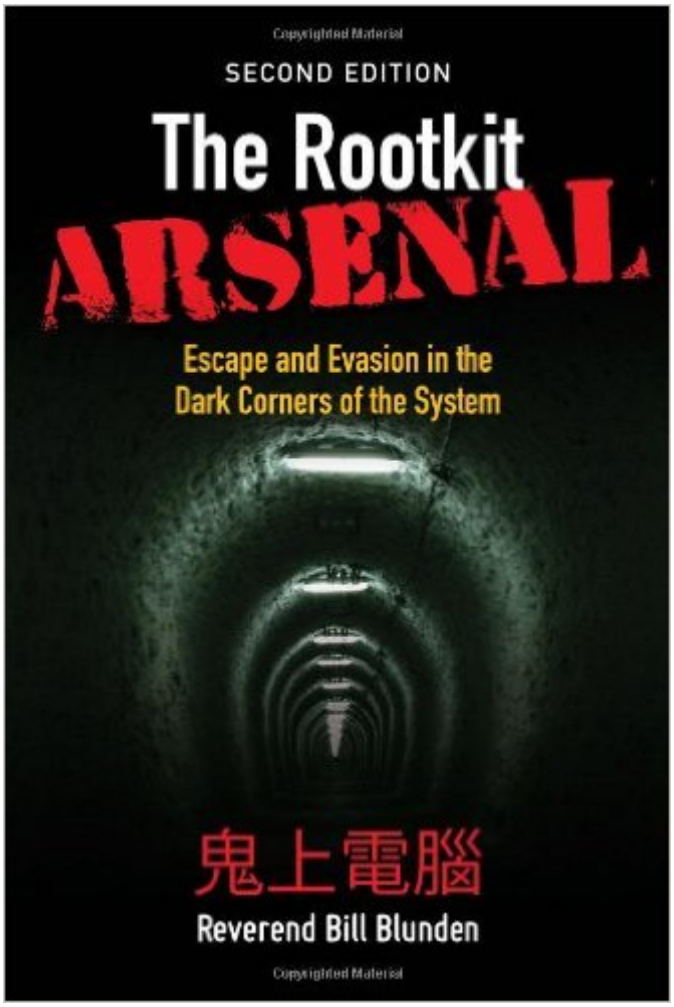
The Rootkit Arsenal: Escape And Evasion In The Dark Corners Of The System



Synopsis

While forensic analysis has proven to be a valuable investigative tool in the field of computer security, utilizing anti-forensic technology makes it possible to maintain a covert operational foothold for extended periods, even in a high-security environment. Adopting an approach that favors full disclosure, the updated Second Edition of The Rootkit Arsenal presents the most accessible, timely, and complete coverage of forensic countermeasures. This book covers more topics, in greater depth, than any other currently available. In doing so the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented. The range of topics presented includes how to: -Evade post-mortem analysis -Frustrate attempts to reverse engineer your command & control modules -Defeat live incident response -Undermine the process of memory analysis -Modify subsystem internals to feed misinformation to the outside -Entrench your code in fortified regions of execution -Design and implement covert channels -Unearth new avenues of attack

Book Information

Paperback: 784 pages

Publisher: Jones & Bartlett Learning; 2 edition (March 30, 2012)

Language: English

ISBN-10: 144962636X

ISBN-13: 978-1449626365

Product Dimensions: 1.8 x 6.2 x 9.2 inches

Shipping Weight: 2.4 pounds (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 starsÂ Â See all reviewsÂ (6 customer reviews)

Best Sellers Rank: #240,620 in Books (See Top 100 in Books) #63 inÂ Books > Computers & Technology > Security & Encryption > Viruses #182 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #198 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

Got my copy of the book 3 weeks ago, I have to say this is one of the best books I’ve read on the subject.I recommended buying it to anyone who wish to know how O/S really works & find out about all those little things that makes the ’magic" happens after boot/login.The book is NOT for beginners: A prior knowledge of assembly & usage of windows debuggers (such as WinDbg or KD) is recommended.I had some experience with both, though I had some "rust", and it took me some time

googling to be reminded of some stuff, and I wish author would put some additional chapter to subject early in the book.As an small example: In chapter 3, there is a deep dive into working example how one could implement a "key logger" into "real mode" via TSR. It would really help if author would give small "intro" to TSR saying "write' performed by placing 25H to AH, DS:DX point to new routine, AL = N & that will hook the new function to slot N. True one could understand that from code & after further check internet for int21 documentation, but again it would make reading much "smoother". I assume someone that uses assembly on daily usage probably seems very obvious...The book is filled with real "gems" as to HOW O/S works, what's get loaded first, who calls who, what registry key to watch out for if someone were to add to list of "Known" DLLs etc. And even though I'm not "security specialist" (I more an hobbyist), I really learned ALOT from this book.I'm a software engineer for over 8 years, and I must admit only now I understand certain compiler flags & concept like ASLR, /GS & DEP...The author takes a chapter to explain one thing at a time, and at the end of the chapter he provides some sort of "overall review", usually inside simple to understand chart/diagram that will help the user deal with the enormous amount of information provided.Author provides alot of KD snippets, that demonstrate & proves the stuff he teach, I only wish some small intro chapter were made to those who less know those commands. Again, just to be clear I'm not referring to a "KD for dummies", but it would sure help to add a small reference to the commands used, so that could provide user with quick reference, instead of having to google for it, to understand what it does.On the assembly side snippets, there are occasional some minor errors in the code snippets, like MOV/PUSH instead of LEA, but I guess that could be to avoid script kiddies to take code & compile right of the book.To sum things up, I really enjoyed reading this book (still reading it...)That's why I'm giving it 5 stars, it deserves it !

Great book for all things rootkit related. This covers the majority of rootkit related code and techniques up till about 2010ish. I have not read it cover to cover but I did not see anything about items like patch guard in the book which is highly relevant to rootkits.This is still one of my highest suggested books even for the few things it does seem to lack.

Solid information with great structure. Must have C back ground with solid CS understanding.

Brilliant book. I wish more than snippets of code were available. Even if you don't end up making rootkit, you'll learn a lot from this book

This is book is brilliant! I really think this is the bible on rootkit development! Have learnt so much from it.

The Book has several well informed documented and updated contents. The singular way that the Author, Bill Blunden, address the topic make the book so interesting to keep reading it. The Technicals words used in combination with the simplicity of his well experienced analogies when referring to a subject has done a straight forward picture of understanding for each Subject on the Book.

The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System Tax Havens: International Tax Avoidance and Evasion Offshore Tax Evasion: IRS Offshore Voluntary Disclosure Program Offshore Tax Evasion: IRS Tax Compliance FATCA/FBAR The Arsenal of Democracy: FDR, Detroit, and an Epic Quest to Arm an America at War Grill Master (Williams-Sonoma): The Ultimate Arsenal of Back-to-Basics Recipes for the Grill When Nature Heals: The Greening of Rocky Mountain Arsenal Arsenal of Democracy: The American Automobile Industry in World War II (Great Lakes Books Series) Images from the Arsenal of Democracy (Painted Turtle) Restoration of Lost or Obliterated Corners and Subdivision of Sections: With Index and references to the 1973 and 2009 Manuals of Survey Instructions Atlas of Adventures: A collection of natural wonders, exciting experiences and fun festivities from the four corners of the globe United Tastes of Texas: Authentic Recipes from All Corners of the Lone Star State Shapes of Needlepoint: Series III - Corners, Hexagons, Ovals, Parallelograms Atlas of Improbable Places: A Journey to the World's Most Unusual Corners Rounding the Human Corners At the Heart of the Liturgy: Conversations with Nathan D. Mitchell's "Amen Corners," 1991-2012 Unix System V/386 Release 3.2: System Administrator's Guide (AT&T UNIX system V/386 library) The Two Marxisms: Contradictions and Anomalies in the Development of Theory (The Dark Side of the Dialectic; V. 3) (His the Dark Side of the Dialectic; V. 3) Dark Web: Exploring and Data Mining the Dark Side of the Web (Integrated Series in Information Systems) The 4 Percent Universe: Dark Matter, Dark Energy, and the Race to Discover the Rest of Reality