Rootkits: Subverting the Windows Kernel

Greg Hoglund, Jamie Butler

Rootkits: Subverting the Windows Kernel

Greg Hoglund, Jamie Butler

Rootkits: Subverting the Windows Kernel Greg Hoglund, Jamie Butler
"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

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

---

From reader reviews:

Teresa Hennessey:

Inside other case, little men and women like to read book Rootkits: Subverting the Windows Kernel. You can choose the best book if you love reading a book. As long as we know about how is important any book Rootkits: Subverting the Windows Kernel. You can add information and of course you can around the world by way of a book. Absolutely right, because from book you can learn everything! From your country until finally foreign or abroad you will end up known. About simple issue until wonderful thing it is possible to know that. In this era, you can open a book or searching by internet device. It is called e-book. You can utilize it when you feel weary to go to the library. Let's read.

David Lussier:

In this 21st hundred years, people become competitive in most way. By being competitive right now, people have do something to make these survives, being in the middle of the particular crowded place and notice by simply surrounding. One thing that at times many people have underestimated that for a while is reading. Yep, by reading a book your ability to survive enhance then having chance to remain than other is high. For you personally who want to start reading a book, we give you this particular Rootkits: Subverting the Windows Kernel book as beginner and daily reading book. Why, because this book is more than just a book.

Kimberly Gomez:

As people who live in typically the modest era should be upgrade about what going on or facts even knowledge to make these people keep up with the era and that is always change and move ahead. Some of you maybe will certainly update themselves by reading through books. It is a good choice to suit your needs but the problems coming to a person is you don't know what one you should start with. This Rootkits: Subverting the Windows Kernel is our recommendation to make you keep up with the world. Why, as this book serves what you want and wish in this era.

Kathleen Jones:

Do you really one of the book lovers? If so, do you ever feeling doubt when you are in the book store? Try to pick one book that you just dont know the inside because don't evaluate book by its cover may doesn't work this is difficult job because you are afraid that the inside maybe not since fantastic as in the outside appearance likes. Maybe you answer might be Rootkits: Subverting the Windows Kernel why because the fantastic cover that make you consider concerning the content will not disappoint you. The inside or content will be fantastic as the outside as well as cover. Your reading 6th sense will directly assist you to pick up this book.

Read Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler for online ebook

Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler books to read online.

Online Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler ebook PDF download

Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler Doc

Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler Mobipocket

Rootkits: Subverting the Windows Kernel by Greg Hoglund, Jamie Butler EPub