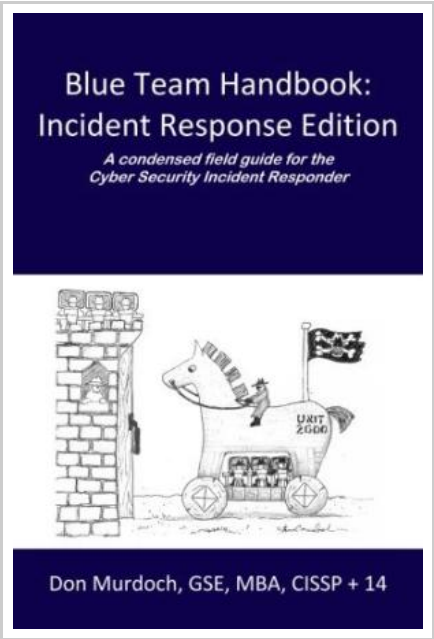

DOWNLOAD PDF

Blue Team Handbook: A Condensed Field Guide for the Cyber Security Incident Responder

By Don Murdoch Gse

Createspace, United States, 2014. Paperback. Book Condition: New. Incident Response ed.. 226 x 150 mm. Language: English . Brand New Book ***** Print on Demand *****.Updated, Expanded, and released to print on 10/5/14! Complete details below! Two new sections, five protocol header illustrations, improved formatting, and other corrections. The Blue Team Handbook is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics. The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way. Version 2.0 updates: - *** A new section on Database incident response was added. - *** A new section on Chain of Custody was added. - *** Matt Baxter...

READ ONLINE
[2.96 MB]

Reviews

Absolutely essential read publication. it absolutely was writtern very completely and valuable. It is extremely difficult to leave it before concluding, once you begin to read the book.

-- ***Sarai Lebsack***

Thorough guide for book enthusiasts. I am quite late in start reading this one, but better then never. Your lifestyle span will be transform when you total reading this article book.

-- ***Lindsey Larson***