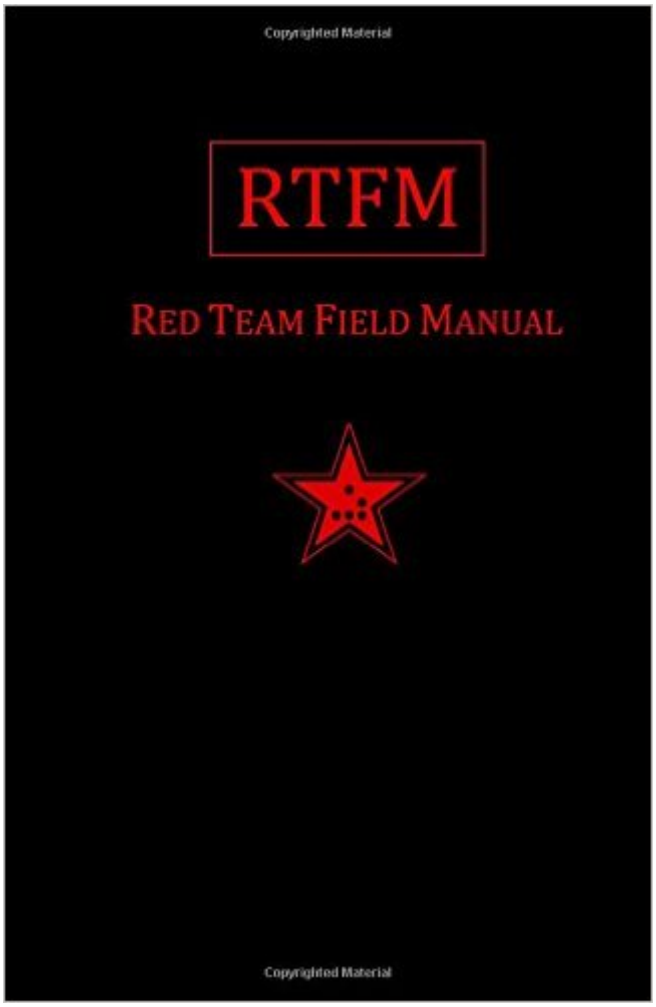
Rtfm: Red Team Field Manual



Synopsis

The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and dsquery command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

Book Information

Paperback: 96 pages
Publisher: CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014)
Language: English
ISBN-10: 1494295504
ISBN-13: 978-1494295509
Product Dimensions: 5.5 x 0.2 x 8.5 inches
Shipping Weight: 5 ounces (View shipping rates and policies)
Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (333 customer reviews)
Best Sellers Rank: #1,996 in Books (See Top 100 in Books) #5 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

These are all fun and stuff, but there needs to be a few actual reviews.This book is essentially a decade’s worth of notes from an experienced network security engineer or pen tester. It looks like someone published an evernote notebook. Formatting is inconsistent and at times confusing. There is a fair amount of duplication. Placeholders are inconsistent. There is no descriptive text or explanatory notes. It is a list of commands, and nothing more.If you are an experienced command line user, it is pretty awesome.That said, with around 2000 commands in the book, there in exactly one page of index. It is impossible to find anything. If it is windows, that’s great, narrows things down to about 30 pages that you have to flip through to find what you want. Even though I often know exactly what I am looking for, I still end up flipping through nearly every page in the book to find it. That is frustrating.It’s true that everything here can be found elsewhere online, but that’s a lot like saying that a thesaurus is just a list of words that you can find online. The proper formatting of

actually useful DOS net commands, for instance, is a great example of why the book is more useful than a Google search.I'd say this is pretty much a must-own book for anyone that has to work with computers. If you are in charge of security or testing, even better. I wish it was better indexed, but can't have everything. Certainly worth the money.

I'm not sure what the bad reviews are all about. They complain about the text not being readable, no table of contents or the commands not being categorized. Totally false. The book is of great quality, the text absolutely normal, it has a table of contents and an Index at the end of the book. Also, all the commands are categorized, such as Windows Utility Commands, Windows Network Commands, Windows Remote Commands, etc. etc.. Table of Contents: Nix, Windows, Networking, Tips and Tricks, Tool Syntax, Web, Databases, Programming, Wireless, References, Index.You will find Nmap commands, SQLMAP, Powershell, Google Hacking, VPN, Putty, MS-SQL, Postgres, Tunneling... so many more to cover it here.All I can think of is that someone got an early copy of this book, a very bad one...?? That's where the bad review came from? Or, someone with bad intentions.Trust me: this is the best field manual you will ever find. Excellent resource.

I have never written a review, but after a co worker brought this in, and i looked it over I instantly put it on my 'to buy list' (and will have in my hands very soon).Many of the items i constantly google for, or carry around in a beat up spiral bound notebook, can be found in this book. Somewhere between 30-50 percent located in a tiny book. Plus stuff i don't currently use, but may at any given moment.The stuff that is missing, and would be HIGHLY useful (hope the author is reading), would be an expansion on the database section to include common SQL injection (union based / error based) and a section on other web based attacks like XSS (including , , body.onload, etc.).As a follow up to those sections, methods of obfuscation (read filter evasion) are also highly needed for web based pen testing (a conversion chart or two for ascii -> url/hex/etc.)Extremely impressed otherwise, and will soon be toting this book instead of my personal notes, very soon!4/5 only because web based attacks were grossly overlooked.

This book is a reference manual with common commands and charts frequently used by penetration testers. Even though I am a novice security professional, my training during Offensive Security Certified Professional (OSCP) training helps me understand a fair portion of the sections and commands within those sections. The book's font is small so there is a lot of information it although it is physically small. Of the sections and commands which are new to me, there is invaluable

information which I will be exploring during my continuation of security training, including (OSCP). The first section relates to *nix operating systems. The majority of Linux network commands listed use flag settings and combinations which I haven't seen in most cases. A large portion of the book is dedicated to Windows commands. I have used some of the commands, but domain-related commands, essential for penetration testing, I have not yet used. Powershell is well-referenced, being the hip, new way to interact with the Windows environment.Some commands listed are absolute gold-examples are creating a Windows native port forwarding, something I did not know possible. There's a nice script to acquire the permissions of all services executables, important for privilege escalation in Windows. Important persistence commands for both Linux and Windows are listed. There are methods to perform screen shots and video of remote users. This could be useful to demonstrate total ownage to a management-type. Showing them working on their own computer gets the point across emphatically.From a novice penetration tester perspective, I feel these is likely benefit to this book and I will keep it handy at all times. It can be used to supplement a repository of reference material.

The best way to describe this book is a cheat sheet or refrence guide.This book won't teach you how to really do anything you need to know that going in, but as a guide to keep next to your laptop or in a bag when you travel can be handy.Nmap, Powershell, Linux, Windows, SQL, basic networking

Organization to a Positive Future Today’s Technician: Manual Transmissions and Transaxles Classroom Manual and Shop Manual Church Drill Team Member’s Manual Red: The True Story of Red Riding Hood NIV, Bible for Kids, Imitation Leather, Purple, Red Letter: Red Letter Edition Red Sox Fans Are from Mars, Yankees Fans Are from Uranus: Why Red Sox Fans Are Smarter, Funnier, and Better Looking (In Language Even Yankee Fans Can Understand) Ruby Red (The Ruby Red Trilogy) Ruby Red (Ruby Red Trilogy Book 1) Red Cross, Red Crescent: When Help Can’t Wait