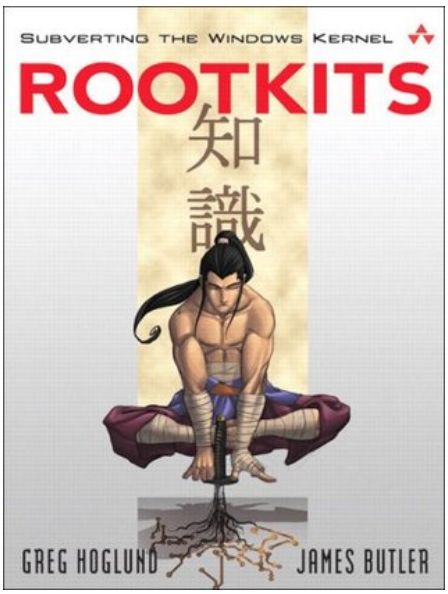

Rootkits: Subverting the Windows Kernel

Greg Hoglund

Download now

Read Online

Rootkits: Subverting the Windows Kernel

Greg Hoglund

Rootkits: Subverting the Windows Kernel Greg Hoglund
"It's imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits."
--*Mark Russinovich, editor,* Windows IT Pro / Windows & .NET Magazine "This material is not only up-to-date, it defines up-to-date. It is truly cutting-edge. As the only book on the subject, ***Rootkits*** will be of interest to any Windows security researcher or security programmer. It's detailed, well researched and the technical information is excellent. The level of technical detail, research, and time invested in developing relevant examples is impressive. In one word: Outstanding."
--*Tony Bautts, Security Consultant; CEO, Xtivix, Inc.* "This book is an essential read for anyone responsible for Windows security. Security professionals, Windows system administrators, and programmers in general will want to understand the techniques used by rootkit authors. At a time when many IT and security professionals are still worrying about the latest e-mail virus or how to get all of this month's security patches installed, Mr. Hoglund and Mr. Butler open your eyes to some of the most stealthy and significant threats to the Windows operating system. Only by understanding these offensive techniques can you properly defend the networks and systems for which you are responsible."
--*Jennifer Kolde, Security Consultant, Author, and Instructor* "What's worse than being owned? Not knowing it. Find out what it means to be owned by reading Hoglund and Butler's first-of-a-kind book on rootkits. At the apex the malicious hacker toolset--which includes decompilers, disassemblers, fault-injection engines, kernel debuggers, payload collections, coverage tools, and flow analysis tools--is the rootkit. Beginning where Exploiting Software left off, this book shows how attackers hide in plain sight.

"Rootkits are extremely powerful and are the next wave of attack technology. Like other types of malicious code, rootkits thrive on stealthiness. They hide away from standard system observers, employing hooks, trampolines, and patches to get their work done. Sophisticated rootkits run in such a way that other programs that usually monitor machine behavior can't easily detect them. A rootkit thus provides insider access only to people who know that it is running and available to accept commands. Kernel rootkits can hide files and running processes to provide a backdoor into the target machine.

"Understanding the ultimate attacker's tool provides an important motivator for those of us trying to defend systems. No authors are better suited to give you a detailed hands-on understanding of rootkits than Hoglund and Butler. Better to own this book than to be owned."
--*Gary McGraw, Ph.D., CTO, Cigital, coauthor of* Exploiting Software *(2004) and* Building Secure Software *(2002), both from Addison-Wesley* "Greg and Jamie are unquestionably the go-to experts when it comes to subverting the Windows API and creating rootkits. These two masters come together to pierce the veil of mystery surrounding rootkits, bringing this information out of the shadows. Anyone even remotely interested in security for Windows systems, including forensic analysis, should include this book very high on their must-read list."
--*Harlan Carvey, author of* Windows Forensics and Incident Recovery *(Addison-Wesley, 2005)* Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the world's leading experts have written the first comprehensive guide to rootkits: what they are, how they work, how to build them, and how to detect them. Rootkit.com's Greg Hoglund and James Butler created and teach Black Hat's legendary course in rootkits. In this book, they reveal never-before-told offensive aspects of rootkit technology--learn how attackers can get in and stay in for years, without detection. Hoglund and Butler show exactly how to subvert the Windows XP and Windows 2000 kernels,

teaching concepts that are easily applied to virtually any modern operating system, from Windows Server 2003 to Linux and UNIX. They teach rootkit programming techniques that can be used for a wide range of software, from white hat security tools to operating system drivers and debuggers. After reading this book, readers will be able to
Understand the role of rootkits in remote command/control and software eavesdropping
Build kernel rootkits that can make processes, files, and directories invisible
Master key rootkit programming techniques, including hooking, runtime patching, and directly manipulating kernel objects
Work with layered drivers to implement keyboard sniffers and file filters
Detect rootkits and build host-based intrusion prevention software that resists rootkit attacks

Rootkits: Subverting the Windows Kernel Details

Date	:	Published July 1st 2005 by Addison-Wesley Professional
ISBN	:	9780321294319
Author	:	Greg Hoglund
Format	:	Paperback 352 pages
Genre	:	Computer Science, Technical, Science, Technology, Computers, Hackers, Nonfiction, Software

Download Rootkits: Subverting the Windows Kernel ...pdf

Read Online Rootkits: Subverting the Windows Kernel ...pdf

Download and Read Free Online Rootkits: Subverting the Windows Kernel Greg Hoglund

From Reader Review Rootkits: Subverting the Windows Kernel for online ebook

Matty says

The 1st chapter has a great overview of key elements in software attacks. Nice start for a security nüb like myself.

James says

They don't all work. But it gives a great overview of what a backdoor does and how it does it. This is ancient history by now, but the principles are good. Scares the heck out the reader, too. Best horror book I've read so far this year.

Ben Holland says

The content is a bit outdated now and the supporting materials online are gone (even from the internet archives).

Charlie says

explanations and sample code of how to write and detect rootkits

---

Tyler says

A fantastic book detailing the ins and outs of windows rootkits. If you are interested in the details surrounding topics such as kernel hooks, DKOM, and process hiding, this is the best book on the market today.

Acc13 says

Probably due for an update; but still great info.

Very informative.

Probably those who have already done some Windows driver coding can skip the chapters on layered drivers, or sending raw TCP packets from kernel level; but the table hooks, inline patches, evasion, etc. was very interesting.

Recommended for those new to rootkits, but with some coding experience.
