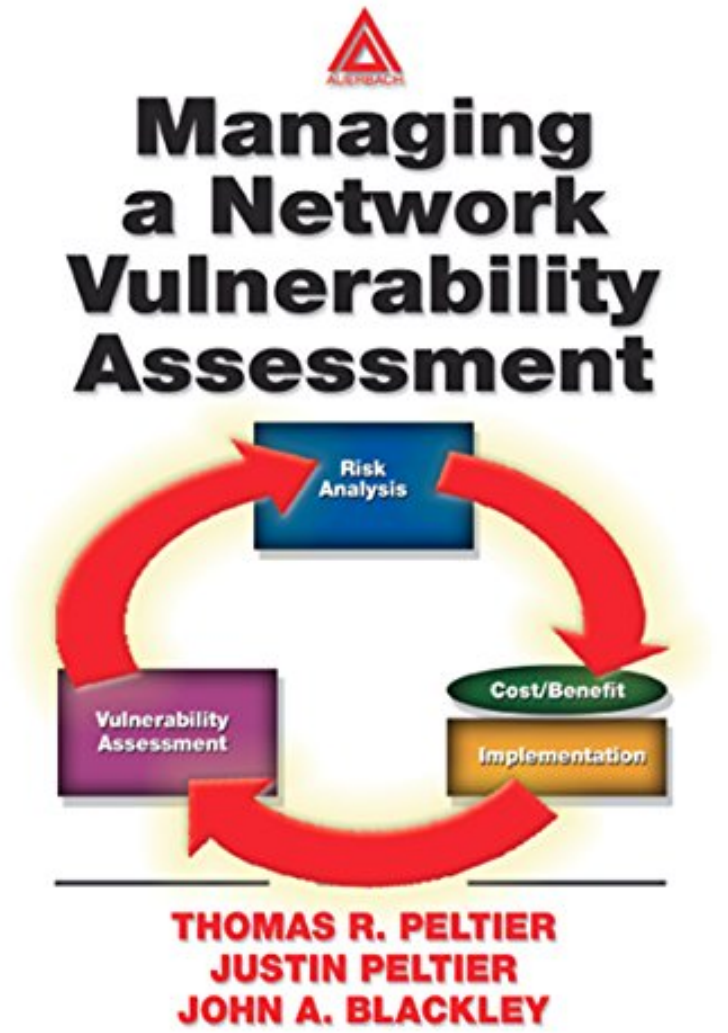
Managing A Network Vulnerability Assessment

Thomas R. Peltier, Justin Peltier, John A. Blackley
*ebooks | Download PDF | *ePub | DOC | audiobook*



#3720650 in eBooks 2003-05-28 2003-05-28File Name: B00UV9JOPC | File size: 56.Mb

Thomas R. Peltier, Justin Peltier, John A. Blackley : Managing A Network Vulnerability Assessment before purchasing it in order to gage whether or not it would be worth my time, and all praised Managing A Network Vulnerability Assessment:

4 of 5 people found the following review helpful. Read this book before you scanBy Ben RothkeWhen performing vulnerability assessments, a mistake many people make is that they will use simply run some software tools, without taking a big picture look at things.Such a haphazard approach will not be effective for large enterprise networks. With that, Managing A Network Vulnerability Assessment, gives the reader a all-inclusive framework for running a network vulnerability assessment.The book goes over issues such as scooping, assessment and scanning

methodologies, reports, etc.The main part of the book is quickly readable at 187 pages.Appendix A is an ISO 17799 self -assessment checklist, which can be used to validate a system to an external reference. There are a few other checklists.Before anyone blindly runs a network scanner, they should read this book first to ensure that their scanning is done effectively and productively.11 of 12 people found the following review helpful. Good, but with some weaknessesBy AntonThis is a good book, especially enlightening for those "security pros" who think that running a major commercial scanner and then printing a 500 page report constitutes "vulnerability assessment"!The book clearly favors management skills over technical ones. It contains many valuable tidbits on things like proper process, methodology, policy, planning and organization. Project scoping is well-covered as well as documentation development (looks good for consultants). The book also relates its assessment methodology to ISO 17799 standard.The book advocates a holistic approach, assessing both policy and technical vulnerabilities and not just scan-and-leave. It contains a nice policy review guidelines by the area of security policy. On the other hand, the section on actually conducting the technical assessment is two pages long out of the books's 186 total number of pages. Lots of "what" with little "how".The technical tools section is a joke. Some examples include: "tcpdump" is absent from the sniffers section, "nmap" - from scanners (mentioned twice in application fingerprinting tools though), queso (which is not currently updated) is recommended, NetSonar is called a promising scanner (the product is long discontinued). You wouldn't believe it was supposedly written in 2003! Other tool descriptions are generic and seem inspired by product web pages rather than the actual tool use. In addition, there is nothing worse than outdated website guide and this book is firmly there :-) No Google, attrition.org is described as a major defacement mirror (its that no more), etc.It is interesting how authors define "vulnerabilities" as published holes or even well-publicized ones (since, according to them, even a web post to a "less known website" supposedly doesn't make the vulnerability public!) Thus, the book is mostly about 'script kiddie defense'. But then again - it does make sense to start somewhere and if you are being constantly "owned" by such attackers - you clearly need to work on your vulnerabilities.Overall, the information in the book is well-organized, I liked chapter summaries and lots of various assessment checklists. Beware of typos though, the book has lots of them.Anton Chuvakin, Ph.D., GCIA, GCIH is a Senior Security Analyst with a major information security company. His areas of infosec expertise include intrusion detection, UNIX security, forensics, honeypots, etc. In his spare time, he maintains his security portal info-secure.org8 of 11 people found the following review helpful. Good content, again horrible writingBy E van EerselAfter having read "Information Security Risk Analysis"[ISRA], written by Peltier as well, I was somewhat unwilling to read this book, particularly because of the crappy proofreading of ISRA. Now that I finished this book, I can only say it's not as disappointing, but it's not a jewel either.The content of the first 5 chapters is good. The writers clearly show that a structured approach to vulnerability assessments should be taken instead of blindly running a network vulnerability scanner and passing those (incomplete) results on to management. The methodology they propose is explained clearly, with good emphasis on practical issues (picking assessment team members, assessment team roles, customer feedback, report structures etc). In less than 80 pages they lay it out clearly.Unfortunately, after describing the administrative part of assessments, they dedicate 60 to 70 pages to tool description. The info provided here is far from new and not set up particularly well. It's simply a list of scanning tools, including vendor comments, which could have been left out, since it's not a product marketing book. The tools and explanations can be found on a million other web pages, as well as in superb books such as Hacking Exposed.The appendices are good. There's an ISO 17799 checklist with loads of useful questions one can ask during a vulnerability assessment, a very basic Windows vulnerability checklist (could have been left out), tables which I loved to have seen on an accompanying CD, as well as a sample vulnerability report.For the content the bnook deserves 4 stars.The writing, however, is horrible, which isn't surprising, given ISRA (see my review of that book to see what I mean). Again, loads of typos, and an unprecedented use of Ctrl+C and Ctrl+V. It even goes so far, that the summary of chapter 3 (pages 45/46) equals the summary of chapter 4 (page 69). Copy, paste, finished! Not suprisingly either is that the Acknowledgements section starts off with the exact same paragraph as in ISRA. Just copy and paste, who'll notice?One of my favorite typos can be found on page 46, when the authors refer to the Windows vulnerability checklist as mentioned above:[...]windows NT 4.0 Server 4.0 was developed by Bob Cartwright, CISSP, of ESAAG, Concord, Calfornia [sic], and is presented here with his permission.[...]Sometimes the writers contradict themselves, or at least should have explained the content a lot better. See e.g.:- page 82: e-mail is a topic-specific policy.- page 83: e-mail is a system- and application-specific policy.Another annoyance is the many references to books that they wrote themselves or were published by Auerbach (see pages xii, 2, 62, 63, 66, 81; I might have missed some). Again a nice marketing move, but annoying after two or three references.So: 1 star for the writing. Averages 2.5 stars, which I'll round off to three stars, since the book outclasses ISRA, which I gave 2 stars.

The instant access that hackers have to the latest tools and techniques demands that companies become more aggressive in defending the security of their networks. Conducting a network vulnerability assessment, a self-induced hack attack, identifies the network components and faults in policies, and procedures that expose a company to the damage caused by malicious network intruders.Managing a Network Vulnerability Assessment provides a formal framework for finding and eliminating network security threats, ensuring that no vulnerabilities are overlooked. This

thorough overview focuses on the steps necessary to successfully manage an assessment, including the development of a scope statement, the understanding and proper use of assessment methodology, the creation of an expert assessment team, and the production of a valuable response report. The book also details what commercial, freeware, and shareware tools are available, how they work, and how to use them.By following the procedures outlined in this guide, a company can pinpoint what individual parts of their network need to be hardened, and avoid expensive and unnecessary purchases.

Readers will find detailed definitions, thorough explanations, step-by-step procedures, and sample reports to guide them through a network vulnerability assessment (NVA). hellip; [The book] is clear and easy to read, conveying the authors' outstanding grasp of the material. Despite the extremely detailed content, the presentation is not too technical or confusing. Numerous graphs, sample reports, and computer illustrations effectively support the text. hellip; Of the many readers who would benefit from this work, security managers responsible for computer protection will learn how to conduct an NVA. IT professionals will benefit from the exposure to detailed security concepts and procedures. Finally, college instructors and students will find that the work serves as an excellent educational resource. - Security Management, Sept. 2004Promo CopyAbout the AuthorJim C. Harper is Assistant Professor at North Carolina Central Central University.