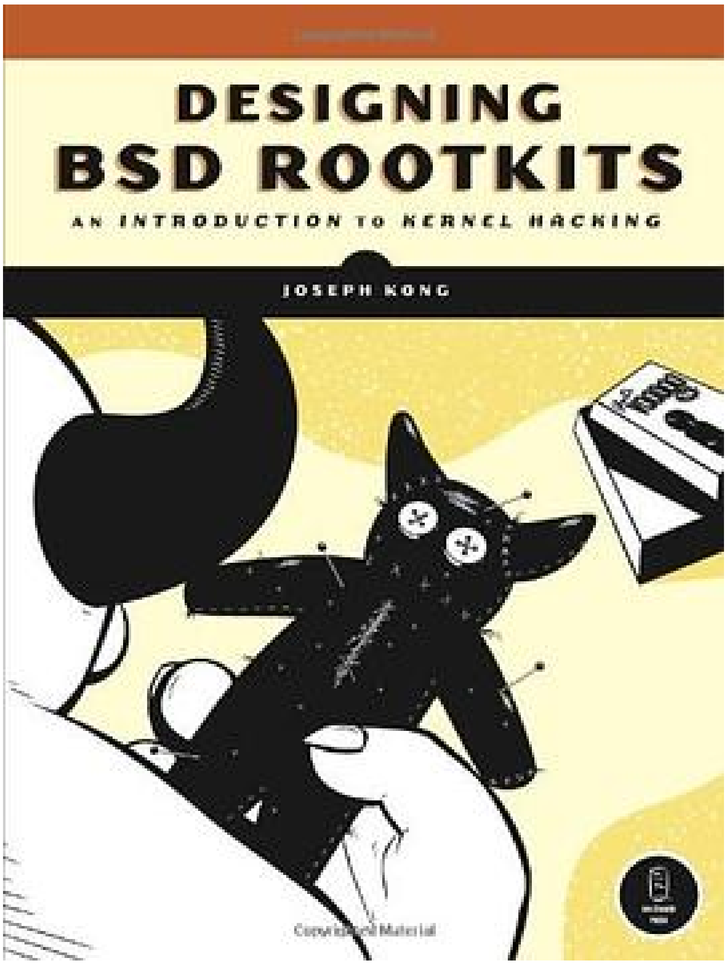
Designing BSD Rootkits



Designing BSD Rootkits_下载链接1_

著者:Joseph Kong

出版者:No Starch Press

出版时间:2007-04-10

装帧:Paperback

isbn:9781593271428

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 programming Using call hooking to subvert the FreeBSD kernel Directly manipulating the objects the kernel depends upon for its internal record-keeping Patching kernel code resident in main memory; in other words, altering the kernel's logic while it's still running How to defend against the attacks described Hack the FreeBSD kernel for yourself!

作者介绍:

Tinkering with computers has always been a primary passion of author Joseph Kong. He is a self-taught programmer who dabbles in information security, operating system theory, reverse engineering, and vulnerability assessment. He has written for Phrack Magazine and was a system administrator for the City of Toronto.

目录:
・・・・・・(收起)

Designing BSD Rootkits_下载链接1_

标签

BSD

计算机

信息安全

UNIX

安全

内核

rootkits

Linux

评论

大致犯了一下目录，都是一些好邪恶的技术，当然最后一章有防范技术的介绍。。。

KLD的基础是kern_linker.c 这个文件，实现了动态的把|ELF文件加载到kernel space。而要用好kld，则需要熟悉各个sub system的kernel API

Designing BSD Rootkits_下载链接1_

书评

Designing BSD Rootkits_下载链接1_