Google Drive

Rootkits: Subverting the Windows Kernel

Greg Hoglund, Jamie Butler

Download now

Click here if your download doesn"t start automatically

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 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, Jamie Butler

---

From reader reviews:

Roger Dupre:

In this 21st one hundred year, people become competitive in most way. By being competitive currently, people have do something to make these survives, being in the middle of the actual crowded place and notice by surrounding. One thing that sometimes many people have underestimated that for a while is reading. That's why, by reading a book your ability to survive improve then having chance to stay than other is high. For you personally who want to start reading any book, we give you that Rootkits: Subverting the Windows Kernel book as beginning and daily reading e-book. Why, because this book is more than just a book.

Theresa Gayle:

Now a day those who Living in the era just where everything reachable by match the internet and the resources inside can be true or not demand people to be aware of each info they get. How people have to be smart in receiving any information nowadays? Of course the reply is reading a book. Looking at a book can help men and women out of this uncertainty Information specifically this Rootkits: Subverting the Windows Kernel book because this book offers you rich info and knowledge. Of course the details in this book hundred per-cent guarantees there is no doubt in it you may already know.

Sharon Garcia:

Do you have something that you like such as book? The book lovers usually prefer to decide on book like comic, small story and the biggest you are novel. Now, why not hoping Rootkits: Subverting the Windows Kernel that give your fun preference will be satisfied by means of reading this book. Reading routine all over the world can be said as the way for people to know world better then how they react towards the world. It can't be claimed constantly that reading routine only for the geeky man but for all of you who wants to be success person. So , for every you who want to start reading through as your good habit, you may pick Rootkits: Subverting the Windows Kernel become your own starter.

Ann Fortune:

A lot of reserve has printed but it takes a different approach. You can get it by online on social media. You can choose the best book for you, science, amusing, novel, or whatever by means of searching from it. It is called of book Rootkits: Subverting the Windows Kernel. You can add your knowledge by it. Without causing the printed book, it might add your knowledge and make a person happier to read. It is most essential that, you must aware about reserve. It can bring you from one destination for a other place.

Download and Read Online Rootkits: Subverting the Windows Kernel Greg Hoglund, Jamie Butler #4AP5SO9BIC8

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