The basics of hacking and penetration testing: ethical hacking and penetration testing made easy


Date Reviewed: May 30 2012

This is a book on the “dark side” of information technology, as it describes how the vulnerabilities of systems and networks can be exploited to gain unauthorized access. It is important that students and practitioners understand how advanced the state of the art in exploiting vulnerabilities is, since only a deep understanding of the problem will lead to good solutions.

Engebretson presents an overview of the tools a penetration tester might use to test the vulnerability of a system or network. The tools are described in some detail, mainly focusing on the syntax of commands. The interpretation of the results is described only superficially. The reader is left wondering what exactly is going on and why. Let me give a few examples to illustrate this point.

In several places, the book warns the penetration tester that stealth is important. However, there is no information on how stealthy the various tools are, nor is there a discussion on how to use the tools in the stealthiest manner.

The book often suggests that the reader should learn about a particular topic—for example, Internet protocols (p. 53): “To truly master port scanning you will need to have a solid understanding of these protocols.” Another example is the discussion (p. 79) of the differences between bind and reverse payloads. The book provides some of the facts, but it does not explain the relevance or the underlying principles. There are no pointers to further studies, references, or even Web pages. What exactly do we have to learn? Why? Where can we find the relevant material?

I have read books similar to this one, but on topics that are far from my area of expertise (for example, Nanotechnology for dummies [1]), which I found more readable because the relevance of the topic was clear, and links to further information were provided. In summary: if the reader knows little about networking and is looking for a book that will get him started on penetration testing, then this book may be useful. But it won’t get the reader anywhere near successful penetration tests, because a much better understanding of networking than the book provides will be needed. Unfortunately, the book does not even try to point readers in the right direction to becoming proficient penetration testers.