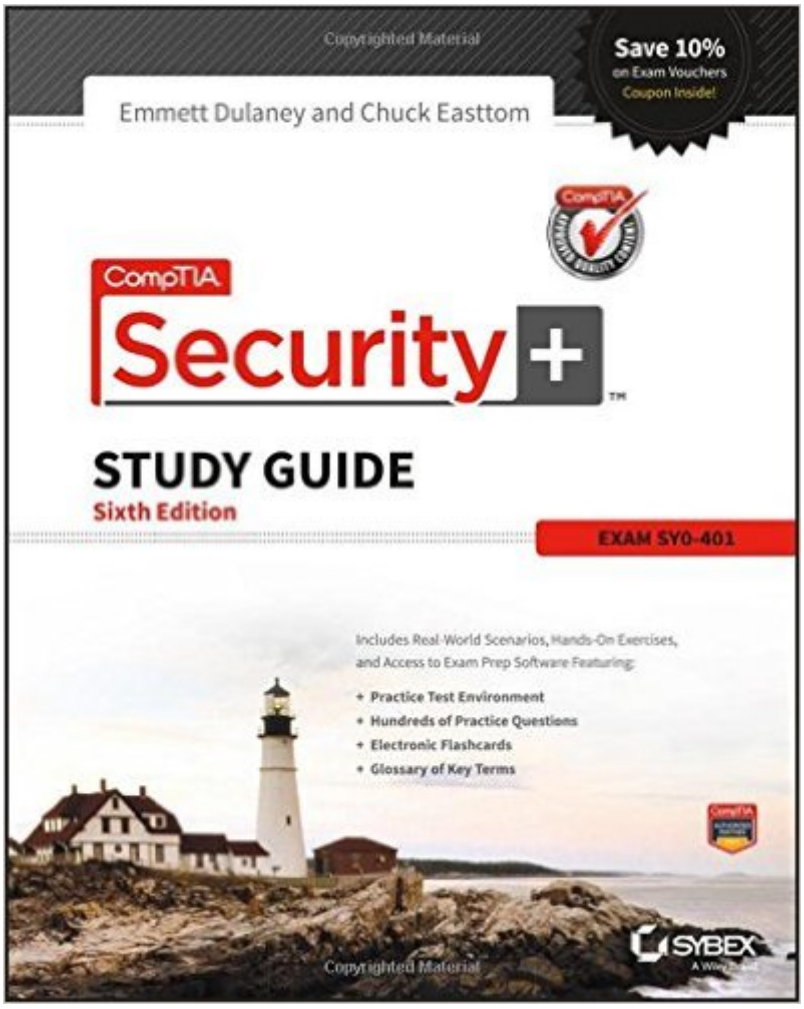
CompTIA Security+ Study Guide: SY0-401



Synopsis

Join over 250,000 IT professionals who've earned Security+ certification If you're an IT professional hoping to progress in your career, then you know that the CompTIA Security+ exam is one of the most valuable certifications available. Since its introduction in 2002, over a quarter million professionals have achieved Security+ certification, itself a springboard to prestigious certifications like the CASP, CISSP, and CISA. The CompTIA Security+ Study Guide: SY0-401 covers 100% of the Security+ exam objectives, with clear and concise information on crucial security topics. You'll find everything you need to prepare for the 2014 version of the Security+ certification exam, including insight from industry experts on a wide range of IT security topics. Readers also get access to a robust set of learning tools, featuring electronic flashcards, assessment tests, robust practice test environment, with hundreds of practice questions, and electronic flashcards. CompTIA authorized and endorsed Includes updates covering the latest changes to the exam, including better preparation for real-world applications Covers key topics like network security, compliance and operational security, threats and vulnerabilities, access control and identity management, and cryptography Employs practical examples and insights to provide real-world context from two leading certification experts Provides the necessary tools to take that first important step toward advanced security certs like CASP, CISSP, and CISA, in addition to satisfying the DoD's 8570 directive If you're serious about jump-starting your security career, you need the kind of thorough preparation included in the CompTIA Security+ Study Guide: SY0-401.

Book Information

Paperback: 552 pages

Publisher: Sybex; 6 edition (May 5, 2014)

Language: English

ISBN-10: 1118875079

ISBN-13: 978-1118875070

Product Dimensions: 7.4 x 1 x 9.3 inches

Shipping Weight: 1.6 pounds (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (107 customer reviews)

Best Sellers Rank: #10,144 in Books (See Top 100 in Books) #9 inÂ Books > Computers & Technology > Certification > Security #30 inÂ Books > Computers & Technology > Security & Encryption #108 inÂ Books > Textbooks > Computer Science

Customer Reviews

I passed the test. No fault to the authors, but practically nothing out there can prepare you for the SY0-401 test. Some people get lucky and get the easy questions like the ones in this book. Others like me get a test that has around 15 questions that aren't covered by this book, or the Comptia Training software called "Cert Master" ,or any other online resource. The test is so hard that if I had failed I would have no idea what to do because so many questions were not covered in this book nor in any training software or practice questions anywhere and because so many are not covered in the book I can't possibly memorize all the hard questions and then google them after the test.My advice is this. Memorize every single protocol and every single port number that has anything to do with any protocol in the book. Some protocols and ports on the test were NOT AT ALL covered in this book so I suggest you use lots of online sources as well as this book.

This is an ideal book to prepare you for the fundamental security exam you need to introduce you to this field, the CompTIA Security+ SY0-401.I'd previously used the last edition as my main source of material when preparing for my own sitting of the exam last Spring, and passed with flying colours thanks to the well laid out chapters, granular and thought out approach - Dulaney really helps you gain a holistic approach to the technologies, methodologies and concepts he covers.This book, if anything, is an improvement on that. The new material is well covered, and integrated in to the more established content in a logical, well explained manner. The diagrams are clean and functional, the end of chapter questions well worded, and the overall editing to a very high standard.This book also came in exceptionally handy while preparing for my first security related job interview, which I subsequently obtained, greatly moving forward my career. It sits pride of place on by desk, next to by SSCP, CASP and CISSP books.As with the previous edition of this book for the SY0-301 exam, I'd recommend this for anyone with an interest in learning about the fundamentals of IT security, both with our without the exam itself on your mind.

I read this book cover to cover, did VERY well on all of the review questions, but failed the exam. I did not fail it by much, but I did nonetheless. The book gets through the material just fine, but don't think that the questions in the book are like the ones in the exam because they aren't even CLOSE to the same. The exam features many "scenario" type questions where you need to pick the BEST answer, so there are multiple right answers, this book does not provide any questions to prepare you for that. Again, the material in the book is good, but to really be successful at the exam with using this book, I feel like you would need to read it 3 or 4 times to memorize every detail of each term/topic.

I read this entire book, but started to regret it about 20% of the way through. The book was included with the Learning Tree course that I took ("CompTIA Security+ Certification Exam Prep"). I liked the succinctness of the class notes/slides over the verbosity of this book. There seems to be a fair amount of extra/unnecessary information in this book that, while sometimes helpful to a sysadmin or security person, does not help you prepare for the exam. For example, there is an exercise on installing Snort in Linux. Why? Knowing that Snort is a popular tool for analyzing network traffic is all you need to know. That other information can easily be looked up if someone was interested but has nothing to do with the Security+ exam. There are several exercises with screen shots that show you how to look up various things on a Windows system, but this mostly just fills up a couple pages for each one without being very useful.There is also repeated information throughout the book. I know that some technologies are applicable to multiple topics, but I'm referring to the exact same definitions and wording used in multiple places. For example, the discussion of tunneling protocols on pages 91 and 144 are the exact same page of text. This is completely unnecessary (you could just mention the protocols again and say they were discussed on page 91 if the reader was just brushing up on that one chapter and not reading the entire book). I saw this again for VLANs, RAID and MAC filtering. I got tired of keeping track of this.In addition, there are several US-centric topics (privacy laws like HIPAA, etc.) that are in the book but would not be covered on an international exam like what CompTIA offers.These issues make the book a longer and more tedious read than it has to be.A bizarre omission is a list of the layers in the OSI seven-layer network model. It's mentioned on page 74 (and later in a discussion of WAFs), but they don't actually say what the layers are, even when referring to "the highest level of the OSI model."Also, the incident response steps in chapter 12 are just plain wrong. The standard was created by the SANS institute and is called PICERL (Preparation, Identification, Containment, Eradication, Recovery and Lessons learned).On the plus side, there are 20 sample questions at the end of each of the 12 chapters that are mostly helpful (answers and explanations are in the back). I would have liked to have seen even more questions including a full-length sample exam at the end, but that's not in the book (but more questions can be downloaded from the publisher's website). In my opinion, a better use of 470+ pages would have been a much more streamlined explanation of the topics/definitions (with no exercises and fewer diagrams) along with several full-length sample exams.Overall, a reasonably thorough presentation of the topics that you need to know for the Security+ exam, but not an outstanding book given the issues and shortcomings mentioned above. If you have notes/slides from a course like the one I took, studying those and a lot of sample exam questions is probably

adequate (as my coworker who passed the test did). If you are not taking a course, this book should help you prepare for the exam, though I recommend also finding as many sample questions as you can in order to become comfortable with the types/formats of questions that are asked on the exam.

I bought three books to study for the Security+ SYO-401 exam and this one, by far, is the best. I like that this book is divided into chapters with chapter quizzes at the end of each chapter. It's an easy way to review the material you just learned before going on to something else. The chapter quizzes also make it easy to refresh yourself on the chapters you have already read. The other books I bought wereÂ CompTIA Security+ Certification Practice Exams, Second Edition (Exam SY0-401) (Certification Press)andÂ Mike MeyersÃ¢Â Â™ CompTIA Security+ Certification Passport, Fourth Edition (Exam SY0-401) (Mike Meyers' Certficiation Passport). Good luck!

This guide is fairly easy to read. It is well organized so that you can pick and choose which subject to study. This is very helpful if you want to distinguish between areas were you're weak and strong. The Kindle version is easy to move around and search for main points of the book. The review questions do a thorough job of testing your knowledge. I would recommend this to my Mom.

CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) CompTIA A+: All-in-One Certification Exam Guide for Beginners! (CompTIA A+, Programming, Computer Language) CompTIA Advanced Security Practitioner (CASP) CAS-002 Cert Guide