The Basics Of Hacking And Penetration Testing: Ethical Hacking And Penetration Testing Made Easy (Syngress Basics Series)
**Synopsis**

The Basics of Hacking and Penetration Testing serves as an introduction to the steps required to complete a penetration test or perform an ethical hack. You learn how to properly utilize and interpret the results of modern day hacking tools; which are required to complete a penetration test. Tool coverage will include, Backtrack Linux, Google, Whois, Nmap, Nessus, Metasploit, Netcat, Netbus, and more. A simple and clean explanation of how to utilize these tools will allow you to gain a solid understanding of each of the four phases and prepare them to take on more in-depth texts and topics. This book includes the use of a single example (pen test target) all the way through the book which allows you to clearly see how the tools and phases relate.

Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Backtrack Linux distribution and focuses on the seminal tools required to complete a penetration test.

**Book Information**

Series: Syngress Basics Series  
Paperback: 180 pages  
Publisher: Syngress; 1 edition (August 4, 2011)  
Language: English  
ISBN-10: 1597496553  
Product Dimensions: 7.5 x 0.4 x 9.2 inches  
Shipping Weight: 1 pounds  
Average Customer Review: 4.3 out of 5 stars  
Best Sellers Rank: #214,441 in Books (See Top 100 in Books)  
#52 in Books > Computers & Technology > Security & Encryption > Encryption  
#56 in Books > Computers & Technology > Security & Encryption > Cryptography  
#163 in Books > Computers & Technology > Internet & Social Media > Hacking

**Customer Reviews**

Very easy to read, very fun and interesting! I'm more into databases but the way everything integrates now in the current IT world, I realized that I need to get a better understanding of how to
protect my database servers (or provide additional value to my Projects), network or at least, being able to discuss about security with my network team without feeling lost. This book is about how to protect yourself from the very "nasty" and "wild" Internet world we all are living in. It will change your false sense of security at work or home, trust me! Even though this is not an in-depth volume about PEN testing tools or techniques, this book delivers what is promised on the cover and much more! All chapters are very coherent, meticulously structured and nicely integrated between each other thanks to the PEN test process it follows. There are even suggestions about how to test all the examples in a secure and practical way. Of course, a virtual lab using any of the virtualization technologies is highly advised. The author suggests VMware, I used Parallels, but there are several free tools out there including Virtual PC or VirtualBox, both are free as well. The book uses Metasploit framework/software for its examples but makes strong emphasize on concepts rather than tools, which it is very good in my opinion because whatever is being taught can be later extrapolated using other tools. PEN test is more a process than mere scripts and tools. I also like the fact that you don’t need a very strong knowledge on networking, cryptography or C++ in order to understand this book.

Download to continue reading...