Corporate Computer And Network Security 3rd Edition

If you ally infatuation such a referred **corporate computer and network security 3rd edition** books that will have the funds for you worth, acquire the completely best seller from us currently from several preferred authors. If you want to humorous books, lots of novels, tale, jokes, and more fictions collections are plus launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections corporate computer and network security 3rd edition that we will no question offer. It is not with reference to the costs. Its virtually what you craving currently. This corporate computer and network security 3rd edition, as one of the most functioning sellers here will utterly be in the middle of the best options to review.

Computer and Network Security Essentials - Kevin Daimi 2017-08-12
This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book’s website at Springer.com.
Introduction to Computer and Network Security - Richard R. Brooks 2013-08-19
Guides Students in Understanding the Interactions between Computing/Networking Technologies and Security Issues Taking an interactive, "learn-by-doing" approach to teaching, Introduction to Computer and Network Security: Navigating Shades of Gray gives you a clear course to teach the technical issues related to security. Unlike most computer security books, which concentrate on software design and implementation, cryptographic tools, or networking issues, this text also explores how the interactions between hardware, software, and users affect system security. The book presents basic principles and concepts, along with examples of current threats to illustrate how the principles can either enable or neutralize exploits. Students see the importance of these concepts in existing and future technologies. In a challenging yet enjoyable way, they learn about a variety of technical topics, including current security exploits, technical factors that enable attacks, and economic and social factors that determine the security of future systems. Extensively classroom-tested, the material is structured around a set of challenging projects. Through staging exploits and choosing countermeasures to neutralize the attacks in the projects, students learn: How computer systems and networks operate How to reverse-engineer processes How to use systems in ways that were never foreseen (or supported) by the original developers Combining hands-on work with technical overviews, this text helps you integrate security analysis into your technical computing curriculum. It will educate your students on security issues, such as side-channel attacks, and deepen their understanding of how computers and networks work.
Cryptography and Network Security - William Stallings 2006
In this age of viruses and hackers, of electronic eavesdropping and electronic fraud, security is paramount. This solid, up-to-date tutorial is a comprehensive treatment of cryptography and network security is ideal for self-study.Explores the basic issues to be addressed by a network security capability through a tutorial and survey of cryptography and network security technology. Examines the practice of network security via practical applications that have been implemented and are in use today. Provides a simplified AES (Advanced Encryption Standard) that enables readers to grasp the essentials of AES more easily. Features block cipher modes of operation, including the CMAC mode for authentication and the CCM mode for authenticated encryption. Includes an expanded, updated treatment of intruders and malicious software.A useful reference for system engineers, programmers, system managers, network managers, product marketing personnel, and system support specialists.

Cryptography and Network Security - William Stallings 2003
For one-semester undergraduate/graduate level courses and for self-study. William Stallings offers a practical survey of both the principles and practice of cryptography and network security, reflecting the latest developments in the field.
Network Security, Firewalls and VPNs - J. Michael Stewart 2013-07-11
This fully revised and updated second edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization's network is connected to the public Internet. It provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks. Topics covered include: the basics of network security--exploring the details of firewall security and how VPNs operate; how to plan proper network security to combat hackers and outside threats; firewall configuration and deployment and managing firewall security; and how to secure local and internet communications with a VP. --
Computer Networks - Larry L. Peterson 2011-03-02
Computer Networks: A Systems Approach, Fifth Edition, explores the key principles of computer networking, with examples drawn from the real world of network and protocol design. Using the Internet as the primary example, this best-selling and classic textbook explains various protocols and networking technologies. The systems-oriented approach encourages students to think about how individual network components fit into a larger, complex system of interactions. This book has a completely updated content with expanded coverage of the topics of utmost importance to networking professionals and students, including P2P, wireless, network security, and network applications such as e-mail and the Web, IP telephony and video streaming, and peer-to-peer file sharing. There is now increased focus on application layer issues where innovative and exciting research and design is currently the center of attention. Other topics include network design and architecture; the ways users can connect to a network; the concepts of switching, routing, and internetworking; end-to-end protocols; congestion control and resource allocation; and end-to-end data. Each chapter includes a problem statement, which introduces issues to be examined; shaded sidebars that elaborate on a topic or introduce a related advanced topic; What’s Next? discussions that deal with emerging issues in research, the commercial world, or society; and exercises. This book is written for graduate or upper-division undergraduate classes in computer networking. It will also be useful for industry professionals retraining for network-related assignments, as well as for network practitioners seeking to understand the workings of network protocols and the big picture of networking. Completely updated content with expanded coverage of the topics of utmost importance to networking professionals and students, including P2P, wireless, security, and applications Increased focus on application layer issues where innovative and exciting research and design is currently the center of attention Free downloadable network simulation software and lab experiments manual available
Principles of Computer Security CompTIA Security+ and Beyond (Exam SY0-301), 3rd Edition - Wm. Arthur Conklin 2011-11-28
Essential Skills for a Successful IT Security Career Learn the fundamentals of computer and information security while getting complete coverage of all the objectives for the latest release of the CompTIA

Security+ certification exam. This up-to-date, full-color guide discusses communication, infrastructure, operational security, attack prevention, disaster recovery, computer forensics, and much more. Written and edited by leaders in the field, Principles of Computer Security: CompTIA Security+ and Beyond, Third Edition will help you pass CompTIA Security+ exam SY0-301 and become an IT security expert. From McGraw-Hill—a Gold-Level CompTIA Authorized Partner, this book offers Official CompTIA Approved Quality Content. Find out how to: Ensure operational, organizational, and physical security Use cryptography and public key infrastructures (PKIs) Secure remote access, wireless, and virtual private networks (VPNs) Harden network devices, operating systems, and applications Defend against network attacks, such as denial of service, spoofing, hijacking, and password guessing Combat viruses, worms, Trojan horses, logic bombs, time bombs, and rootkits Manage e-mail, instant messaging, and web security Understand secure software development requirements Enable disaster recovery and business continuity Implement risk, change, and privilege management measures Handle computer forensics and incident response Understand legal, ethical, and privacy issues The CD-ROM features: Two full practice exams PDF copy of the book Each chapter includes: Learning objectives Photographs and illustrations Real-world examples Try This! and Cross Check exercises Key terms highlighted Tech Tips, Notes, and Warnings Exam Tips End-of-chapter quizzes and lab projects

Fundamentals of Information Systems Security - David Kim 2016-10-15

Revised and updated with the latest data in the field, Fundamentals of Information Systems Security, Third Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transition to a digital world. Part 2 presents a high level overview of the Security+ Exam and provides students with information as they move toward this certification.

Computer Network Security - Joseph Migga Kizza 2005-04-07

A comprehensive survey of computer network security concepts, methods, and practices. This authoritative volume provides an optimal description of the principles and applications of computer network security in particular, and cyberspace security in general. The book is thematically divided into three segments: Part I describes the operation and security conditions surrounding computer networks; Part II builds from there and exposes readers to the prevailing security situation based on a constant security threat; and Part III - the core - presents readers with most of the best practices and solutions currently in use. It is intended as both a teaching tool and reference. This broad-ranging text/reference comprehensively surveys computer network security concepts, methods, and practices and covers network security tools, policies, and administrative goals in an integrated manner. It is an essential security resource for undergraduate or graduate study, practitioners in networks, and professionals who develop and maintain secure computer network systems.

Corporate Computer and Network Security - R. R. Panko 2010

A strong managerial focus along with a solid technical presentation of security tools. Guided by discussions with IT security professionals, Corporate Computer and Network Security covers the specific material that all IT majors and future IT security specialists need to learn from an introductory network security course. This text has been entirely rewritten in its second edition to reflect the latest trends and cutting-edge technology that students will work with in their future careers.

Guide to Computer Network Security - Joseph Migga Kizza 2013-01-03

This comprehensive guide exposes the security risks and vulnerabilities of computer networks and networked devices, offering advice on developing improved algorithms and best practices for enhancing system security. Fully revised and updated, this new edition embraces a broader view of computer networks that encompasses agile mobile systems and social networks. Features: provides supporting material for lecturers and students, including an instructor’s manual, slides, solutions, and laboratory materials; includes both quick and more thought-provoking exercises at the end of each chapter; devotes an entire chapter to laboratory exercises; discusses flaws and vulnerabilities in computer network infrastructures and protocols; proposes practical and efficient solutions to security issues; explores the role of legislation, regulation, and law enforcement in maintaining computer and computer network security; examines the impact of developments in virtualization, cloud computing, and mobile systems.

Handbook of Information Security, Key Concepts, Infrastructure, Standards, and Protocols - Hossein Bidgoli 2006-03-20

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Information Security - Mark Stamp 2005-11-11

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Computer Security Fundamentals - Chuck Easttom 2012

One-volume coverage of all the core concepts, terminology, issues, and practical skills modern computer security professionals need to know * *The most up-to-date computer security concepts text on the market. *Strong coverage and comprehensive analysis of key attacks, including denial of service, malware, and viruses. *Covers oft-neglected subject areas such as cyberterrorism, computer fraud, and industrial espionage. *Contains end-of-chapter exercises, projects, review questions, and plenty of realworld tips. Computer Security Fundamentals, Second Edition is designed to be the ideal one volume gateway into the entire field of computer security. It brings together thoroughly updated coverage of all basic concepts, terminology, and issues, along with the practical skills essential to security. Drawing on his extensive experience as both an IT professional and instructor, Chuck Easttom thoroughly covers core topics such as vulnerability assessment, virus attacks, buffer overflow, hacking, spyware, network defense, firewalls, VPNs, Intrusion Detection Systems, and passwords. Unlike many other authors, however, he also fully addresses more specialized issues, including cyber terrorism, industrial espionage and encryption - including public/private key systems, digital signatures, and certificates. This edition has been extensively updated to address the latest issues and technologies, including cyberbullying/cyberstalking, session hijacking, steganography, and more. Its examples have been updated to reflect the current state-of-the-art in both attacks and defense. End-of-chapter exercises, projects, and review questions guide readers in applying the knowledge they've gained, and Easttom offers many tips that readers would otherwise have to discover through hard experience.

NETWORK SECURITY AND MANAGEMENT - BRIJENDRA SINGH 2011-12-24

Written in an easy-to-understand style, this textbook, now in its third edition, continues to discuss in detail important concepts and major developments in network security and management. It is designed for a one-semester course for undergraduate students of Computer Science, Information Technology, and undergraduate and postgraduate students of Computer Applications. Students are first exposed to network

security principles, organizational policy and security infrastructure, and then drawn into some of the deeper issues of cryptographic algorithms and protocols underlying network security applications. Encryption methods, secret key and public key cryptography, digital signature and other security mechanisms are emphasized. Smart card, biometrics, virtual private networks, trusted operating systems, pretty good privacy, database security, and intrusion detection systems are comprehensively covered. An in-depth analysis of technical issues involved in security management, risk management and security and law is presented. In the third edition, two new chapters—one on Information Systems Security and the other on Web Security—and many new sections such as digital signature, Kerberos, public key infrastructure, software security and electronic mail security have been included. Additional matter has also been added in many existing sections. KEY FEATURES : Extensive use of block diagrams throughout helps explain and clarify the concepts discussed. About 250 questions and answers at the end of the book facilitate fruitful revision of the topics covered. Includes a glossary of important terms. KEY FEATURES : Extensive use of block diagrams throughout helps explain and clarify the concepts discussed. About 250 questions and answers at the end of the book facilitate fruitful revision of the topics covered. Includes a glossary of important terms.

Fundamentals of Information Systems Security - David Kim 2013-07-11

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

Corporate Computer Security - Randy J. Boyle 2013-11-01

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Boyle/Panko provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies.

Foundations of Computer Security - David Salomon 2005-12-23

Anyone with a computer has heard of viruses, had to deal with several, and has been struggling with spam, spyware, and disk crashes. This book is intended as a starting point for those familiar with basic concepts of computers and computations and who would like to extend their knowledge into the realm of computer and network security. Its comprehensive treatment of all the major areas of computer security aims to give readers a complete foundation in the field of Computer Security. Exercises are given throughout the book and are intended to strengthening the reader’s knowledge - answers are also provided. Written in a clear, easy to understand style, aimed towards advanced undergraduates and non-experts who want to know about the security problems confronting them everyday. The technical level of the book is low and requires no mathematics, and only a basic concept of computers and computations. Foundations of Computer Security will be an invaluable tool for students and professionals alike.

Practical UNIX and Internet Security - Simson Garfinkel 2003-02-21

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.

Computer and Information Security Handbook - John R. Vacca 2017-05-10

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

Network and System Security - John R. Vacca 2013-08-26

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

Network Security and Cryptography - Sarhan M. Musa 2018-03-20
Network Security and Cryptography introduces the basic concepts in computer networks and the latest trends and technologies in cryptography and network security. The book is a definitive guide to the principles and techniques of cryptography and network security, and introduces basic concepts in computer networks such as classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, and Internet security. It features the latest material on emerging technologies, related to IoT, cloud computing, SCADA, blockchain, smart grid, big data analytics, and more. Primarily intended as a textbook for courses in computer science and electronics & communication, the book also serves as a basic reference and refresher for professionals in these areas. FEATURES: • Includes the latest material on emerging technologies, related to IoT, cloud computing, smart grid, big data analytics, blockchain, and more • Features separate chapters on the mathematics related to network security and cryptography • Introduces basic concepts in computer networks including classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, Internet security services, and system security • Includes end of chapter review questions
Network Security Assessment - Chris McNab 2016-02-25
How secure is your network? The best way to find out is to attack it. Network Security Assessment provides you with the tools and techniques that professional security analysts use to identify and assess risks in government, military, and commercial networks. Armed with this book, you can work to create environments that are hardened and immune from unauthorized use and attack. Author Chris McNab demonstrates how determined adversaries map attack surface and exploit security weaknesses at both the network and application level. The third edition is a complete overhaul—grouping and detailing the latest hacking techniques used to attack enterprise networks. By categorizing individual threats, you will be able to adopt defensive strategies against entire attack classes, providing protection now and into the future. The testing approaches within the book are written in-line with internationally recognized standards, including NIST SP 800-115, NSA IAM, CESG CHECK, and PCI DSS.
Computer Security - ESORICS 94 - Dieter Gollmann 1994-10-19
This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer security research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.
Security in Computing Charles P. Pfleeger 2009

Security+ Guide to Network Security Fundamentals - Mark Ciampa 2012-07-27
Reflecting the latest trends and developments from the information security field, best-selling Security+ Guide to Network Security Fundamentals, Fourth Edition, provides a complete introduction to practical network and computer security and maps to the CompTIA Security+ SY0-301 Certification Exam. The text covers the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The updated edition includes new topics, such as psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. The new edition features activities that link to the Information Security Community Site, which offers video lectures, podcats, discussion boards, additional hands-on activities and more to provide a wealth of resources and up-to-the minute information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Corporate Computer Security - Randall J. Boyle 2014-01-07
For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience-for you and your students. Here's how: Encourage Student's to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.
Network Security First-Step - Thomas M. Thomas 2004-05-21
Your first step into the world of network security No security experience required Includes clear and easily understood explanations Makes learning easy Your first step to network security begins here! Learn about hackers and their attacks Understand security tools and technologies Defend your network with firewalls, routers, and other devices Explore security for wireless networks Learn how to prepare for security incidents Welcome to the world of network security! Computer networks are indispensable-but they're also not secure. With the proliferation of Internet viruses and worms, many people and companies are considering increasing their network security. But first, you need to make sense of this complex world of hackers, viruses, and the tools to combat them. No security experience needed! Network Security First-Step explains the basics of network security in easy-to-grasp language that all of us can understand. This book takes you on a guided tour of the core technologies that make up and control network security. Whether you are looking to take your first step into a career in network security or are interested in simply gaining knowledge of the technology, this book is for you!
Computer Security - William Stallings 2012
Computer Security: Principles and Practice, 2e, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically – and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. The Text and Academic Authors Association named Computer Security: Principles and Practice, 1e, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008.
Elementary Information Security - Richard E. Smith 2013
Comprehensive and accessible, Elementary Information Security covers the entire range of topics required for US government courseware certification NSTISSI 4013 and urges students analyze a variety of security problems while gaining experience with basic tools of the trade. Written for the one-term undergraduate course, the text emphasises both the technical and non-technical aspects of information security and uses practical examples and real-world assessment tools. Early chapters in the text discuss individual computers and small LANS, while later chapters deal with distributed site security and the Internet. Cryptographic topics follow the same progression, starting on a single computer and evolving to Internet-level connectivity. Mathematical concepts throughout the text are defined and tutorials with mathematical tools are provided to ensure students grasp the information at hand. Rather than emphasizing memorization, this text challenges students to learn how to analyze a variety of security problems and gain experience with the basic tools of this growing trade.Key Features:-Covers all topics required by the US government curriculum standard NSTISSI 4013.- Unlike other texts on the topic, the author goes beyond defining the math concepts and provides students with tutorials and practice with mathematical tools, making the text appropriate for a broad range of readers.- Problem Definitions describe a practical situation that includes a security dilemma.- Technology Introductions provide a practical explanation of security technology to be used in the specific chapters- Implementation Examples show the technology being used to enforce the security policy at hand- Residual Risks describe the limitations to the technology and illustrate various tasks against it.- Each chapter includes worked examples of techniques students will need to be successful in the course. For instance, there will be numerous examples of how to calculate the number of attempts needed to crack secret information in particular formats; PINs, passwords and encryption keys.
Computer System and Network Security Gregory B. White 2017-12-14

Computer System and Network Security provides the reader with a basic understanding of the issues involved in the security of computer systems and networks. Introductory in nature, this important new book covers all aspects related to the growing field of computer security. Such complete coverage in a single text has previously been unavailable, and college professors and students, as well as professionals responsible for system security, will find this unique book a valuable source of information, either as a textbook or as a general reference. Computer System and Network Security discusses existing and potential threats to computer systems and networks and outlines the basic actions that are generally taken to protect them. The first two chapters of the text introduce the reader to the field of computer security, covering fundamental issues and objectives. The next several chapters describe security models, authentication issues, access control, intrusion detection, and damage control. Later chapters address network and database security and systems/networks connected to wide-area networks and internetworks. Other topics include firewalls, cryptography, malicious software, and security standards. The book includes case studies with information about incidents involving computer security, illustrating the problems and potential damage that can be caused when security fails. This unique reference/textbook covers all aspects of computer and network security, filling an obvious gap in the existing literature.

Computer Security - Dieter Gollmann 2011-02-28

A completely up-to-date resource on computer security Assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security. This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different from one another. Unravels the complex topic of computer security and breaks it down in such a way as to serve as an ideal introduction for beginners in the field of computer security Examines the foundations of computer security and its basic principles Addresses username and password, password protection, single sign-on, and more Discusses operating system integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

Network Security, Firewalls, and VPNs - J. Michael Stewart 2020-10-15

Network Security, Firewalls, and VPNs, third Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization’s network is connected to the public Internet.

Computer Network Security and Cyber Ethics, 4th ed. - Joseph Migga Kizza 2014-03-21

In its 4th edition, this book remains focused on increasing public awareness of the nature and motives of cyber vandalism and cybercriminals, the weaknesses inherent in cyberspace infrastructure, and the means available to protect ourselves and our society. This new edition aims to integrate security education and awareness with discussions of morality and ethics. The reader will gain an understanding of how the security of information in general and of computer networks in particular, on which our national critical infrastructure and, indeed, our lives depend, is based squarely on the individuals who build the hardware and design and develop the software that run the networks that store our vital information. Addressing security issues with ever-growing social networks are two new chapters: “Security of Mobile Systems” and “Security in the Cloud Infrastructure.” Instructors considering this book for use in a course may request an examination copy here.

Guide to Computer Network Security - Joseph Migga Kizza 2020-06-03

This timely textbook presents a comprehensive guide to the core topics in cybersecurity, covering issues of security that extend beyond traditional computer networks to the ubiquitous mobile communications and online social networks that have become part of our daily lives. In the context of our growing dependence on an ever-changing digital ecosystem, this book stresses the importance of security awareness, whether in our homes, our businesses, or our public spaces. This fully updated new edition features new material on the security issues raised by blockchain technology, and its use in logistics, digital ledgers, payments systems, and digital contracts. Topics and features: Explores the full range of security risks and vulnerabilities in all connected digital systems Inspires debate over future developments and improvements necessary to enhance the security of personal, public, and private enterprise systems Raises thought-provoking questions regarding legislative, legal, social, technical, and ethical challenges, such as the tension between privacy and security Describes the fundamentals of traditional computer network security, and common threats to security Reviews the current landscape of tools, algorithms, and professional best practices in use to maintain security of digital systems Discusses the security issues introduced by the latest generation of network technologies, including mobile systems, cloud computing, and blockchain Presents exercises of varying levels of difficulty at the end of each chapter, and concludes with a diverse selection of practical projects Offers supplementary material for students and instructors at an associated website, including slides, additional projects, and syllabus suggestions This important textbook/reference is an invaluable resource for students of computer science, engineering, and information management, as well as for practitioners working in data- and information-intensive industries.

Network Defense and Countermeasures - William (Chuck) Easttom II 2013-10-18

Everything you need to know about modern network attacks and defense, in one book Clearly explains core network security concepts, challenges, technologies, and skills Thoroughly updated for the latest attacks and countermeasures The perfect beginner’s guide for anyone interested in a network security career ¿ Security is the IT industry’s hottest topic–and that’s where the hottest opportunities are, too. Organizations desperately need professionals who can help them safeguard against the most sophisticated attacks ever created–attacks from well-funded global criminal syndicates, and even governments. ¿ Today, security begins with defending the organizational network. Network Defense and Countermeasures, Second Edition is today’s most complete, easy-to-understand introduction to modern network attacks and their effective defense. From malware and DDoS attacks to firewalls and encryption, Chuck Easttom blends theoretical foundations with up-to-the-minute best-practice techniques. Starting with the absolute basics, he discusses crucial topics many security books overlook, including the emergence of network-based espionage and terrorism. ¿ If you have a basic understanding of networks, that’s all the background you’ll need to succeed with this book: no math or advanced computer science is required. You’ll find projects, questions, exercises, case studies, links to expert resources, and a complete glossary–all designed to deepen your understanding and prepare you to defend real-world networks. ¿ Learn how to Understand essential network security concepts, challenges, and careers Learn how modern attacks work Discover how firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) combine to protect modern networks Select the right security technologies for any network environment Use encryption to protect information Harden Windows and Linux systems and keep them patched Securely configure web browsers to resist attacks Defend against malware Define practical, enforceable security policies Use the “6 Ps” to assess technical and human aspects of system security Detect and fix system vulnerability Apply proven security standards and models, including Orange Book, Common Criteria, and Bell-LaPadula Ensure physical security and prepare for disaster recovery Know your enemy: learn basic hacking, and see how to counter it Understand standard forensic techniques and prepare for investigations of digital crime ¿

Computer & Internet Security - Wenliang Du 2022-05

Unique among computer security texts, this book, in its third edition, builds on the author's long tradition of teaching complex subjects through a hands-on approach. For each security principle, the book uses a series of hands-on activities to help explain the principle. Readers can "touch", play with, and experiment with the principle, instead of just reading about it. The hands-on activities are based on the author's widely adopted SEED Labs, which have been used by over 1000 institutes worldwide. The author has also published online courses on Udemy based on this book. Topics covered in the book including the following. Software security: attacks and countermeasures; Web security: attacks and countermeasures; Hardware security: Meltdown and Spectre attacks; Network security: attacks on TCP/IP and DNS protocols; Firewall and Virtual Private Network (VPN); Cryptography and attacks on algorithms and protocols; Public Key Infrastructure- Common hacking and defense techniques.

Network Security - Mike Speciner 2002-04-22

The classic guide to network security—now fully updated!"Bob and Alice are back!" Widely regarded as the

most comprehensive yet comprehensible guide to network security, the first edition of Network Security received critical acclaim for its lucid and witty explanations of the inner workings of network security protocols. In the second edition, this most distinguished of author teams draws on hard-won experience to explain the latest developments in this field that has become so critical to our global network-dependent society. Network Security, Second Edition brings together clear, insightful, and clever explanations of every key facet of information security, from the basics to advanced cryptography and authentication, secure Web and email services, and emerging security standards. Coverage includes: All-new discussions of the Advanced Encryption Standard (AES), IPsec, SSL, and Web security Cryptography: In-depth, exceptionally clear introductions to secret and public keys, hashes, message digests, and other crucial concepts Authentication: Proving identity across networks, common attacks against authentication systems, authenticating people, and avoiding the pitfalls of authentication handshakes Core Internet security standards: Kerberos 4/5, IPsec, SSL, PKIX, and X.509 Email security: Key elements of a secure email system-plus detailed coverage of PEM, S/MIME, and PGP Web security: Security issues associated with URLs, HTTP, HTML, and cookies Security implementations in diverse platforms, including Windows, NetWare, and Lotus Notes The authors go far beyond documenting standards and technology: They contrast competing schemes, explain strengths and weaknesses, and identify the crucial errors most likely to compromise secure systems. Network Security will appeal to a wide range of professionals, from those who design or evaluate security systems to system administrators and programmers who want a better understanding of this important field. It can also be used as a textbook at the graduate or advanced undergraduate level.

Top-down Network Design - Priscilla Oppenheimer 2004

A systems analysis approach to enterprise network design Master techniques for checking the health of an existing network to develop a baseline for measuring performance of a new network design Explore solutions for meeting QoS requirements, including ATM traffic management, IETF controlled-load and guaranteed services, IP multicast, and advanced switching, queuing, and routing algorithms Develop network designs that provide the high bandwidth and low delay required for real-time applications such as multimedia, distance learning, and videoconferencing Identify the advantages and disadvantages of various switching and routing protocols, including transparent bridging, Inter-Switch Link (ISL), IEEE 802.1Q, IGRP, EIGRP, OSPF, and BGP4 Effectively incorporate new technologies into enterprise network designs, including VPNs, wireless networking, and IP Telephony Top-Down Network Design, Second Edition, is a practical and comprehensive guide to designing enterprise networks that are reliable, secure, and manageable. Using illustrations and real-world examples, it teaches a systematic method for network design that can be applied to campus LANs, remote-access networks, WAN links, and large-scale internetworks. You will learn to analyze business and technical requirements, examine traffic flow and QoS requirements, and select protocols and technologies based on performance goals. You will also develop an understanding of network performance factors such as network utilization, throughput, accuracy, efficiency, delay, and jitter. Several charts and job aids will help you apply a top-down approach to network design. This Second Edition has been revised to include new and updated material on wireless networks, virtual private networks (VPNs), network security, network redundancy, modularity in network designs, dynamic addressing for IPv4 and IPv6, new network design and management tools, Ethernet scalability options (including 10-Gbps Ethernet, Metro Ethernet, and Long-Reach Ethernet), and networks that carry voice and data traffic. Top-Down Network Design, Second Edition, has a companion website at http://www.topdownbook.com, which includes updates to the book, links to white papers, and supplemental information about design resources. This book is part of the Networking Technology Series from Cisco Press¿ which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

Hands-On Ethical Hacking and Network Defense - Michael T. Simpson 2016-10-10

Cyber-terrorism and corporate espionage are increasingly common and devastating threats, making trained network security professionals more important than ever. This timely text helps you gain the knowledge and skills to protect networks using the tools and techniques of an ethical hacker. The authors begin by exploring the concept of ethical hacking and its practitioners, explaining their importance in protecting corporate and government data from cyber attacks. The text then provides an in-depth guide to performing security testing against computer networks, covering current tools and penetration testing methodologies. Updated for today’s cyber security environment, the Third Edition of this trusted text features new computer security resources, coverage of emerging vulnerabilities and innovative methods to protect networks, a new discussion of mobile security, and information on current federal and state computer crime laws, including penalties for illegal computer hacking. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.