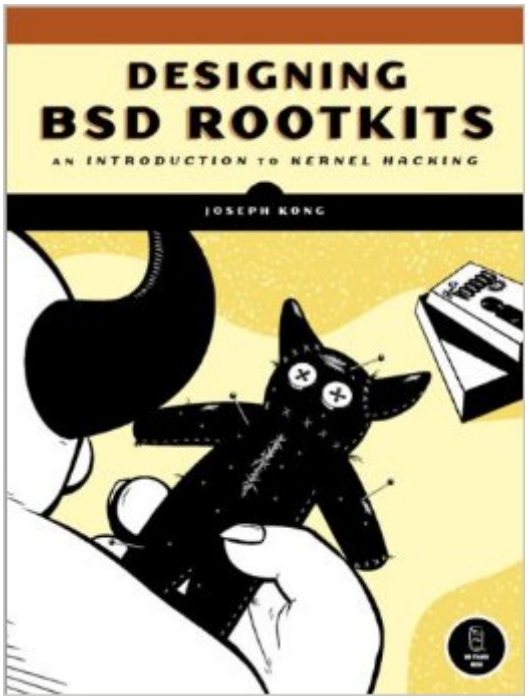
Designing BSD Rootkits: An Introduction To Kernel Hacking



Synopsis

Though rootkits have a fairly negative image, they can be used for both good and evil. Designing BSD Rootkits arms you with the knowledge you need to write offensive rootkits, to defend against malicious ones, and to explore the FreeBSD kernel and operating system in the process.Organized as a tutorial, Designing BSD Rootkits will teach you the fundamentals of programming and developing rootkits under the FreeBSD operating system. Author Joseph Kong’s goal is to make you smarter, not to teach you how to write exploits or launch attacks. You’ll learn how to maintain root access long after gaining access to a computer and how to hack FreeBSD.Kongs liberal use of examples assumes no prior kernel-hacking experience but doesn’t water down the information. All code is thoroughly described and analyzed, and each chapter contains at least one real-world application.Included:The fundamentals of FreeBSD kernel module programmingUsing call hooking to subvert the FreeBSD kernelDirectly manipulating the objects the kernel depends upon for its internal record-keepingPatching kernel code resident in main memory; in other words, altering the kernel’s logic while it’s still runningHow to defend against the attacks describedHack the FreeBSD kernel for yourself!

Book Information

File Size: 383 KB

Print Length: 144 pages

Simultaneous Device Usage: Unlimited

Publisher: No Starch Press; 1 edition (April 9, 2007)

Publication Date: August 20, 2009

Sold by:Â Digital Services LLC

Language: English

ASIN: B002MZAR6I

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Enabled

Best Sellers Rank: #928,814 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #28 inÂ Books > Computers & Technology > Operating Systems > BSD #254 inÂ Kindle Store > Kindle eBooks > Computers & Technology > Operating Systems > Unix #521 inÂ Books > Computers &

Customer Reviews

I loved Designing BSD Rootkits (DBR) by Joseph Kong, and I’m not even a kernel hacker. Rather, I’m an incident responder and FreeBSD administrator. This book is directly on target and does not waste the reader’s time. If you understand C and want to learn how to manipulate the FreeBSD kernel, Designing BSD Rootkits is for you. Peer into the depths of a powerful operating system and bend it to your will!DBR covers much of the same sorts of material found in the earlier Rootkits: Subverting the Windows Kernel by Greg Hoglund and James Butler, except Kong’s book is all about FreeBSD. I actually read the Windows text first, but found Kong’s more direct language and examples easier than the Hoglund/Butler text. After reading DBR I have a stronger understanding of each of the main chapters’ techniques, i.e., kernel modules, hooking, direct kernel object manipulation, kernel object hooking, run-time kernel memory patching, and detection mechanisms. I particularly liked the author showing his sample rootkit’s effectiveness against Tripwire, simply to demonstrate his methods.DBR follows another tenet of great books: it credits previous work. Several times in the text Kong says where he learned a technique or what code he’s modifying to do his bidding. This should serve as an example to other technical authors. Kong also does not treat his subject matter as a dark art practiced by people in long black coats at Def Con. He is professional and mentions where certain techniques like run-time kernel memory patching are used by commercial operating systems for "hot patching," as happens with Windows.

--- DISCLAIMER: This is a requested review by No Starch Press, however any opinions expressed within the review are my personal ones. ---This enjoyable readable book gradually and very systematically evolves around hacking the kernel of a BSD system.Chapter 1: Loadable Kernel Modules 22p.Chapter 2: Hooking 13p.Chapter 3: Direct Kernel Object Manipulation 20p.Chapter 4: Kernel Object Hooking 4p.Chapter 5: Run-Time Kernel Memory Patching 27p.Chapter 6: Putting It All Together 26p.Chapter 7: Detection 8p.Its written in a style that allows also non-developers to grasp the main procedures and steps involved for modifying a systems kernel (assuming the attacker got access to a privileged system account).Chapters 1 to 5 explain the several methods for modifying the kernel.While the book is divided into 7 chapters, its most value really is the Chapters 6 which has many of those WoW effects included.All or most technics described of chapters 1-5 will be used in chapter 6 for show casing how to circumvent an HIDS. Here is where all learned technics finally come all together.So the reader dabbles with the author from an initial "simple" idea of

bypassing an HIDS from one issue to the next. First the system call is hooked, so technically its kind of working, but then we realize that in order to make it perfect we need to hide the just created file (which contains the execution redirection routine). So the next obvious step is to hide the file so we dont leave a footprint on the system, just to realize that we need to hide the KLD (Dynamic Kernel Linker).

Preemptive, Multitasking Kernel for Microprocessors, Microcontrollers & DSPs (Board NOT Included) Kernel of the Kernel (Suny Series in Islam) Malware, Rootkits & Botnets A Beginner's Guide Hacking: Tapping into the Matrix Tips, Secrets, steps, hints, and hidden traps to hacking: Hacker, Computer, Programming, Security & Encryption