visual Payloads View attacks as visible to the end user, including notation of

variants. * Timeline of Mobile Hoaxes and Threats Understand the history of major attacks and horizon for emerging threates. * Overview of Mobile Malware Families Identify and understand groups of mobile malicious code and their variations. * Taxonomy of Mobile Malware Bring order to known samples based on infection, distribution, and payload strategies. * Phishing, SMishing, and Vishing Attacks Detect and mitigate phone-based phishing (vishing) and SMS phishing (SMishing) techniques. * Operating System and Device Vulnerabilities Analyze unique OS security issues and examine offensive mobile device threats. * Analyze Mobile Malware Design a sandbox for dynamic software analysis and use MobileSandbox to analyze mobile malware. * Forensic Analysis of Mobile Malware Conduct forensic analysis of mobile devices and learn key differences in mobile forensics. * Debugging and Disassembling Mobile Malware Use IDA and other tools to reverse-engineer samples of malicious code for analysis. * Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

"This set of books represents a detailed compendium of authoritative, research-based entries that define the contemporary state of knowledge on technology"--Provided by publisher.

Essential Computer Security provides the vast home user and small office computer market with the information they must know in order to understand the risks of computing on the Internet and what they can do to protect themselves. Tony Bradley is the Guide for the About.com site for Internet Network Security. In his role managing the content for a site that has over 600,000 page views per month and a weekly newsletter with 25,000 subscribers, Tony has learned how to talk to people, everyday people, about computer security. Intended for the security illiterate, Essential Computer Security is a source of jargon-less advice everyone needs to operate their computer securely. * Written in easy to understand non-technical language that novices can comprehend * Provides detailed coverage of the essential security subjects that everyone needs to know * Covers just enough information to educate without being overwhelming

Following the migration of workflows, data, and communication to the Cloud and other Internet-based frameworks, interaction over the Web has become ever more commonplace. As with any social situation, there are rules and consequences to actions within a virtual environment. Cyber Behavior: Concepts, Methodologies, Tools, and Applications explores the role of cyberspace in modern communication and interaction, including considerations of ethics, crime, security, and education. With chapters on a variety of topics and concerns inherent to a contemporary networked society, this multi-volume work will be of particular interest to students and academicians, as well as software developers, computer scientists, and specialists in the field of Information Technologies.

This timely handbook traces the development of cyber capabilities from their roots in information warfare and cryptology to their potential military application in combat. • Incorporates expertise from diverse viewpoints from the military, government agencies, industry, and academia • Provides an informative timeline of key events in the development of cyber warfare capabilities • Highlights the most prominent and effective cyber attacks in history as well as legal attempts to curb them

This brief provides readers a complete and self-contained resource for information about DDoS attacks and how to defend against them. It presents the latest developments in this increasingly crucial field along with background context and survey material. The book also supplies an overview of DDoS attack issues, DDoS attack detection methods, DDoS attack source traceback, and details on how hackers organize DDoS attacks. The author concludes with future directions of the field, including the impact of DDoS attacks on cloud computing and cloud technology. The concise yet comprehensive nature of this brief makes it an ideal reference for researchers and professionals studying DDoS attacks. It is also a useful resource for graduate students interested in cyberterrorism and networking.

Papers from the conference covering cyberwarfare, malware, strategic information warfare, cyber espionage etc.

Mobile forensics has grown from a relatively obscure tradecraft to a crucial part of many criminal investigations, and is now used daily by examiners and analysts within local, state, and federal law enforcement as well as within the military, US government organizations, and the private “e-Discovery” industry. Developments in forensic research, tools, and processes over the past decade have been very successful and continue to change at a rapid pace. Forensic Investigations and Risk Management in Mobile and Wireless Communications is a collection of innovative research on the methods and applications of analyzing mobile devices and data for collection of information pertaining to the legal evidence related to various security breaches and intrusion detection. While highlighting topics including cybercrime, neural networks, and smartphone security, this book is ideally designed for security analysts, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.

The First International Conference on Digital Forensics and Cyber Crime (ICDF2C) was held in Albany from September 30 to October 2, 2009. The field of digital for- sics is growing rapidly with implications for several fields including law enforcement, network security, disaster recovery and accounting. This is a multidisciplinary area that requires expertise in several areas including, law, computer science, finance, networking, data mining, and criminal justice. This conference brought together pr- titioners and researchers from diverse fields providing opportunities for business and intellectual engagement among attendees. All the conference sessions were very well attended with vigorous discussions and strong audience interest. The conference featured an excellent program comprising high-quality paper pr- entations and invited speakers from all around the world. The first day featured a plenary session including George Philip, President of University at Albany, Harry Corbit, Suprintendent of New York

State Police, and William Pelgrin, Director of New York State Office of Cyber Security and Critical Infrastructure Coordination. An outstanding keynote was provided by Miklos Vasarhelyi on continuous auditing. This was followed by two parallel sessions on accounting fraud /financial crime, and m- timedia and handheld forensics. The second day of the conference featured a mesm- izing keynote talk by Nitesh Dhanjani from Ernst and Young that focused on psyc- logical profiling based on open source intelligence from social network analysis. The third day of the conference featured both basic and advanced tutorials on open source forensics.
Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization, cryptography, system intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless network security, cellular network security, RFID security, and more. Chapters contributed by leaders in the field covering foundational and practical aspects of system and network security, providing a new level of technical expertise not found elsewhere Comprehensive and updated coverage of the subject area allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions
The book begins with real world cases of botnet attacks to underscore the need for action. Next the book will explain botnet fundamentals using real world examples. These chapters will cover what they are, how they operate, and the environment and technology that makes them possible. The following chapters will analyze botnets for opportunities to detect, track, and remove them. Then the book will describe intelligence gathering efforts and results obtained to date. Public domain tools like OurMon, developed by Jim Binkley of Portland State University, will be described in detail along with discussions of other tools and resources that are useful in the fight against Botnets. This is the first book to explain the newest internet threat - Botnets, zombie armies, bot herders, what is being done, and what you can do to protect your enterprise Botnets are the most complicated and difficult threat the hacker world has unleashed - read how to protect yourself
Our world is increasingly driven by sophisticated networks of advanced computing technology, and the basic operation of everyday society is becoming increasingly vulnerable to these networks' shortcomings. The implementation and upkeep of a strong network defense is a substantial challenge, beset not only by economic disincentives but also by an inherent logistical bias that grants advantage to attackers. Research Anthology on Combating Denial-of-Service Attacks examines the latest research on the development of intrusion detection systems and best practices for preventing and combatting cyber-attacks intended to disrupt business and user experience. Highlighting a range of topics such as network administration, application-layer protocols, and malware detection, this publication is an ideal reference source for cybersecurity professionals, IT specialists, policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.
This definitive reference resource on cyber warfare covers all aspects of this headline topic, providing historical context of cyber warfare and an examination its rapid development into a potent technological weapon of the 21st century. • Provides comprehensive coverage of the major individuals, organizations, impacts, and issues related to cyber warfare that enables readers to better understanding of the impact of cyber warfare on modern conflicts • Includes a detailed chronology that documents the evolution and use of cyber warfare over the past few decades • Supplies further readings and a lengthy bibliography that offer a wealth of options to students conducting extensive research on the subject
Guarding against network intrusions requires the monitoring of network traffic for particular

network segments or devices and analysis of network, transport, and application protocols to identify suspicious activity. This chapter provides a detailed discussion of network-based intrusion protection technologies. It contains a brief overview of the major components of network-based intrusion protection systems and explains the architectures typically used for deploying the components. It also examines the security capabilities of the technologies in depth, including the methodologies they use to identify suspicious activity. The rest of the chapter discusses the management capabilities of the technologies and provides recommendations for implementation and operation.

This is a monumental reference for the theory and practice of computer security. Comprehensive in scope, this text covers applied and practical elements, theory, and the reasons for the design of applications and security techniques. It covers both the management and the engineering issues of computer security. It provides excellent examples of ideas and mechanisms that demonstrate how disparate techniques and principles are combined in widely-used systems. This book is acclaimed for its scope, clear and lucid writing, and its combination of formal and theoretical aspects with real systems, technologies, techniques, and policies.

Computer and Information Security Handbook, Third Edition, provides the most current and complete reference on computer security available in one volume. The book offers deep coverage of an extremely wide range of issues in computer and cybersecurity theory, applications, and best practices, offering the latest insights into established and emerging technologies and advancements. With new parts devoted to such current topics as Cloud Security, Cyber-Physical Security, and Critical Infrastructure Security, the book now has 100 chapters written by leading experts in their fields, as well as 12 updated appendices and an expanded glossary. It continues its successful format of offering problem-solving techniques that use real-life case studies, checklists, hands-on exercises, question and answers, and summaries. Chapters new to this edition include such timely topics as Cyber Warfare, Endpoint Security, Ethical Hacking, Internet of Things Security, Nanoscale Networking and Communications Security, Social Engineering, System Forensics, Wireless Sensor Network Security, Verifying User and Host Identity, Detecting System Intrusions, Insider Threats, Security Certification and Standards Implementation, Metadata Forensics, Hard Drive Imaging, Context-Aware Multi-Factor Authentication, Cloud Security, Protecting Virtual Infrastructure, Penetration Testing, and much more. Written by leaders in the field Comprehensive and up-to-date coverage of the latest security technologies, issues, and best practices Presents methods for analysis, along with problem-solving techniques for implementing practical solutions

Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Industrial Electronics, Technology & Automation, Telecommunications and Networking, Systems, Computing Sciences and Software Engineering, Engineering Education, Instructional Technology, Assessment, and E-learning. This book includes the proceedings of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2010). The proceedings are a set of rigorously reviewed world-class manuscripts presenting the state of international practice in Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications.

Many international terrorist groups now actively use computers and the Internet to communicate, and several may develop or acquire the necessary technical skills to direct a co-ordinated attack against computers in the United States. A cyberattack intended to harm the U.S. economy would likely target computers that operate the civilian critical infrastructure and government agencies. However, there is disagreement among some observers about whether a co-

ordinated cyberattack against the U.S. critical infrastructure could be extremely harmful, or even whether computers operating the civilian critical infrastructure actually offer an effective target for furthering terrorists' goals. While there is no published evidence that terrorist organisations are currently planning a co-ordinated attack against computers, computer system vulnerabilities persist world-wide, and initiators of the random cyberattacks that plague computers on the Internet remain largely unknown. Reports from security organisations show that random attacks are now increasingly implemented through use of automated tools, called "bots", that direct large numbers of compromised computers to launch attacks through the Internet as swarms. The growing trend toward the use of more automated attack tools has also overwhelmed some of the current methodologies used for tracking Internet cyberattacks. This book provides background information for three types of attacks against computers (cyberattack, physical attack, and electromagnetic attack), and discusses related vulnerabilities for each type of attack. The book also describes the possible effects of a co-ordinated cyberattack, or computer network attack (CNA), against U.S. infrastructure computers, along with possible technical capabilities of international terrorists. Issues for Congress may include how could trends in cyberattacks be measured more effectively; what is appropriate guidance for DOD use of cyberweapons; should cybersecurity be combined with, or remain separate from, the physical security organization within DHS; how can commercial vendors be encouraged to improve the security of their products; and what are options to encourage U.S. citizens to follow better cybersecurity practices? Appendices to this book describe computer viruses, spyware, and "bot networks", and how malicious programs are used to enable cybercrime and cyberespionage. Also, similarities are drawn between planning tactics currently used by computer hackers and those used by terrorists groups for conventional attacks.

Members of AVIEN (the Anti-Virus Information Exchange Network) have been setting agendas in malware management for several years: they led the way on generic filtering at the gateway, and in the sharing of information about new threats at a speed that even anti-virus companies were hard-pressed to match. AVIEN members represent the best-protected large organizations in the world, and millions of users. When they talk, security vendors listen: so should you. AVIEN’s sister organization AVIEWS is an invaluable meeting ground between the security vendors and researchers who know most about malicious code and anti-malware technology, and the top security administrators of AVIEN who use those technologies in real life. This new book uniquely combines the knowledge of these two groups of experts. Anyone who is responsible for the security of business information systems should be aware of this major addition to security literature. * “Customer Power” takes up the theme of the sometimes stormy relationship between the antivirus industry and its customers, and tries to dispel some common myths. It then considers the roles of the independent researcher,

the vendor-employed specialist, and the corporate security specialist. * “Stalkers on Your Desktop” considers the thorny issue of malware nomenclature and then takes a brief historical look at how we got here, before expanding on some of the malware-related problems we face today. * “A Tangled Web” discusses threats and countermeasures in the context of the World Wide Web. * “Big Bad Bots” tackles bots and botnets, arguably Public Cyber-Enemy Number One. * “Crème de la CyberCrime” takes readers into the underworld of old-school virus writing, criminal business models, and predicting future malware hotspots. * “Defense in Depth” takes a broad look at DiD in the enterprise, and looks at some specific tools and technologies. * “Perilous Outsorcery” offers sound advice on how to avoid the perils and pitfalls of outsourcing, incorporating a few horrible examples of how not to do it. * “Education in Education” offers some insights into user education from an educationalist’s perspective, and looks at various aspects of security in schools and other educational establishments. * “DIY Malware Analysis” is a hands-on, hands-dirty approach to security management, considering malware analysis and forensics techniques and tools. * “Antivirus Evaluation & Testing” continues the D-I-Y theme, discussing at length some of the thorny issues around the evaluation and testing of antimalware software. * “AVIEN & AVIEWS: the Future” looks at future developments in AVIEN and AVIEWS. * Unique, knowledgeable, unbiased and hype-free commentary. * Written by members of the anti-malware community; most malware books are written by outsiders. * Combines the expertise of truly knowledgeable systems administrators and managers, with that of the researchers who are most experienced in the analysis of malicious code, and the development and maintenance of defensive programs.

A guide to low tech computer hacking covers such topics as social engineering, locks, penetration testing, and information security.

This important reference work is an extensive, up-to-date resource for students wanting to immerse themselves in the world of cybercrime, or for those seeking further knowledge of specific attacks both domestically and internationally. Cybercrime is characterized by criminal acts that take place in the borderless digital realm. It takes on many forms, and its perpetrators and victims are varied. From financial theft, destruction of systems, fraud, corporate espionage, and ransoming of information to the more personal, such as stalking and web-cam spying as well as cyberterrorism, this work covers the full spectrum of crimes committed via cyberspace. This comprehensive encyclopedia covers the most noteworthy attacks while also focusing on the myriad issues that surround cybercrime. It includes entries on such topics as the different types of cyberattacks, cybercrime techniques, specific cybercriminals and cybercrime groups, and cybercrime investigations. While objective in its approach, this book does not shy away from covering such relevant, controversial topics as Julian Assange and Russian interference in the 2016 U.S. presidential election. It also provides detailed information on all of the latest developments in this constantly

evolving field. Includes an introductory overview essay that discusses all aspects of cybercrime—how it's defined, how it developed, and its massive expansion in recent years Offers a wide array of entries regarding cybercrime and the many ways it can be committed Explores the largest, most costly cyber attacks on a variety of victims, including corporations, governments, consumers, and individuals Provides up-to-date information on the ever-evolving field of cybercrime

This book constitutes the refereed proceedings of the 7th International Conference on Information Systems Security, ICISS 2011, held in Kolkata, India, in December 2011. The 20 revised full papers presented together with 4 short papers and 4 invited papers were carefully reviewed and selected from 105 submissions. The papers are organized in topical sections on access control and authorization, malwares and anomaly detection, crypto and steganographic systems, verification and analysis, wireless and mobile systems security, Web and network security.

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. Defend your system against the real threat of computer viruses with help from this comprehensive resource. Up-do-date and informative, this book presents a full-scale analysis on computer virus protection. Through use of case studies depicting actual virus infestations, this guide provides both the technical knowledge and practical solutions necessary to guard against the increasing threat of virus attacks.

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics VII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Forensic Techniques, Fraud and Malware Investigations, Network Forensics, and Advanced Forensic Techniques. This book is the 7th volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of 21 edited papers from the 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, held at the National

Center for Forensic Science, Orlando, Florida, USA in the spring of 2011. Advances in Digital Forensics VII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson is an Associate Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science at the University of Tulsa, Tulsa, Oklahoma, USA.

A compilation of the fundamental knowledge, skills, techniques, and tools require by all security professionals, Information Security Handbook, Sixth Edition sets the standard on which all IT security programs and certifications are based. Considered the gold-standard reference of Information Security, Volume 2 includes coverage of each domain of the Common Body of Knowledge, the standard of knowledge required by IT security professionals worldwide. In step with the lightening-quick, increasingly fast pace of change in the technology field, this book is updated annually, keeping IT professionals updated and current in their field and on the job.

Contrary to popular belief, there has never been any shortage of Macintosh-related security issues. OS9 had issues that warranted attention. However, due to both ignorance and a lack of research, many of these issues never saw the light of day. No solid techniques were published for executing arbitrary code on OS9, and there are no notable legacy Macintosh exploits. Due to the combined lack of obvious vulnerabilities and accompanying exploits, Macintosh appeared to be a solid platform. Threats to Macintosh's OS X operating system are increasing in sophistication and number. Whether it is the exploitation of an increasing number of holes, use of rootkits for post-compromise concealment or disturbed denial of service, knowing why the system is vulnerable and understanding how to defend it is critical to computer security. Macintosh OS X Boot Process and Forensic Software All the power, all the tools, and all the geekery of Linux is present in Mac OS X. Shell scripts, X11 apps, processes, kernel extensions...it's a UNIX platform....Now, you can master the boot process, and Macintosh forensic software Look Back Before the Flood and Forward Through the 21st Century Threatscape Back in the day, a misunderstanding of Macintosh security was more or less industry-wide. Neither the administrators nor the attackers knew much about the platform. Learn from Kevin Finisterre how and why that has all changed! Malicious Macs: Malware and the Mac As OS X moves further from desktops, laptops, and servers into the world of consumer technology (iPhones, iPods, and so on), what are the implications for the further spread of malware and other security breaches? Find out from David Harley Malware Detection and the Mac Understand why the continuing insistence of vociferous Mac zealots that it "can't happen here" is likely to aid OS X exploitationg Mac OS X for Pen Testers With its BSD roots, super-slick graphical interface, and near-bulletproof reliability, Apple's Mac OS X provides a great platform for pen testing WarDriving

and Wireless Penetration Testing with OS X Configure and utilize the KisMAC WLAN discovery tool to WarDrive. Next, use the information obtained during a WarDrive, to successfully penetrate a customer's wireless network Leopard and Tiger Evasion Follow Larry Hernandez through exploitation techniques, tricks, and features of both OS X Tiger and Leopard, using real-world scenarios for explaining and demonstrating the concepts behind them Encryption Technologies and OS X Apple has come a long way from the bleak days of OS9. THere is now a wide array of encryption choices within Mac OS X. Let Gareth Poreus show you what they are. Cuts through the hype with a serious discussion of the security vulnerabilities of the Mac OS X operating system Reveals techniques by which OS X can be "owned" Details procedures to defeat these techniques Offers a sober look at emerging threats and trends

Internet usage has become a facet of everyday life, especially as more technological advances have made it easier to connect to the web from virtually anywhere in the developed world. However, with this increased usage comes heightened threats to security within digital environments. The Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security identifies emergent research and techniques being utilized in the field of cryptology and cyber threat prevention. Featuring theoretical perspectives, best practices, and future research directions, this handbook of research is a vital resource for professionals, researchers, faculty members, scientists, graduate students, scholars, and software developers interested in threat identification and prevention.

Know how to mitigate and handle ransomware attacks via the essential cybersecurity training in this book so you can stop attacks before they happen. Learn the types of ransomware, distribution methods, internal structure, families (variants), defense strategies, recovery methods, and legal issues related to reporting ransomware incidents to authorities and other affected parties. This book also teaches you how to develop a ransomware incident response plan to minimize ransomware damage and recover normal operations quickly. Ransomware is a category of malware that can encrypt your computer and mobile device files until you pay a ransom to unlock them. Ransomware attacks are considered the most prevalent cybersecurity threats today—the number of new ransomware variants has grown 30-fold since 2015 and they currently account for roughly 40% of all spam messages. Attacks have increased in occurrence from one every 40 seconds to one every 14 seconds. Government and private corporations are targets. Despite the security controls set by organizations to protect their digital assets, ransomware is still dominating the world of security and will continue to do so in the future. Ransomware Revealed discusses the steps to follow if a ransomware infection occurs, such as how to pay the ransom through anonymous payment methods, perform a backup and restore your affected files, and search online to find a decryption tool to unlock (decrypt) your files for free. Mitigation steps are discussed in depth for both

endpoint devices and network systems. What You Will Learn Be aware of how ransomware infects your system Comprehend ransomware components in simple terms Recognize the different types of ransomware families Identify the attack vectors employed by ransomware to infect computer systems Know how to prevent ransomware attacks from successfully comprising your system and network (i.e., mitigation strategies) Know what to do if a successful ransomware infection takes place Understand how to pay the ransom as well as the pros and cons of paying Set up a ransomware response plan to recover from such attacks Who This Book Is For Those who do not specialize in the cybersecurity field (but have adequate IT skills) and want to fully understand the anatomy of ransomware threats. Although most of the book's content will be understood by ordinary computer users, it will also prove useful for experienced IT users aiming to understand the ins and outs of ransomware threats without diving deep into the technical jargon of the internal structure of ransomware.

An all-star cast of authors analyze the top IT security threats for 2008 as selected by the editors and readers of Infosecurity Magazine. This book, compiled from the Syngress Security Library, is an essential reference for any IT professional managing enterprise security. It serves as an early warning system, allowing readers to assess vulnerabilities, design protection schemes and plan for disaster recovery should an attack occur. Topics include Botnets, Cross Site Scripting Attacks, Social Engineering, Physical and Logical Convergence, Payment Card Industry (PCI) Data Security Standards (DSS), Voice over IP (VoIP), and Asterisk Hacking. Each threat is fully defined, likely vulnerabilities are identified, and detection and prevention strategies are considered. Wherever possible, real-world examples are used to illustrate the threats and tools for specific solutions. * Provides IT Security Professionals with a first look at likely new threats to their enterprise * Includes real-world examples of system intrusions and compromised data * Provides techniques and strategies to detect, prevent, and recover * Includes coverage of PCI, VoIP, XSS, Asterisk, Social Engineering, Botnets, and Convergence

How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide

remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambigue d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne. L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

Although surveillance hit the headlines with revelations by Edward Snowden that the National Security Agency had been tracking phone calls worldwide, surveillance of citizens by their governments actually has been conducted for centuries. Only now, with the advent of modern technologies, it has exponentially evolved so that today you can barely step out your door without being watched or recorded in some way. In addition to the political and security surveillance unveiled by the Snowden revelations, think about corporate surveillance: each swipe of your ID card to enter your office is recorded, not to mention your Internet activity. Or economic surveillance: what you buy online or with a credit card is

recorded and your trip to the supermarket is videotaped. Drive through a tollbooth, and your license plate is recorded. Simply walk down a street and your image is recorded again and again and again. Where does this begin and end? In all levels of social structure, from the personal to the political to the economic to the judicial, The SAGE Encyclopedia of Surveillance, Security, and Privacy uncovers and explains how surveillance has come to be an integral part of how our contemporary society operates worldwide and how it impacts our security and privacy Key features include: Approximately 450 signed entries from contributors around the globe Further readings and cross-references conclude each article to guide students further as they explore a topic A Reader's Guide organizes entries by broad thematic areas

Every year, in response to new technologies and new laws in different countries and regions, there are changes to the fundamental knowledge, skills, techniques, and tools required by all IT security professionals. In step with the lightning-quick, increasingly fast pace of change in the technology field, the Information Security Management Handbook, updated yearly, has become the standard on which all IT security programs and certifications are based. It reflects new updates to the Common Body of Knowledge (CBK) that IT security professionals all over the globe need to know. Captures the crucial elements of the CBK Exploring the ten domains of the CBK, the book explores access control, telecommunications and network security, information security and risk management, application security, and cryptography. In addition, the expert contributors address security architecture and design, operations security, business continuity planning and disaster recovery planning. The book also covers legal regulations, compliance, investigation, and physical security. In this anthology of treatises dealing with the management and technical facets of information security, the contributors examine varied topics such as anywhere computing, virtualization, podslurping, quantum computing, mashups, blue snarfing, mobile device theft, social computing, voting machine insecurity, and format string vulnerabilities. Also available on CD-ROM Safeguarding information continues to be a crucial concern of all IT professionals. As new risks threaten the security of our systems, it is imperative that those charged with protecting that information continually update their armor of knowledge to guard against tomorrow’s hackers and software vulnerabilities. This comprehensive Handbook, also available in fully searchable CD-ROM format keeps IT professionals abreast of new developments on the security horizon and reinforces timeless concepts, providing them with the best information, guidance, and counsel they can obtain.

The stories about phishing attacks against banks are so true-to-life, it’s chilling.” --Joel Dubin, CISSP, Microsoft MVP in Security Every day, hackers are devising new ways to break into your network. Do you have what it takes to stop them? Find out in Hacker’s Challenge 3. Inside, top-tier security experts offer 20 brand-new, real-world network security incidents to test your computer forensics and response skills. All the latest hot-button topics are covered, including phishing

and pharming scams, internal corporate hacking, Cisco IOS, wireless, iSCSI storage, VoIP, Windows, Mac OS X, and UNIX/Linux hacks, and much more. Each challenge includes a detailed explanation of the incident--how the break-in was detected, evidence and clues, technical background such as log files and network maps, and a series of questions for you to solve. In Part II, you'll get a detailed analysis of how the experts solved each incident.