

## Book Review: Dissecting the Hack: The F0rb1dd3n Network, Revised Edition

Review by RichM

&ldquo;Dissecting the Hack: The F0rb1dd3n Network, Revised Edition&rdquo; by Jayson E. Street, Kent Nabors and Brian Baskin is not intended for the average reader of The Ethical Hacker Network, and this is what makes the book so intriguing. The forward specifically points out how hard it is to speak with management about security, and how lost they get. It even comes complete with an explanation of the &ldquo;glazed over eyes.&rdquo; Talking with decision makers is a topic often overlooked, and something that needs to be explored and dissected. At the end of the day, no matter how great you think your idea is, if you don't get management buy-in, the idea dies and you are forced to re-bury your department's head back in the proverbial sand.

I would imagine that at this point most readers are affirmatively shaking their heads, because by and large most managers/executives know very little about information security. I personally have dealt with this on more than one occasion, painstakingly detailing the largest (most obvious) vulnerabilities and the most cost efficient way to mitigate these risks. After I finished (each time) I was met by the aforementioned blank stares and confused looks. I was thanked for my effort, no changes were made, and I eventually left frustrated and annoyed. My chances of getting through to these decision makers may have improved if &ldquo;Dissecting the Hack&rdquo; had been in my arsenal.

[del.icio.us](http://del.icio.us)

Discuss in Forums {mos\_smf\_discuss:Book Reviews}

## Part 1A

On the surface, this book is a quick read about international espionage and some curious hackers that find themselves in a situation that is way over their heads. As you read the book, however, you realize the author has sucked you in to a page turner that perfectly illustrates how important security is, and what can happen if defense in-depth is not implemented properly. I would have liked more character development, but it is clear that the story is secondary. There is a lot of information that is covered, which may be completely foreign to the uninitiated. But by keeping the details to a minimum, the technical stuff rises to the surface and becomes the focus of the book. To help illustrate how helpful this book is for the non-techie, I asked a management level professional to read Part 1 and give me their honest opinion.

## Part 1B: Review by Non-techie

As someone with little to no IT knowledge, I was nervous to begin the novel. Most books that are focused on a particular topic (Sci-Fi, IT, etc.) are often difficult to follow, because the requisite knowledge is not there. This leads to a reader without this knowledge to gloss over a lot of the details. There is also the exact opposite, books which are too dumbed down or, even worse, completely incorrect. Then the reader just feels insulted. This book struck a nice balance. It wasn't overly complicated, and there was no need to skip paragraphs. It was informative enough that it piqued my curiosity multiple times, and I sought out additional information. The book is a straightforward read and kept my attention. In the end, I'm not sure if I would read another book of this type, but I am not ruling it out either.

## Part 2

I have attended multiple "hacking courses" both consisting of online course material as well as courses that are taught in person. While there is a wealth of knowledge that can be gained, sometimes taking part in those classes can be cost prohibitive. Those looking for this type of knowledge are forced to seek out bits and pieces of these courses, often missing vital information. "Dissecting the Hack" now puts this information in the hands of virtually anyone that has a desire to learn. This text is the only book a person new to information security needs in order to get a thorough overview of basic hacking and the main steps including information gathering, identification, footprinting, enumeration, exploitation and covering your tracks. Dissecting will not make you l33t, but it will give an individual with a desire to learn about information security a solid foundation to build on.

## Conclusion

When I read Part 1, I initially thought, "What a great way to trick (scare) a Manager/Executive into fixing obvious security vulnerabilities." It may not make an executive get what you do, but it levels the playing field. Most importantly it keeps the door open for further discussion. However, as I read the book (and became engrossed in the story), the more I realized that this book was of a genre that we do not have enough books in. We need more books that are entertaining and spread technical knowledge simultaneously. Finally, I read Part 2 and realized that there is actually a separate and third audience, the newbie crowd. I would have loved to have had this book available when I first started

learning infosec. There is something to be said about teaching yourself through exploration and constant searching, but to have all this information at my fingertips would have streamlined the process and cut the learning time in half.

Clearly this book is a multi-purpose piece of reference that should be put on all IT Departments' reference shelf. Of course, like most things in life, going back to basics can be good even for the most seasoned of penetration testers. I defy anyone to read Part 2 and not walk away with a single bit of new learned information.

Read other articles by RichM in his EH-Net Column.