

## Principles Information Security Michael Whitman

GUIDE TO NETWORK SECURITY, International Edition is a wide-ranging new text that provides a detailed review of the network security field, including essential terminology, the history of the discipline, and practical techniques to manage implementation of network security solutions. It begins with an overview of information, network, and web security, emphasizing the role of data communications and encryption. The authors then explore network perimeter defense technologies and methods, including access controls, firewalls, VPNs, and intrusion detection systems, as well as applied cryptography in public key infrastructure, wireless security, and web commerce. The final section covers additional topics relevant for information security practitioners, such as assessing network security, professional careers in the field, and contingency planning. Perfect for both aspiring and active IT professionals, GUIDE TO NETWORK SECURITY, International Edition is an ideal resource for readers who want to help organizations protect critical information assets and secure their systems and networks, both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future.

In the Business Continuity State of the Industry Report, authors Herbert Mattord and Michael Whitman provide a comprehensive overview of recent research and news related to business continuity programs. Using the most recent surveys, reports, and research data available, the authors provide an objective analysis of the state of business continuity today. The report covers events that have shaped the industry, including natural, economic, and technological disasters; the perspective of business continuity from top management executives; business continuity job descriptions and compensation data; the legal and regulatory environment; and emerging trends. It brings together what fragmented bits of information are currently available into one easy-to-read document. The Business Continuity State of the Industry Report is a part of Elsevier's Security Executive Council Risk Management Portfolio, a collection of real world solutions and "how-to" guidelines that equip executives, practitioners, and educators with proven information for successful security and risk management programs. Saves you time by bringing together the most important pieces of research and news into one document. Can be used for a quick update on what business continuity programs look like today, what trends exist, and what resources are available for addressing gaps. Includes appendices that cover business continuity key terms, industry events, job descriptions and compensation trend data, and more.

This text provides students with a set of industry focused readings and cases illustrating real-world issues in information security. GUIDE TO NETWORK SECURITY is a wide-ranging new text that provides a detailed review of the network security field, including essential terminology, the history of the discipline, and practical techniques to manage implementation of network security solutions. It begins with an overview of information, network, and web security, emphasizing the role of data communications and encryption. The authors then explore network perimeter defense technologies and methods, including access controls, firewalls, VPNs, and intrusion detection systems, as well as applied cryptography in public key infrastructure, wireless security, and web commerce. The final section covers additional topics relevant for information security practitioners, such as assessing network security, professional careers in the field, and contingency planning. Perfect for both aspiring and active IT professionals, GUIDE TO NETWORK SECURITY is an ideal resource for students who want to help organizations protect critical information assets and secure their systems and networks, both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The frontiers are the future of humanity. Peacefully and sustainably managing them is critical to both security and prosperity in the twenty-first century.

Never HIGHLIGHT a Book Again Virtually all testable terms, concepts, persons, places, and events are included. Cram101 Textbook Outlines gives all of the outlines, highlights, notes for your textbook with optional online practice tests. Only Cram101 Outlines are Textbook Specific. Cram101 is NOT the Textbook. Accompanys: 9780521673761

MANAGEMENT OF INFORMATION SECURITY, Sixth Edition prepares you to become an information security management practitioner able to secure systems and networks in a world where continuously emerging threats, ever-present attacks and the success of criminals illustrate the weaknesses in current information technologies. You'll develop both the information security skills and practical experience that organizations are looking for as they strive to ensure more secure computing environments. The text focuses on key executive and managerial aspects of information security. It also integrates coverage of CISSP and CISM throughout to effectively prepare you for certification. Reflecting the most recent developments in the field, it includes the latest information on NIST, ISO and security governance as well as emerging concerns like Ransomware, Cloud Computing and the Internet of Things.

Master the latest technology and developments from the field with the book specifically oriented to the needs of those learning information systems -- PRINCIPLES OF INFORMATION SECURITY, 6E. Taking a managerial approach, this bestseller emphasizes all aspects of information security, rather than just the technical control perspective. Readers gain a broad overview of the entire field of information security and related elements with the detail to ensure understanding. The book highlights terms used in the field and a history of the discipline as readers learn how to manage an information security program. This edition highlights the latest practices with fresh examples that explore the impact of emerging technologies, such as the Internet of Things, Cloud Computing, and DevOps. Updates address technical security controls, emerging legislative issues, digital forensics, and ethical issues in IS security, making this the ideal IS resource for business decision makers. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Hands-On Information Security Lab Manual, Second Edition allows students to apply the basics of their introductory security knowledge in a hands-on environment with detailed exercises using Windows 2000, XP and Linux. This non-certification based lab manual includes coverage of scanning, OS vulnerability analysis and resolution firewalls, security maintenance, forensics, and more. A full version of the software needed to complete these projects is included on a CD with every text, so instructors can effortlessly set up and run labs to correspond with their classes. The Hands-On Information Security Lab Manual, Second Edition is a suitable resource for introductory, technical and managerial courses, and is the perfect accompaniment to Principles of Information Security, Second Edition and Management of Information Security.

????????????????????,?????????LAN?????????,????????????????????

Discover the latest trends, developments and technology in information security with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of information systems

students like you, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets, digital forensics and the most recent policies and guidelines that correspond to federal and international standards. MindTap digital resources offer interactive content to further strength your success as a business decision-maker.

PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Equip your students with a management-focused overview of information security as well as the tools to effectively administer it with Whitman/Mattord's MANAGEMENT OF INFORMATION SECURITY, Sixth Edition. More than ever, we need to prepare information security management students to build and staff security programs capable of securing systems and networks to meet the challenges in a world where continuously emerging threats, ever-present attacks and the success of criminals illustrate weaknesses in current information technologies. This text offers an exceptional blend of skills and experiences to administer and manage the more secure computing environments that organizations need. Reflecting the latest developments from the field, it includes updated coverage of NIST, ISO and security governance along with emerging concerns like Ransomware, Cloud Computing and the Internet of Things.

????????????????????,????????????????,????????????????????,????????????????????.

Now updated—your expert guide to twenty-first century information security Information security is a rapidly evolving field. As businesses and consumers become increasingly dependent on complex multinational information systems, it is more imperative than ever to protect the confidentiality and integrity of data. Featuring a wide array of new information on the most current security issues, this fully updated and revised edition of Information Security: Principles and Practice provides the skills and knowledge readers need to tackle any information security challenge. Taking a practical approach to information security by focusing on real-world examples, this book is organized around four major themes:

Cryptography: classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers, information hiding, and cryptanalysis Access control: authentication and authorization, password-based security, ACLs and capabilities, multilevel security and compartments, covert channels and inference control, security models such as BLP and Biba's model, firewalls, and intrusion detection systems Protocols: simple authentication protocols, session keys, perfect forward secrecy, timestamps, SSH, SSL, IPSec, Kerberos, WEP, and GSM Software: flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering, digital rights management, secure software development, and operating systems security This Second Edition features new discussions of relevant security topics such as the SSH and WEP protocols, practical RSA timing attacks, botnets, and security certification. New background material has been added, including a section on the Enigma cipher and coverage of the classic "orange book" view of security. Also featured are a greatly expanded and upgraded set of homework problems and many new figures, tables, and graphs to illustrate and clarify complex topics and problems. A comprehensive solutions manual is available to assist in course development. Minimizing theory while providing clear, accessible content, Information Security remains the premier text for students and instructors in information technology, computer science, and engineering, as well as for professionals working in these fields.

Firewalls are among the best-known security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when they are backed by effective security planning, a well-designed security policy, and when they work in concert with anti-virus software, intrusion detection systems, and other tools. This book aims to explore firewalls in the context of these other elements, providing readers with a solid, in-depth introduction to firewalls that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The second edition offers updated content and brand new material, from enhanced coverage of non-firewall subjects like information and network security to an all-new section dedicated to intrusion detection in the context of incident response.

?????:??

Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management, and more explanations of cloud-based systems and Web-accessible tools to prepare you for success.

HANDS-ON INFORMATION SECURITY LAB MANUAL, Fourth Edition, helps you hone essential information security skills by applying your knowledge to detailed, realistic exercises using Microsoft Windows 2000, Windows XP, Windows 7, and Linux. This wide-ranging, non-certification-based lab manual includes coverage of scanning, OS vulnerability analysis and resolution, firewalls, security maintenance, forensics, and more. The Fourth Edition includes new

introductory labs focused on virtualization techniques and images, giving you valuable experience with some of the most important trends and practices in information security and networking today. All software necessary to complete the labs are available online as a free download. An ideal resource for introductory, technical, and managerial courses or self-study, this versatile manual is a perfect supplement to the PRINCIPLES OF INFORMATION SECURITY, SECURITY FUNDAMENTALS, and MANAGEMENT OF INFORMATION SECURITY books. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Incorporating both the managerial and technical aspects of this discipline, the authors address knowledge areas of Certified Information Systems Security Professional certification throughout and include many examples of issues faced by today's businesses.

Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts, persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9781111138219 .

MANAGEMENT OF INFORMATION SECURITY, Fourth Edition gives readers an overview of information security and assurance using both domestic and international standards, all from a management perspective. Beginning with the foundational and technical components of information security, this edition then focuses on access control models, information security governance, and information security program assessment and metrics. The Fourth Edition is revised and updated to reflect changes in the field, including the ISO 27000 series, so as to prepare readers to succeed in the workplace. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Information security-driven topic coverage is the basis for this updated book that will benefit readers in the information technology and business fields alike. Management of Information Security, provides an overview of information security from a management perspective, as well as a thorough understanding of the administration of information security. Written by two Certified Information Systems Security Professionals (CISSP), this book has the added credibility of incorporating the CISSP Common Body of Knowledge (CBK), especially in the area of information security management. The second edition has been updated to maintain the industry currency and academic relevance that made the previous edition so popular, and case studies and examples continue to populate the book, providing real-life applications for the topics covered.

ROADMAP TO INFORMATION SECURITY: FOR IT AND INFOSEC MANAGERS provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management, and more explanation of cloud-based systems and Web-accessible tools to prepare you for success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Firewalls are among the best-known network security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. GUIDE TO FIREWALLS AND VPNs, THIRD EDITION explores firewalls in the context of these critical elements, providing an in-depth guide that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The text also features an abundant selection of realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. GUIDE TO FIREWALLS AND VPNs includes new and updated cases and projects, enhanced coverage of network security and VPNs, and information on relevant National Institute of Standards and Technology guidelines used by businesses and information technology professionals. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts, persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9781423901778 .

Are you ready to respond to an unauthorized intrusion to your computer network or server? Principles of Incident Response and Disaster Recovery presents methods to identify vulnerabilities and take appropriate countermeasures to prevent and mitigate failure risks for an organization. Not only does book present a foundation in disaster recovery principles and planning, but it also emphasizes the importance of incident response minimizing prolonged downtime that can potentially lead to irreparable loss. This book is the first of its kind to address the overall problem of contingency planning rather than focusing on specific tasks of incident response or disaster recovery.

Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not

