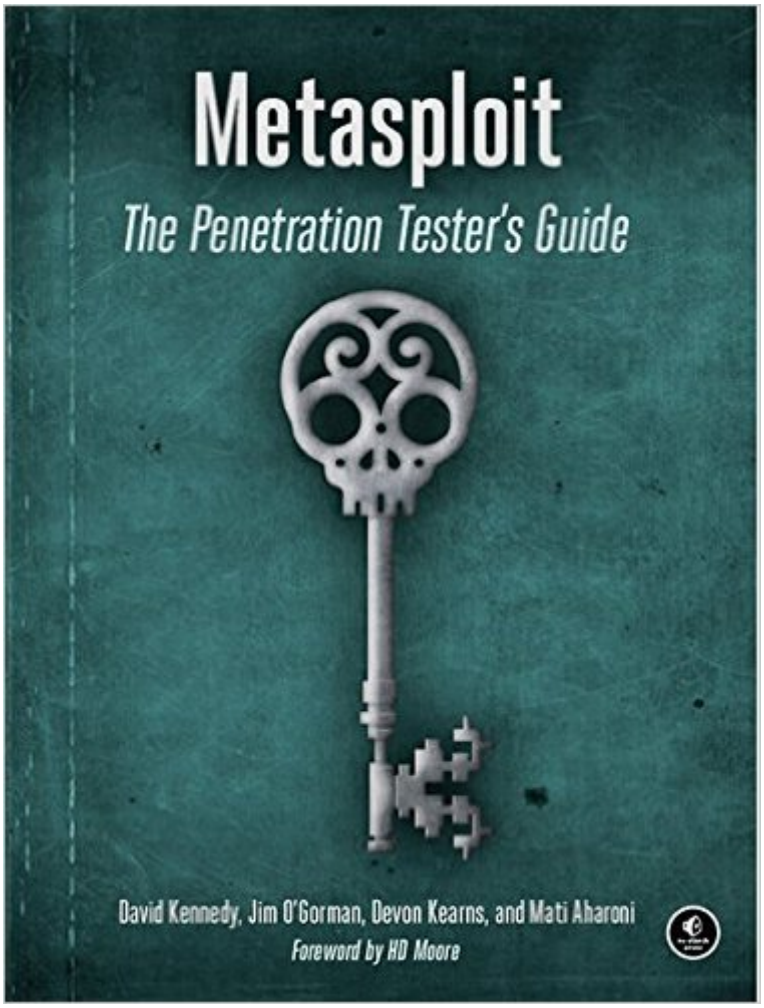
Metasploit: The Penetration Tester's Guide



Synopsis

"The best guide to the Metasploit Framework."—HD Moore, Founder of the Metasploit Project The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester’s Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you’ve built your foundation for penetration testing, you’ll learn the Framework’s conventions, interfaces, and module system as you launch simulated attacks. You’ll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: Find and exploit unmaintained, misconfigured, and unpatched systemsPerform reconnaissance and find valuable information about your targetBypass anti-virus technologies and circumvent security controlsIntegrate Nmap, NeXpose, and Nessus with Metasploit to automate discoveryUse the Meterpreter shell to launch further attacks from inside the networkHarness standalone Metasploit utilities, third-party tools, and plug-insLearn how to write your own Meterpreter post exploitation modules and scripts You’ll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else’s to the test, Metasploit: The Penetration Tester’s Guide will take you there and beyond.

Book Information

Paperback: 328 pages
Publisher: No Starch Press; 1 edition (July 25, 2011)
Language: English
ISBN-10: 159327288X
ISBN-13: 978-1593272883
Product Dimensions: 7 x 1.2 x 9.2 inches
Shipping Weight: 1.4 pounds (View shipping rates and policies)
Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (116 customer reviews)
Best Sellers Rank: #30,381 in Books (See Top 100 in Books) #17 inÂ Books > Computers & Technology > Security & Encryption > Viruses #27 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #29 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

I’m an accomplished test automation/performance engineer, but one area of testing that I’m pretty green at is penetration testing. Luckily, I came across Metasploit: The Penetration Tester’s Guide, which is a book about penetration testing using the opensource Metasploit Framework testing and is a great introduction to security testing in general. Since I’m a complete novice when it comes to Metasploit, the book was great for getting me started with the basics of the framework. (A more experience Metasploit user, however, will probably want to read something a bit more advanced.)The book assumes the reader has zero experience, and begins with a brief history of Metasploit and how to install it. Although you don’t need to be a programmer to read it, most of the examples are written in Ruby and Python. You should also be familiar with Linux and how to set up VMs.Overall, the book is written with a hands-on, tutorial-like style that is great for people like me who prefer to learn by doing. The book is a progression, beginning by establishing the methodologies/phases and terminology of penetration testing and an intro to the utilities and functions within the Metasploit framework. The first few chapters are a great help in getting up to speed on what penetration testing is and provide a nice overview of the different phases of a penetration test. The author then walks you through how to identify different types of vulnerabilities and how to exploit them using the tool. I really liked the sections on how to attack MS SQL, Browser-Based & File exploits and Social Engineering attacks. Many different modules of the framework are covered, as well as how to create a module. The book ends with a realistic simulation of an actual penetration test.

The book covers the basics of using Metasploit with other related tools (SET and Fast-Track). If the reader is expecting to become a penetration tester expert by reading this book then I will say that the expectations are wrong. The author has managed to put in a single book the methodology used for penetration testing, named as PTES (Penetration Testing Execution Standard) and described as the redefined methodology for penetration testing and a general overview of the Metasploit framework, how it works, how is composed and how you can leverage the power of using this framework to make adaptations in different situations or scenarios. Also the author has recalled the fact that every situation is different and the penetration tester should deal with obstacles that he may find in the way to exploit a system.The author begins the book by describing the PTES methodology and also referring the user to the penetration standard organization website in order to get more information (for people that are new in penetration testing). Then the author moves on with the metasploit basics, explaining the terminology and how the framework is composed. It also makes a

brief explanation about Metasploit Express and Metasploit Pro. In the Chapter 2 the book deals with an important step (information gathering), if not the most important, when conducting a penetration test. People tend to overlook this step because sometimes it will not have the "expected" fun necessary but users should understand that the success of exploiting a system is the time spent on gathering information of the target. The information gathering process, in this book, covers the identification of the target and the discovery of different applications or possible attack vectors.

Dmca