By Chuck Easttom System Forensics Investigation And Response 2nd Edition

Get complete coverage of all six CCFP exam domains developed by the International Information Systems Security Certification Consortium (ISC)2. Written by a leading computer security expert, this authoritative guide fully addresses cyber forensics techniques, standards, technologies, and legal and ethical principles. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. COVERS ALL SIX EXAM DOMAINS: Legal and ethical principles Investigations Forensic science Digital forensics Application forensics Hybrid and emerging technologies ELECTRONIC CONTENT INCLUDES: 250 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain

????:????

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Completely revised and rewritten to keep pace with the fast-paced field of Computer Forensics! Computer crimes call for forensics specialists, people who know how to find and follow the evidence. System Forensics, Investigation, and Response, Second Edition begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. It then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. New and Key Features of the Second Edition: Examines the fundamentals of system forensics Discusses computer crimes and forensic methods Written in an accessible and engaging style Incorporates real-world examples and engaging cases Instructor Materials for System Forensics, Investigation, and Response include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts Instructor's Manual

System Forensics, Investigation, and ResponseJones & Bartlett Learning

????9???,??????????????????????????????LAN??????????????????PIX????IOS????VPN????GRE?L2TP?IPSec??????Cisco??????AAA?TACACS+?RADIUS???AAA????????????????????????????????????NBAR??????????CAR????????????????

"This manual includes lab instructions to be carried out using the Jones & Bartlett Learning Virtual Security Cloud Labs powered by Toolwire. These labs allow users to experience hands-on, equipment-based labs that mimic real-world IT security scenarios in a realistic mock environment."--P. [4] of cover.

Traditional Chinese Edition of [Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers]

Print Textbook & Cloud Lab Access: 180-day subscription. The cybersecurity Cloud Labs for Digital Forensics,

Investigation, and Response provide fully immersive mock IT infrastructures with live virtual machines and real software, where students will learn and practice the foundational information security skills they will need to excel in their future careers. Unlike simulations, these hands-on virtual labs reproduce the complex challenges of the real world, without putting an institution's assets at risk. Available as a standalone lab solution or bundled with Jones & Bartlett Learning textbooks, these cybersecurity Cloud Labs are an essential tool for mastering key course concepts through hands-on training. Labs: Lab 1: Applying the Daubert Standard to Forensic Evidence Lab 2: Recognizing the Use of Steganography in Forensic Evidence Lab 3: Recovering Deleted and Damaged Files Lab 4: Conducting an Incident Response Investigation Lab 5: Conducting Forensic Investigations on Windows Systems Lab 6: Conducting Forensic Investigations on Linux Systems Lab 7: Conducting Forensic Investigations on Email and Chat Logs Lab 8: Conducting Forensic Investigations on Mobile Devices Lab 9: Conducting Forensic Investigations on Network Infrastructure Lab 10: Conducting Forensic Investigations on System Memory Supplemental Lab 1: Conducting Forensic Investigations on Cloud Services Supplemental Lab 2: Conducting Forensic Investigations on Social Media

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

Mobile devices are ubiquitous; therefore, mobile device forensics is absolutely critical. Whether for civil or criminal investigations, being able to extract evidence from a mobile device is essential. This book covers the technical details of mobile devices and transmissions, as well as forensic methods for extracting evidence. There are books on specific issues like Android forensics or iOS forensics, but there is not currently a book that covers all the topics covered in this book. Furthermore, it is such a critical skill that mobile device forensics is the most common topic the Author is asked to teach to law enforcement. This is a niche that is not being adequately filled with current titles. An In-Depth Guide to Mobile Device Forensics is aimed towards undergraduates and graduate students studying cybersecurity or digital forensics. It covers both technical and legal issues, and includes exercises, tests/quizzes, case studies, and slides to aid comprehension.

This comprehensive guide to modern data encryption makes cryptography accessible to information security professionals of all skill levels—with no math expertise required Cryptography underpins today’s cyber-security; however, few information security professionals have a solid understanding of these encryption methods due to their complex mathematical makeup. Modern Cryptography: Applied Mathematics for Encryption and Information Security leads readers through all aspects of the field, providing a comprehensive overview of cryptography and practical instruction on the latest encryption methods. The book begins with an overview of the evolution of cryptography and moves on to modern protocols with a discussion of hashes, cryptanalysis, and steganography. From there, seasoned security author

Chuck Easttom provides readers with the complete picture—full explanations of real-world applications for cryptography along with detailed implementation instructions. Unlike similar titles on the topic, this reference assumes no mathematical expertise—the reader will be exposed to only the formulas and equations needed to master the art of cryptography. Concisely explains complex formulas and equations and makes the math easy Teaches even the information security novice critical encryption skills Written by a globally-recognized security expert who has taught cryptography to various government and civilian groups and organizations around the world

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

????????·????

Welcome to today's most useful and practical one-volume introduction to computer security. Chuck Easttom brings together up-to-the-minute coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started in the field. Drawing on his extensive experience as a security instructor and consultant, Easttom thoroughly covers core topics, such as vulnerability assessment, virus attacks, hacking, spyware, network defense, passwords, firewalls, VPNs, and intrusion detection. Writing clearly and simply, he fully addresses crucial issues that many introductory security books ignore, from industrial espionage to cyberbullying. Computer Security Fundamentals, Second Edition is packed with tips and examples, all extensively updated for the state-of-the-art in both attacks and defense. Each chapter offers exercises, projects, and review questions designed to deepen your understanding and help you apply all you've learned. Whether you're a student, a system or network administrator, a manager, or a law enforcement professional, this book will help you protect your systems and data and expand your career options . Learn how to Identify the worst threats to your network and assess your risks Get inside the minds of hackers, so you can prevent their attacks Implement a proven layered approach to network security Use basic networking knowledge to improve security Resist the full spectrum of Internet-based scams and frauds Defend against today's most common Denial of Service (DoS) attacks Prevent attacks by viruses, spyware, and other malware Protect against low-tech social engineering attacks Choose the best encryption methods for your organization Select firewalls and other security technologies Implement security policies that will work in your environment Scan your network for vulnerabilities Evaluate potential security consultants Understand cyberterrorism and information warfare Master basic computer forensics and know what to do after you're attacked.

Advanced JavaScript, Third Edition provides an in-depth examination of the most important features of JavaScript. Beginning with an overview of JavaScript, the book quickly moves into more advanced features needed for complex yet robust JavaScript scripts, such as objects, arrays, and date and time functions. Additionally, various features of JavaScript that are essential for modern web pages are discussed, including manipulating the status bar, creating dynamic calendars, and working with forms, images, and the Document Object Model. Numerous examples illustrate how to implement various techniques. Topics covered how to enhance your web pages with LED signs, banners, and images; implementing cookies to store and retrieve information; the structure of the Document Object Model and how it can be used to view, access, and change an HTML document; Security measures to protect private information while using the Internet.

???12?.??????,??????????,?????????,?????????,??????????,?????,??????,IP???.

Clearly explains core concepts, terminology, challenges, technologies, and skills Covers today’s latest attacks and countermeasures The

perfect beginner's guide for anyone interested in a computer security career Dr. Chuck Easttom brings together complete coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started. Drawing on 30 years of experience as a security instructor, consultant, and researcher, Easttom helps you take a proactive, realistic approach to assessing threats and implementing countermeasures. Writing clearly and simply, he addresses crucial issues that many introductory security books ignore, while addressing the realities of a world where billions of new devices are Internet-connected. This guide covers web attacks, hacking, spyware, network defense, security appliances, VPNs, password use, and much more. Its many tips and examples reflect new industry trends and the state-of-the-art in both attacks and defense. Exercises, projects, and review questions in every chapter help you deepen your understanding and apply all you've learned. Whether you're a student, a professional, or a manager, this guide will help you protect your assets—and expand your career options. LEARN HOW TO Identify and prioritize potential threats to your network Use basic networking knowledge to improve security Get inside the minds of hackers, so you can deter their attacks Implement a proven layered approach to network security Resist modern social engineering attacks Defend against today's most common Denial of Service (DoS) attacks Halt viruses, spyware, worms, Trojans, and other malware Prevent problems arising from malfeasance or ignorance Choose the best encryption methods for your organization Compare security technologies, including the latest security appliances Implement security policies that will work in your environment Scan your network for vulnerabilities Evaluate potential security consultants Master basic computer forensics and know what to do if you're attacked Learn how cyberterrorism and information warfare are evolving

This textbook is a practical yet in depth guide to cryptography and its principles and practices. The book places cryptography in real-world security situations using the hands-on information contained throughout the chapters. Prolific author Dr. Chuck Easttom lays out essential math skills and fully explains how to implement cryptographic algorithms in today's data protection landscape. Readers learn and test out how to use ciphers and hashes, generate random keys, handle VPN and Wi-Fi security, and encrypt VoIP, Email, and Web communications. The book also covers cryptanalysis, steganography, and cryptographic backdoors and includes a description of quantum computing and its impact on cryptography. This book is meant for those without a strong mathematics background _ only just enough math to understand the algorithms given. The book contains a slide presentation, questions and answers, and exercises throughout. Presents a comprehensive coverage of cryptography in an approachable format; Covers the basic math needed for cryptography _ number theory, discrete math, and algebra (abstract and linear); Includes a full suite of classroom materials including exercises, Q&A, and examples.

??????

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Security Policies and Implementation Issues, Third Edition offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. Written by industry experts, the new Third Edition presents an effective balance between technical knowledge and soft skills, while introducing many different concepts of information security in clear simple terms such as governance, regulator mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of security policies and frameworks. Instructor Materials for Security Policies and Implementation Issues include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts About the Series This book is part of the Information Systems Security and Assurance Series from Jones and Bartlett

Learning. Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Theory Lab Access. Security Policies and Implementation Issues, Third Edition offers a comprehensive, end-to-end view of information security policies and frameworks from the raw organizational mechanics of building to the psychology of implementation. Written by industry experts, the new Third Edition presents an effective balance between technical knowledge and soft skills, while introducing many different concepts of information security in clear simple terms such as governance, regulator mandates, business drivers, legal considerations, and much more. With step-by-step examples and real-world exercises, this book is a must-have resource for students, security officers, auditors, and risk leaders looking to fully understand the process of implementing successful sets of security policies and frameworks. Labs: Lab 1: Crafting an Organization-Wide Security Management Policy for Acceptable Use Lab 2: Developing an Organization-Wide Policy Framework Implementation Plan Lab 3: Defining an Information Systems Security Policy Framework for an IT Infrastructure Lab 4: Crafting a Layered Security Management Policy - Separation of Duties Lab 5: Crafting an Organization-Wide Security Awareness Policy-BIA and Recovery Time Lab 6: Defining a Remote Access Policy to Support Remote Health Care Clinics Lab 7: Identifying Necessary Policies for Business Continuity - BIA and Recovery Time Objectives Lab 8: Crafting a Security or Computer Incident Response Policy - CIRT Response Team Lab 9: Assessing and Auditing an Existing IT Security Policy Framework Definition Lab 10: Aligning an IT Security Policy Framework to the Seven Domains of a Typical IT Infrastructure

A book that includes case studies and coverage of expert witnesses presents an overview of computer crime covering both legal and technical aspects and providing a broad overview of computer forensics, computer laws and computer-related trials. Original.

ONE-VOLUME INTRODUCTION TO COMPUTER SECURITY Clearly explains core concepts, terminology, challenges, technologies, and skills Covers today's latest attacks and countermeasures The perfect beginner's guide for anyone interested in a computer security career Chuck Easttom brings together complete coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started. Drawing on 20+ years of experience as a security instructor, consultant, and researcher, Easttom helps you take a proactive, realistic approach to assessing threats and implementing countermeasures. Writing clearly and simply, he addresses crucial issues that many introductory security books ignore, while addressing the realities of a world where billions of new devices are Internet-connected. This guide covers web attacks, hacking, spyware, network defense, security appliances, VPNs, password use, and much more. Its many tips and examples reflect new industry trends and the state-of-the-art in both attacks and defense. Exercises, projects, and review questions in every chapter help you deepen your understanding and apply all you've learned. Whether you're a student, a professional, or a manager, this guide will help you protect your assets--and expand your career options. Learn how to · Identify and prioritize potential threats to your network · Use basic networking knowledge to improve security · Get inside the minds of hackers, so you can deter their attacks · Implement a proven layered approach to network security · Resist modern social engineering attacks · Defend against today's most common Denial of Service (DoS) attacks · Halt viruses, spyware, worms, Trojans, and other malware · Prevent problems arising from malfeasance or ignorance ·

Choose the best encryption methods for your organization · Compare security technologies, including the latest security appliances · Implement security policies that will work in your environment · Scan your network for vulnerabilities · Evaluate potential security consultants · Master basic computer forensics and know what to do if you're attacked · Learn how cyberterrorism and information warfare are evolving. All you need to know about defending networks, in one book · Clearly explains concepts, terminology, challenges, tools, and skills · Covers key security standards and models for business and government · The perfect introduction for all network/computer security professionals and students Welcome to today's most useful and practical introduction to defending modern networks. Drawing on decades of experience, Chuck Easttom brings together updated coverage of all the concepts, terminology, techniques, and solutions you'll need to be effective. Easttom thoroughly introduces the core technologies of modern network security, including firewalls, intrusion-detection systems, and VPNs. Next, he shows how encryption can be used to safeguard data as it moves across networks. You'll learn how to harden operating systems, defend against malware and network attacks, establish robust security policies, and assess network security using industry-leading standards and models. You'll also find thorough coverage of key issues such as physical security, forensics, and cyberterrorism. Throughout, Easttom blends theory and application, helping you understand both what to do and why. In every chapter, quizzes, exercises, projects, and web resources deepen your understanding and help you use what you've learned–in the classroom and in your career. Learn How To · Evaluate key network risks and dangers · Choose the right network security approach for your organization · Anticipate and counter widespread network attacks, including those based on "social engineering" · Successfully deploy and apply firewalls and intrusion detection systems · Secure network communication with virtual private networks · Protect data with cryptographic public/private key systems, digital signatures, and certificates · Defend against malware, including ransomware, Trojan horses, and spyware · Harden operating systems and keep their security up to date · Define and implement security policies that reduce risk · Explore leading security standards and models, including ISO and NIST standards · Prepare for an investigation if your network has been attacked · Understand the growing risks of espionage and cyberterrorism

Digital Forensics, Investigation, and Response, Fourth Edition examines the fundamentals of system forensics, addresses the tools, techniques, and methods used to perform computer forensics and investigation, and explores incident and intrusion response,

Revised edition of the author's System forensics, investigation, and response, c2014.

Welcome to today's most useful and practical one-volume introduction to computer security. Chuck Easttom brings together up-to-the-minute coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started in the field. Drawing on his extensive experience as a security instructor and consultant, Easttom thoroughly covers core topics, such as vulnerability assessment, virus attacks, hacking, spyware, network defense, passwords, firewalls, VPNs, and intrusion detection. Writing clearly and simply, he fully addresses crucial issues that many introductory security books ignore, from industrial espionage to cyberbullying. Computer Security Fundamentals, Third Edition is packed with tips and examples, all extensively updated for the state-of-the-art in both attacks and defense. Each chapter offers exercises, projects, and review questions designed to deepen your understanding and help you apply all you've learned. Whether you're a student, a system or network

administrator, a manager, or a law enforcement professional, this book will help you protect your systems and data and expand your career options. Learn how to Identify the worst threats to your network and assess your risks Get inside the minds of hackers, so you can prevent their attacks Implement a proven layered approach to network security Use basic networking knowledge to improve security Resist the full spectrum of Internet-based scams and frauds Defend against today's most common Denial of Service (DoS) attacks Prevent attacks by viruses, spyware, and other malware Protect against low-tech social engineering attacks Choose the best encryption methods for your organization Select firewalls and other security technologies Implement security policies that will work in your environment Scan your network for vulnerabilities Evaluate potential security consultants Understand cyberterrorism and information warfare Master basic computer forensics and know what to do after you're attacked

???????????

Part of the Jones & Bartlett Learning Information Systems Security & Assurance Series! System Forensics, Investigation, and Response, Third Edition examines the fundamentals concepts readers must know as they prepare for a career in the cutting-edge field of system forensics.

??????????????????????????????,?????????,??????????????????