Sec506 Securing Linux Unix Sans

The book you have been waiting for to make you a Master of TShark Network Forensics, is finally here!!! Be it you are a Network Engineer, a Network Forensics Analyst, someone new to packet analysis or someone who occasionally looks at packet, this book is guaranteed to improve your TShark skills, while moving you from Zero to Hero. Mastering TShark Network Forensics, can be considered the definitive repository of practical TShark knowledge. It is your one-stop shop for all you need to master TShark, with adequate references to allow you to go deeper on peripheral topics if you so choose. Book Objectives: Introduce packet capturing architecture Teach the basics of TShark Teach some not so basic TShark tricks Solve real world challenges with TShark Identify services hiding behind other protocols Perform "hands-free" packet capture with TShark Analyze and decrypt TLS encrypted traffic Analyze and decrypt WPA2 Personal Traffic Going way beyond - Leveraging TShark and Python for IP threat intelligence Introduce Lua scripts Introduce packet editing Introduce packet merging Introduce packet rewriting Introduce remote packet capturing Who is this book for?While this book is written specifically for Network Forensics Analysts, it is equally beneficial to anyone who supports the network infrastructure. This means, Network Administrators, Security Specialists, Network Engineers, etc., will all benefit from this book. Considering the preceding, I believe the following represents the right audience for this book: Individuals starting off their Cybersecurity careers Individuals working in a Cyber/Security Operations Center (C/SOC) General practitioners of Cybersecurity Experienced Cybersecurity Ninjas who may be looking for a trick or two Anyone who just wishes to learn more about TShark and its uses in network forensics Anyone involved in network forensics More importantly, anyhow who is looking for a good read Not sure if this book is for you? Take a glimpse at the sample chapter before committing to it. Mastering TShark sample chapters can be found at: https: //bit.ly/TShark All PCAPS used within this book can be found at: https: //github.com/SecurityNik/SUWtHEh- As an addition to this book, the tool, pktIntel: Tool used to perform threat intelligence against packet data can be found at: https: //github.com/SecurityNik/pktIntel
This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.
Digital Crime and Forensic Science in CyberspaceIGI Global
Recent corporate events have exposed the frequency and consequences of poor system security implementations and inadequate protection of private information. In a world of increasingly complex computing environments, myriad compliance regulations and the soaring costs of security breaches, it is economically essential for companies to become proactive in implementing effective system and data security measures. This volume is a comprehensive reference for understanding security risks, mitigations and best practices as they apply to the various components of these business-critical computing environments. HP NonStop Servers are used by Financial, Medical, Manufacturing enterprises where there can be no down time. Securing HP NonStop Servers in an Open Systems World: OSS, TCP/IP, and SQL takes a wide angle view of NonStop Server use. This book addresses protection of the Open Systems Services environment, network interfaces including TCP/IP and standard SQL databases. It lays out a roadmap of changes since our first book HP has made to Safeguard, elaborating on the advantages and disadvantages of implementing each new version. Even the security aspects of managing Operating System upgrades are given attention. Auditors, security policy makers, information security administrators and system managers will find the practical information they need for putting security principles into practice to meet industry standards as well as compliance regulations. * Addresses security issues in Open Systems Services * Critical security topics for network interfaces TCP/IP, SQL, etc. * Updates to safeguard thru since publication of XYPRO's last book
Inside Network Perimeter Security
Fifth Edition
HCNA Networking Study Guide
Phenomena, Challenges and Legal Response
Prevention and Detection of Cyber Crimes
Official (ISC)2® Guide to the CISSP®-ISSEP® CBK®
Securing virtual environments for VMware, Citrix, and Microsoft hypervisors Virtualization changes the playing field when it comes to security. There are new attack vectors, new operational patterns and complexity, and changes in IT architecture and deployment life cycles. What's more, the technologies, best practices, and strategies used for securing physical environments do not provide sufficient protection for virtual environments. This book includes step-by-step configurations for the security controls that come with the three leading hypervisor--VMware vSphere and ESXi, Microsoft Hyper-V on Windows Server 2008, and Citrix XenServer. Includes strategy for securely implementing network policies and integrating virtual networks into the existing physical infrastructure Discusses vSphere and Hyper-V native virtual switches as well as the Cisco Nexus 1000v and Open vSwitch switches Offers effective practices for securing virtual machines without creating additional operational overhead for administrators Contains methods for integrating virtualization into existing workflows and creating new policies and processes for change and configuration management so that virtualization can help make these critical operations processes more effective This must-have resource offers tips and tricks for improving disaster recovery and business continuity, security-specific scripts, and examples of how Virtual Desktop Infrastructure benefits security.
This timely book provides contributions on international, comparative crime phenomena: gangs, trafficking, fear of crime, and crime prevention. It highlights contributions originally prepared for the XVII World Congress of Criminology and for the 2015 Cybercrime Conference in Oñati, Spain which have been selected, reviewed, and adapted for inclusion in this volume. The work features international contributors sharing the latest research and approaches from a variety of global regions. The first part examines the impact of gangs on criminal activities and violence. The second part explores illegal trafficking of people, drugs, and other illicit goods as a global phenomenon, aided by the ease of international travel, funds transfer, and communication. Finally, international approaches to crime detection prevention are presented. The work provides case studies and fieldwork that will be relevant across a variety of disciplines and a rich resource for future

research. This work is relevant for researchers in criminology and criminal justice, as well as related fields such as international and comparative law, public policy, and public health.
The DISASTER RECOVERY/VIRTUALIZATION SECURITY SERIES is comprised of two books that are designed to fortify disaster recovery preparation and virtualization technology knowledge of information security students, system administrators, systems engineers, enterprise system architects, and any IT professional who is concerned about the integrity of their network infrastructure. Topics include disaster recovery planning, risk control policies and countermeasures, disaster recovery tools and services, and virtualization principles. The series when used in its entirety helps prepare readers to take and succeed on the E|CDR and E|CVT, Disaster Recovery and Virtualization Technology certification exam from EC-Council. The EC-Council Certified Disaster Recovery and Virtualization Technology professional will have a better understanding of how to set up disaster recovery plans using traditional and virtual technologies to ensure business continuity in the event of a disaster. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.
Becoming an Ethical Hacker
Cybercrime
Cyber Rights
Learning by Practicing - Mastering TShark Network Forensics
Incident Response & Computer Forensics, Third Edition
Hackers

Cybercrime focuses on the growing concern about the use of electronic communication for criminal activities and the appropriateness of the countermeasures that are being adopted by law enforcement agencies, security services and legislators to address such anxieties. Fuelled by sensational media headlines and news coverage which has done much to encourage the belief that technologies like the Internet are likely to lead to a lawless electronic frontier, Cybercrime provides a more considered and balanced perspective on what is an important and contested arena for debate. It looks at: *legislation *electronic criminal behaviour *privacy and liberty *the dangers of surveillance. Cybercrime explains the basic issues surrounding cybercrime and its impact on society.
An acclaimed investigative journalist explores ethical hacking and presents a reader-friendly, informative guide to everything there is to know about entering the field of cybersecurity. It’s impossible to ignore the critical role cybersecurity plays within our society, politics, and the global order. In Becoming an Ethical Hacker, investigative reporter Gary Rivlin offers an easy-to-digest primer on what white hat hacking is, how it began, and where it’s going, while providing vivid case studies illustrating how to become one of these “white hats” who specializes in ensuring the security of an organization’s information systems. He shows how companies pay these specialists to break into their protected systems and networks to test and assess their security. Readers will learn how these white hats use their skills to improve security by exposing vulnerabilities before malicious hackers can detect and exploit them. Weaving practical how-to advice with inspiring case studies, Rivlin provides concrete, practical steps anyone can take to pursue a career in the growing field of cybersecurity.
Provides an overview and case studies of computer crimes and discusses topics including data recovery, evidence collection, preservation of digital evidence, information warfare, and the cyber underground.
Describes various types of malware, including viruses, worms, user-level RootKits, and kernel-level manipulation, their haracteristics and attack method, and how to defend against an attack.
Hands on Hacking
Network Security Bible
Understanding Cybercrime
Hackers Beware
Criminal Justice Resource Manual
Cybercrime, Organized Crime, and Societal Responses

Examines how various security methods are used and how they work, covering options including packet filtering, proxy firewalls, network intrusion detection, virtual private networks, and encryption.
This book is a study guide for Huawei (HCNA) certification. It has been written to help readers understand the principles of network technologies. It covers topics including network fundamentals, Ethernet, various protocols such as those used in routing, and Huawei ’s own VRP operating system—all essential aspects of HCNA certification. Presenting routing and switching basics in depth, it is a valuable resource for information and communications technology (ICT) practitioners, university students and network technology fans.
Tired of playing catchup with hackers? Does it ever seem they have all of the cool tools? Does it seem like defending a network is just not fun? This books introduces new cyber-security defensive tactics to annoy attackers, gain attribution and insight on who and where they are. It discusses how to attack attackers in a way which is legal and incredibly useful.
Techniques of Crime Scene Investigation, Fifth Edition provides field-tested techniques and methods for crime scene investigation and crime detection. The book features methods for using lasers and cyanoacrylate fuming in fingerprint detection, procedures for investigating serial murder cases, and health and safety concerns when dealing with toxic reagents and biological evidence. It also presents a new series of cases to demonstrate the importance of physical evidence, as well as 61 new illustrations.
A Step-by-step Guide to Computer Attacks and Effective Defenses
Protecting Mobile Devices and their Applications

Network Intrusion Detection
Securing HP NonStop Servers in an Open Systems World
Report (to Accompany Treaty Doc. 108-11).
Protecting Virtualized Environments

*The target audience for this book is any IT professional responsible for designing, configuring, deploying or managing information systems. This audience understands that the purpose of ethics in information security is not just morally important; it equals the survival of their business. A perfect example of this is Enron. Enron's ultimate failure due to a glitch in the ethics systems of the business created the most infamous example of an ethics corporate breakdown resulting in disaster. Ethics is no longer a matter of morals anymore when it comes to information security; it is also a matter of success or failure for big business. * This groundbreaking book takes on the difficult ethical issues that IT professional confront every day. * The book provides clear guidelines that can be readily translated into policies and procedures. * This is not a text book. Rather, it provides specific guidelines to System Administrators, Security Consultants and Programmers on how to apply ethical standards to day-to-day operations.*

Cyber attacks are on the rise. The media constantly report about data breaches and increasingly sophisticated cybercrime. Even governments are affected. At the same time, it is obvious that technology alone cannot solve the problem. What can countries do? Which issues can be addressed by policies and legislation? How to draft a good law? The report assists countries in understanding what cybercrime is about, what the challenges are in fighting such crime and supports them in drafting policies and laws.

Hacker Techniques, Tools, and Incident Handling, Third Edition begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. It goes on to review the technical overview of hacking: how attacks target networks and the methodology they follow. The final section studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on the Web. Written by subject matter experts, with numerous real-world examples, Hacker Techniques, Tools, and Incident Handling, Third Edition provides readers with a clear, comprehensive introduction to the many threats on our Internet environment and security and what can be done to combat them.

The Real Cost of Insecure Software • In 1996, software defects in a Boeing 757 caused a crash that killed 70 people… • In 2003, a software vulnerability helped cause the largest U.S. power outage in decades… • In 2004, known software weaknesses let a hacker invade T-Mobile, capturing everything from passwords to Paris Hilton's photos… • In 2005, 23,900 Toyota Priuses were recalled for software errors that could cause the cars to shut down at highway speeds… • In 2006 dubbed "The Year of Cybercrime," 7,000 software vulnerabilities were discovered that hackers could use to access private information… • In 2007, operatives in two nations brazenly exploited software vulnerabilities to cripple the infrastructure and steal trade secrets from other sovereign nations… Software has become crucial to the very survival of civilization. But badly written, insecure software is hurting people–and costing businesses and individuals billions of dollars every year. This must change. In Geekonomics, David Rice shows how we can change it. Rice reveals why the software industry is rewarded for carelessness, and how we can revamp the industry's incentives to get the reliability and security we desperately need and deserve. You'll discover why the software industry still has shockingly little accountability–and what we must do to fix that. Brilliantly written, utterly compelling, and thoroughly realistic, Geekonomics is a long-overdue call to arms. Whether you're software user, decision maker, employee, or business owner this book will change your life…or even save it.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
LSC (GLOBE UNIVERSITY) SD256: VS ePub for Mobile Application Security
The Real Cost of Insecure Software
International Approaches
Counter Hack Reloaded
Computer Crime Scene Investigation

In this text the author looks at the battle between the computer underground and the security industry. He talks to people on both sides of the law about the practicalities, objectives and wider implications of what they do.

Secure today's mobile devices and applications Implement a systematic approach to security in your mobile application development with help from this practical guide. Featuring case studies, code examples, and best practices, Mobile Application Security details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware, and buffer overflow exploits are also covered in this comprehensive resource. Design highly isolated, secure, and authenticated mobile applications Use the Google Android emulator, debugger, and third-party security tools Configure Apple iPhone APIs to prevent overflow and SQL injection attacks Employ private and public key cryptography on Windows Mobile devices Enforce fine-grained security policies using the BlackBerry Enterprise Server Plug holes in Java Mobile Edition, SymbianOS, and WebOS applications Test for XSS, CSRF, HTTP redirects, and phishing attacks on WAP/Mobile HTML applications Identify and eliminate threats from Bluetooth, SMS, and GPS services Himanshu Dwivedi is a co-founder of iSEC Partners (www.isecpartners.com), an information security firm specializing in application security. Chris Clark is a principal security consultant with iSEC Partners. David Thiel is a principal security consultant with iSEC Partners.

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. • An introduction to the same hacking techniques that malicious hackers will use against an organization • Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks • Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written

by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.
The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans
TCP/IP, OSS and SQL
Law in Cyber Space
Digital Crime and Forensic Science in Cyberspace

Computer Forensics
Hacker Techniques, Tools, and Incident Handling
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); Certifica
This guide empowers network and system administrators to defend their information and computing assets--whether or not they have security experience. Skoudis presents comprehensive, insider's explanations of today's most destructive hacker tools and tactics, and specific, proven countermeasures for both UNIX and Windows environments.
The comprehensive A-to-Z guide on network security, fully revised and updated Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security. Covers all core areas of network security and how they interrelate Fully revised to address new techniques, technology, and methods for securing an enterprise worldwide Examines new trends and best practices in use by organizations to secure their enterprises Features additional chapters on areas related to data protection/correlation and forensics Includes cutting-edge topics such as integrated cybersecurity and sections on Security Landscape, with chapters on validating security, data protection, forensics, and attacks and threats If you need to get up to date or stay current on network security, Network Security Bible, 2nd Edition covers everything you need to know.
Law needs to be developed to take advantage of technological improvements and to ensure that states can respond to computer crime and related criminal law issues. This book sets out the reports of two expert working groups.
The Art of Active Defense
Defending Free speech in the Digital Age
Techniques of Crime Scene Investigation
Moving From Zero to Hero
Computer Crime
Council of Europe Convention on Cybercrime (Treaty Doc. 108-11)
The second edition of Kerrs popular computer crimes text reflects the many new caselaw and statutory developments since the publication of the first edition in 2006. It also adds a new section on encryption that covers both Fourth Amendment and Fifth Amendment issues raised by its use to conceal criminal activity. Computer crime law will be an essential area for tomorrow's criminal law practitioners, and this book offers an engaging and user-friendly introduction to the field. It is part traditional casebook, part treatise: It both straightforwardly explains the law and presents many exciting and new questions of law that courts are only now beginning to consider. The book reflects the author's practice experience, as well: Orin Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. No advanced knowledge of computers and the Internet is required or assumed This book covers every aspect of crime in the digital age. Topics range from Internet surveillance law and the Fourth Amendment to computer hacking laws and international computer crimes. More and more crimes involve digital evidence, and computer crime law will be an essential area for tomorrow's criminal law practitioners. Many U.S. Attorney's Offices have started computer crime units, as have many state Attorney General offices, and any student with a background in this emerging area of law will have a leg up on the competition. This is the first law school book dedicated entirely to computer crime law. The materials are authored entirely by Orin Kerr, a new star in the area of criminal law and Internet law who has recently published articles in the Harvard Law Review, Columbia Law Review, NYU Law Review, and Michigan Law Review. The book is filled with ideas for future scholarship, including hundreds of important questions that have never been addressed in the scholarly literature. The book reflects the author's practice experience, as well: Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. Students will find it easy and fun to read, and professors will find it an angaging introduction to a new world of scholarly ideas. The book is ideally suited either for a 2-credit seminar or a 3-credit course, and should appeal both to criminal law professors and those interested in cyberlaw or law and technology. No advanced knowledge of computers and the Internet is required or assumed.
Cybersecurity Operations Handbook is the first book for daily operations teams who install, operate and maintain a range of security technologies to protect corporate infrastructure. Written by experts in security operations, this book provides extensive guidance on almost all aspects of daily operational security, asset protection, integrity management, availability methodology, incident response and other issues that operational teams need to know to properly run security products and services in a live environment. Provides a master document on Mandatory FCC Best Practices and complete coverage of all critical operational procedures for meeting Homeland Security requirements. · First book written for daily operations teams · Guidance on almost all aspects of daily operational security, asset protection, integrity management · Critical information for compliance with Homeland Security
Cybercrime is a complex and ever-changing phenomenon. This book offers a clear and engaging introduction to this fascinating subject by situating it in the wider context of social, political, cultural and economic change. Taking into account recent developments in social

networking and mobile communications, this new edition tackles a range of themes spanning criminology, sociology, law, politics and cultural studies, including: - computer hacking - cyber-terrorism - piracy and intellectual property theft - financial fraud and identity theft - hate speech - internet pornography - online stalking - policing the internet - surveillance and censorship Complete with useful recommendations for further reading, incisive discussion questions and an updated glossary of key terms, Cybercrime and Society is an essential resource for all students and academics interested in cybercrime and the future of the Internet.

"Digital forensics is the science of collecting the evidence that can be used in a court of law to prosecute the individuals who engage in electronic crime"--Provided by publisher.

Security and Surveillance in the Information Age

Cybercrime and Society

Virtualization Security

Crime in the Digital Sublime

Computer Crime Law

Cybersecurity Operations Handbook

The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 9780101674223), and established the Office of Cyber Security to provide strategic leadership across Government. This document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.

The reason as to why I decided to write this book is the fact that many of us lives with a belief that we have only four common domains in this world, which are land, sea, air and outer space. But currently due to the development of science and technology a fifth common domain has been created, and that is cyberspace. This new common domain creates a new environment for the commission of crimes known as cyber crimes. And because of its nature, it became difficult to deal with these natures of crimes. The widespread digital accessibility creates new opportunities for the unprincipled because the manners in which offenders commit crimes changed from traditional to digital means. A lot of currencies are lost by both businesses and consumers to computer-criminals. Fair enough, computers and networks can be used to harass victims or set them up for violent attacks such as to coordinate and carry out terrorist activities that threaten us all. Coming back to our country Tanzania, regrettably in many cases law enforcement institutions have insulated behind these criminals, deficient in the technology and the trained recruits to address this fresh and rising risk. To make things worse, old laws did not fairly prevent the crimes from being committed. Furthermore, new laws had not quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. It is from this book whereby the position of cyber security, prevention and detection in Tanzania against cyber crimes, is determined. Actually, by looking at the Cyber Crime Act No.14 of 2015 on how the concepts above have been provided and implemented. Magalla Jr.Note de l'éditeur (FRENCH):Cet essai juridique en anglais traite du droit des nouvelles technologies de l'information et de la communication (NTIC) en Tanzanie, en particulier de la cybercriminalité, de sa définition, de sa prévention et de sa répression en fonction des formes multiples qu'elle prend dans le cyber espace. Après avoir dépeint le cadre général et international du droit des NTIC, l'auteur va décrire la situation tanzanienne. L'approche se veut à la fois doctrinale et pratique. Les principales sources du droit des NTIC sont décrites et l'ouvrage se termine sur des cas pratiques rencontrés dans des tribunaux tanzaniens.

A first-person account of the fight to preserve First Amendment rights in the digital age. Lawyer and writer Mike Godwin has been at the forefront of the struggle to preserve freedom of speech on the Internet. In Cyber Rights he recounts the major cases and issues in which he was involved and offers his views on free speech and other constitutional rights in the digital age. Godwin shows how the law and the Constitution apply, or should apply, in cyberspace and defends the Net against those who would damage it for their own purposes. Godwin details events and phenomena that have shaped our understanding of rights in cyberspace—including early antihacker fears that colored law enforcement activities in the early 1990s, the struggle between the Church of Scientology and its critics on the Net, disputes about protecting copyrighted works on the Net, and what he calls "the great cyberporn panic." That panic, he shows, laid bare the plans of those hoping to use our children in an effort to impose a new censorship regime on what otherwise could be the most liberating communications medium the world has seen. Most important, Godwin shows how anyone—not just lawyers, journalists, policy makers, and the rich and well connected—can use the Net to hold media and political institutions accountable and to ensure that the truth is known.

IT Ethics Handbook:

A Treatise on the Law of Stock and Stockholders as Applicable to Railroad, Banking, Insurance, Manufacturing, Commercial, Business Turnpike, Bridge, Canal, and Other Private Corporations

Offensive Countermeasures

Topics in Dosimetry & Treatment Planning for Neutron Capture Therapy

Geekonomics

Fighting Malicious Code