BOOK REVIEWS

Diane Barrett
Book Review Editor
University of Advancing Technology
2625 W. Baseline Rd
Tempe, AZ 85283

If you have any suggestions on books for review, would like to write a book review for us, or have any comments or concerns on the book reviews published in this column, please feel free to send an email to Diane Barrett, the editor for this column, at dm_barrett@msn.com.

BOOK REVIEW

Wilhelm, T. (2013). *Professional Penetration Testing: Creating and Learning in a Hacking Lab 2E*. Waltham, MA: Syngress, 464 pages, ISBN-10: 1597499935; ISBN-13: 978-1597499934, US$79.99

Reviewed by ***Joshua Bartolomie, CISSP, CEECS, CFCE, DFCP, CRISC, CSM***

Organizations often strive for proactive information security programs in an effort to limit occurrence and impact of security breaches. However, traditional security programs run the risk of being unable to provide adequate insight and proactive awareness into real attack vectors that may exist within their organizations. With attack methods and efforts becoming increasingly aggressive, and effective, organizations must take equally assertive measures to protect their critical information and assets. Penetration testing is one of those tools that is often misunderstood, overlooked, and undervalued. A true adversary would not hesitate to exploit every potential to gain entry or cause a disruption to their target.

Wilhelm (2013) states in his introduction that the book is specifically focused on providing a mannerly layout so that readers can better identify, learn, and practice the tools, techniques, and tactics that fall within their respective skill and knowledge level. This book consists of 15 chapters that provide a range of topics that present the reader with a solid set of practical and usable information in this highly technical realm. I was very pleased to note that the author stressed and covered the essential, and often glossed over, non-technical components of penetration testing activities including ethics, program management, and reporting. To provide that aforementioned level-set of information scope and scale, each chapter beings with a breakdown that

delineates the covered topics. This simple addition enhanced and provided a level-set expectation of the information that was covered within each chapter.

The authors writing style was very easy to follow and the breakout of tips and references provided a wealth of external resources, tips, and advice that highlight the author's lessons learned and real world insights within the penetration testing field. Where specific frameworks, organizations, or tools are highlighted the author makes every attempt to compare and contrast more than one of each, and relays to the reader that there is not a single solution for everything that needs to be considered in this field. This consistent checks-and-balances approach is refreshing and provides the reader with a broad base of knowledge and understanding of the diversity within this field and how there is no 'one shoe fits all' solution.

The first chapter of the book provides an overview of the design and information flow for the book, the topics that can be expected to be covered, and details for obtaining supplemental information, tools, and templates. In an effort to provide the reader with continually up-to-date information and resources, Wilhelm (2013) maintains a dedicated website as a central location to obtain the tools, virtual machine images, procedures, and templates referenced throughout the book. Subsequent review of this website found it to be regularly updated and a robust repository of knowledge and resources.

Following the first chapter, the author dedicates the next chapter wholly to the discussion of ethics. I was appreciative to see ethics addressed and discussed up front, because a lot of texts on this subject matter purely focus on the technical aspects of penetration testing, or at best quickly gloss over an individual's responsibilities and related considerations. Wilhelm (2013) provides concrete examples of multiple ethical charters and standards that are employed by well-known information security organizations as well as the importance of consciously recognizing ethical and legal obligations.

The third chapter focuses on getting a baseline testing environment established for the reader to being testing penetration testing tools and techniques in a safe and controlled environment. The author details multiple architectural implementation and several considerations that the reader should be conscious of when designing a testing environment. The author includes details regarding multiple tools, virtualization technologies, prebuilt images, and live CDs that can greatly assist the reader in repeatedly getting an environment setup quickly and easily. Additional considerations are presented to the reader, providing logical progression paths for the continued expansion and evolution of testing environments for continual expansion of their skill set and capabilities.

Chapters 4 through 8 bring the reader directly to the initial phases of the penetration testing process including a discussion on the pros and cons of multiple penetration testing frameworks, passive and active information

gathering, vulnerability identification, and initial vulnerability exploitation. Common tools and techniques are documented and provide the reader with a beginning knowledge on how to conduct open source intelligence gathering as well as how to gain an initial baseline of their target environment. Wilhelm (2013) again goes out of his way to call out and stress the soft skills that are essential, but often overlooked, within penetration testing and dedicated the fifth chapter specifically to the topic of penetration project management. While the core of a penetration test focuses on the technical skills and prowess of the penetration tester, being able to manage time, resources, information flow, and teammates is often paramount to the successfulness of the engagement and satisfaction of the customer.

Following the sequence of progressively technical topics, chapters 9 through 13 highlight the technical core that most consider to be true penetration testing and include topics such as local system attacks, privilege escalation, choosing appropriate targets, and web based application attack techniques. The author provides sufficient examples and explanations for each of these topics. Through the use of the lab environment that was defined within the second chapter, readers are able to follow the author's examples and recreate the documented and expected results in a sufficient manner to better grasp the overall process.

Chapter 14 provides the reader with insight into another soft skill that anyone within a technical field is required to utilize, reporting. A penetration test could be a complete success from a technical stance, however if the penetration tester has not, or cannot, properly document their activities, findings, and subsequent details then it serves little purpose or benefit for their customer. In this chapter, Wilhelm (2013) also stresses that the job of a penetration tester is not to 'tell' the customer what to do, which is something that all too many attempt to do, but rather to provide the customer with appropriate advice and remediation recommendations, allowing the customer to decide future actions.

The last chapter of the book addresses one of the more common questions that a newcomer to this field often finds themselves asking, "How do I make a career out of this?" The quick truth of any technical field, such as penetration testing, is that if you do not stay up-to-date and are not constantly learning, you are doing yourself, your customers, and your field a disservice. This is another area in which the author provides a substantial amount of real-world and practical advice, information, and resources to help those in the field determine next steps, begin networking with other penetration testers and security personnel, and begin establishing a network of contacts and intelligence sources. A wide berth of career and advancement resources and advice is highlighted including technical, and non-technical, certification programs, membership with associations and organizations, and advice on resume writing, volunteering, and internships.

It is implausible for any book to delve into all potential examples and details surrounding the multitude and constantly emerging attack methodologies, techniques, tools, and tactics that a penetration tester can utilize in the course of their work. However, Wilhelm (2013) does a good job of providing sufficient details, references, methodologies, and relevant examples to provide the reader with a understanding of the topics being discussed and to start an overall learning progression within this dynamic field.

I was impressed with the overall flow of information that was presented to the reader, as well as the interweaving of technical and soft skills that are required to successfully establish oneself as a penetration tester. While this text may not hold as high of relevance for seasoned penetration testers or as a go-to reference, it is a solid resource for those new to the field and for those that may be looking to expand their skill set and understanding.