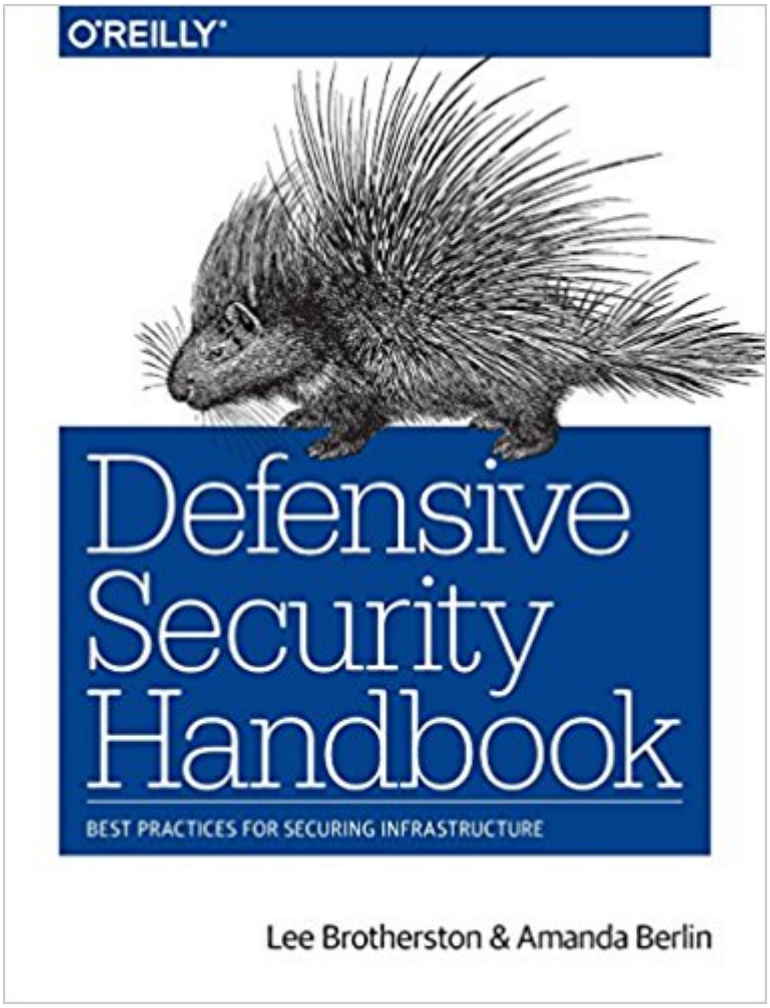
Defensive Security Handbook: Best Practices For Securing Infrastructure



Synopsis

Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations donâ ™t have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost.Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks.Learn fundamentals of starting or redesigning an InfoSec programCreate a base set of policies, standards, and proceduresPlan and design incident response, disaster recovery, compliance, and physical securityBolster Microsoft and Unix systems, network infrastructure, and password managementUse segmentation practices and designs to compartmentalize your networkExplore automated process and tools for vulnerability managementSecurely develop code to reduce exploitable errorsUnderstand basic penetration testing concepts through purple teamingDelve into IDS, IPS, SOC, logging, and monitoring

Book Information

Paperback: 284 pages

Publisher: O'Reilly Media; 1 edition (April 21, 2017)

Language: English

ISBN-10: 1491960388

ISBN-13: 978-1491960387

Product Dimensions: 6.9 x 0.5 x 9 inches

Shipping Weight: 1 pounds (View shipping rates and policies)

Average Customer Review: 4.5 out of 5 stars 22 customer reviews

Best Sellers Rank: #53,680 in Books (See Top 100 in Books) #5 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Disaster & Recovery #33 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #64 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

View larger From the Preface Our Goal Our goal is to not only make this a standard that can be applied to most enterprise networks, but also be a little entertaining to read along the way. There are already deep-dive standards out there from a variety of government and private organizations that can drone on and on about the validity of one security measure or the next. We want this to be an informative dialog backed by real-life experiences in the industry. There will be good policy, best practices, code snippets, screenshots, walkthroughs, and snark all mixed in together. We want to reach out to the massesÃ¢Â Â”the net admins who canÃ¢Â Â™t get approval to hire help; directors who want to know they arenÃ¢Â Â™t the only ones fighting the battles that we see day in and day out; and the people who are getting their hands dirty in the trenches and arenÃ¢Â Â™t even close to being ready to start down the path of reading whitepapers and RFCs. Who This Book Is For This book is designed to serve as a Security 101 handbook that is applicable to as many environments as possible, in order to drive maximum improvement in your security posture for the minimum financial spend. Types of positions that will be able to take away knowledge and actionable data from this include upper-level CIOs, directors, security analysts, systems administrators, and other technological roles. Navigating the Book We have deliberately written this so that you do not have to adopt an all-or-nothing approach. Each of the chapters can serve as a standalone body of knowledge for a particular area of interest, meaning that you can pick and choose which subjects work for you and your organization, and ignore any that you feel may not apply. The aim is not to achieve compliance with a particular framework or compliance regime, but to improve on the current situation in sensible, pragmatic, manageable chunks. We have purposefully ordered this book to begin with the fundamentals of starting or redesigning an information security program. It will take you from the skeleton steps of program creation on a wild rollercoaster ride into the depths of more technical topics.

Lee Brotherston is a Senior Security Advisor with Leviathan Security, providing Information Security consulting services to a range of clients. Having spent more than a decade in Information Security, Lee has worked as an Internal Security resource across many verticals including Finance, Telecommunications, Hospitality, Entertainment, and Government in roles ranging from Engineer to IT Security Manager.Amanda Berlin is an Information Security Architect for a consulting firm in Northern Ohio. She has spent over a decade in different areas of technology and sectors providing infrastructure support, triage, and design. Amanda has been involved in implementing a secure Payment Card Industries (PCI) process and Health Insurance Portability and Accountability Act (HIPAA) compliance as well as building a comprehensive phishing and awards-based user

education program. She is the author for a Blue Team best practices book called "Defensive Security Handbook: Best Practices for Securing Infrastructure" through O'Reilly Media. She is a co-host on the Brakeing Down Security podcast and writes for several blogs. On Twitter, she's @InfoSystir.

This book is meant as a primer for beginners. It lightly touches on several areas within defensive security. If your just getting started it is a worthwhile read. For those more seasoned some of these topics may act as a reminder of things to consider if there not in your wheel house.

Amazingly written. Tons of resources to use and the information is top notch from professionals in the area. I definitely recommend.

Amazing and well written. This handbook should be on your shelf if you are currently working or thinking of entering the Information Technology (IT) or Security (Infosec). It breaks down topics into understandable steps and concerns. This will really help you get your infosec house in order. By following the topics laid out in this book you will drastically improve your security posture and go a long way in thwarting cyber issues from threat actors like hackers.I have worked in Information Security for over a decade, holding several industry certificates, and wish I had a book like this when I was entering the workforce. This book is a treasure trove of gems that take years to learn on your own. Just pick it up today.

I cannot tell you how appreciative I am of this book and its authors. I am deeply grateful for their effort in starting at the beginning and not being the typical "if you don't know this, it's because you are an idiot" approach. In fact, I was so impressed with this book I ordered 2 more and made it assigned reading for my newest team members. Do not let the naysayers deter you from learning something new. If you have been at this a while, sure this may be elementary. If you are needing an insight in what to do next, read this book. Or if you find yourself needing a good primer this is it. Don't let your pride and the ego a few allow you to miss out on something well thought out and executed.

I purchased this book directly from O'Reilly during the pre-order push. It's clearly a 101-type of book, and while I noticed some grammatical issues, I blame the editors on the publishing side for not catching them.The information collected here is something I wish I had decades ago when I

entered IT. An example of this can be seen in Chapter 10, Microsoft Windows Infrastructure. While some, if not all of the information in this section might be second nature for an experienced administrator Ã¢Â Â“ those just getting started can avoid some common and painful mistakes after reading this.Think of this book as a reference manual. A collection of tips that can be used to answer basic questions in some cases, or an outline to help someone who is just getting started. It's not going to solve all your problems, and you're not going to become a super admin after reading it. However, when comes to building a security program, this book will give you a decent start.

This book does not teach you how to actually protect yourself. It does talk about security items from an extremely high level. It does briefly mention some random tools but nothing in detail. If you are looking to protect yourself from Cyber threats this is not the book for you. If you are looking for a high level introduction to Cyber threats in the corporate world this is a great entry level book.

Very pleased with this book, a great intro for anyone entering the field yet detailed and advanced enough for the seasoned vet.

If you're an IT manager or sysadmin who is looking to implement an InfoSec program at your company, this book provides an excellent starting point. The authors walk you through developing policies and procedures, crafting compliance and incident response plans, how to develop a physical security program, and more. As a policy wonk, I especially enjoyed the inclusion of disaster recovery planning, a crucial facet of InfoSec that is far too often overlooked by many organizations.If you are an IT generalist who is interested in learning the basics of Blue Teaming, this book is an excellent place to start.

(Transnational Crime, Crime Control and Security) Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) Critical Infrastructure Security: Assessment, Prevention, Detection, Response (WIT Transactions on State-of-the-art iin Science and Engineering) Critical Infrastructure: Homeland Security and Emergency Preparedness, Third Edition Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection Business Data Communications- Infrastructure, Networking and Security (7th Edition) Urban Survival Handbook: The Beginners Guide to Securing Your Territory, Food and Weapons (How to Survive Your First Disaster) Social Security Handbook 2017: Overview of Social Security Programs Handbook of Financial Cryptography and Security (Chapman & Hall/CRC Cryptography and Network Security Series) Defensive Shield: An Israeli Special Forces Commander on the front line of counterterrorism