NO STARCH PRESS

FOR IMMEDIATE RELEASE
Media contact: camille@nostarch.com
415.863.9900 x303

No Starch Press Releases DESIGNING BSD ROOTKITS: An Introduction to Kernel Hacking

April 11, 2007, San Francisco—For most computer-savvy readers, the word “rootkits” is synonymous with the word “evil.” (We all remember the Sony rootkit, right?) Traditionally, rootkits are used to covertly give a remote attacker complete control of a computer, including administrative privileges, while evading detection by hiding running processes and files. Rootkits are a growing threat to even the most secure operating systems.

However, learning how rootkits work can teach us a lot about an operating system. In **Designing BSD Rootkits: An Introduction to Kernel Hacking** (No Starch Press, April 2007, http://www.nostarch.com/rootkits.htm), author Joseph Kong shows how to write offensive rootkits, defend against malicious ones, and explore the FreeBSD kernel in the process. As the first book to approach rootkits from a FreeBSD-centric perspective, Kong's goal is to make readers smarter, not teach them how to write exploits or launch attacks.

While **Designing BSD Rootkits** focuses on programming and developing rootkits under FreeBSD, most concepts apply to other operating systems, such as GNU/Linux or Windows. Kong’s liberal examples assume no prior kernel-hacking experience. All code is thoroughly described and analyzed, and each chapter contains at least one real-world application.

Readers of **Designing BSD Rootkits** learn

- The fundamentals of FreeBSD kernel module programming
- How to use call hooking to subvert the kernel
- How to manipulate the objects the kernel depends upon for its internal record-keeping
- How to patch kernel code stored in main memory, thus altering the kernel’s logic while it’s still running
- How to defend against the attacks described

“The word “hacking” has a bad name, but there is more to hacking than breaking into systems,” said No Starch Press founder Bill Pollock. “This is not a book for script kiddies who just want to launch easy exploits. This is heady stuff. This is a book for real hackers who want to understand how the kernel works so that they can better secure their OS, whether it's FreeBSD or other.”

Anyone with an interest in systems administration, open source operating systems, or computer security has something to learn from **Designing BSD Rootkits**.

Additional Resources:
Table of contents: http://www.nostarch.com/rootkits_toc.htm
Sample chapter: http://www.nostarch.com/download/rootkits_ch2.pdf

ABOUT THE AUTHOR: Joseph Kong (www.thestackframe.org/) 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.

Designing BSD Rootkits: An Introduction to Kernel Hacking
Joseph Kong, April 2007, 144pp., ISBN 978-1-59327-142-8 US$29.95
Available at fine bookstores everywhere, from www.oreilly.com/nostarch, or directly from No Starch Press (www.nostarch.com, 800.420.7240, +1 415.863.9900).

ABOUT NO STARCH PRESS: Founded in 1994, No Starch Press is one of the few remaining independent computer book publishers. We publish the finest in geek entertainment—unique books on technology, with a focus on Open Source, security, hacking, programming, and alternative operating systems. Our titles have personality, our authors are passionate, and our books tackle topics that people care about. No Starch Press books have been included in the prestigious Communication Arts Design Annual and STEP inside 100 competition, and have won the Ippy Award from Independent Publisher magazine. See www.nostarch.com for more information and our complete online catalog. (And most No Starch Press books use RepKover, a lay-flat binding that won’t snap shut.)

# # #