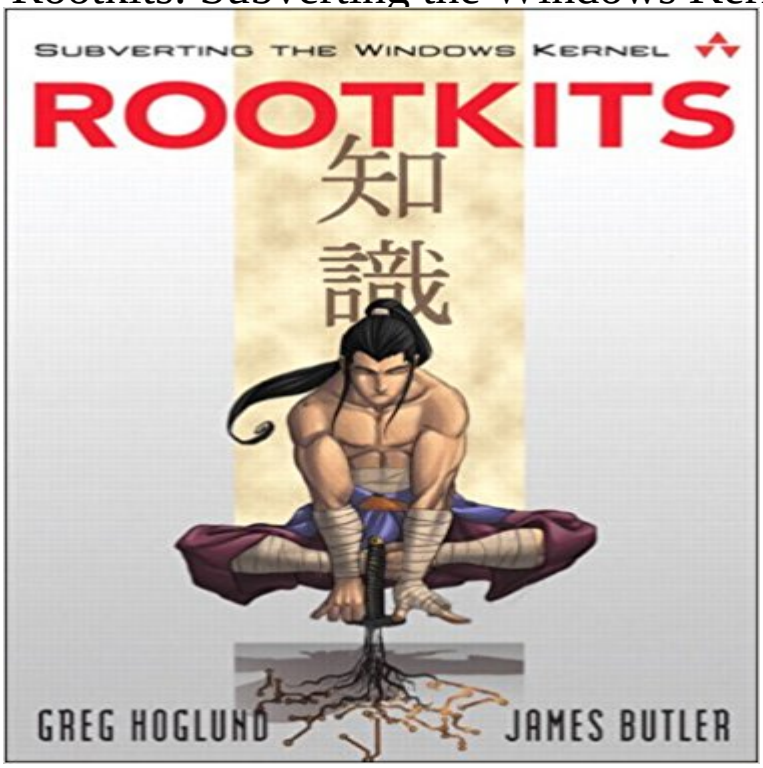
Rootkits: Subverting the Windows Kernel



Its 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. Its 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 months 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 Whats worse than being owned? Not knowing it. Find out what it means to be owned by reading Hoglund and Butlers 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 cant 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 attackers 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 worlds 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.coms Greg Hoglund and James Butler created and teach Black Hats 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 [Book] - Safari Books Online Written by Greg Hoglund. A brilliantly written book on everything one would want to know about Rootkits in the Microsoft Windows world. **Rootkits: Subverting the Windows Kernel (Addison - Thriftbooks** Buy Rootkits: Subverting the Windows Kernel on ? FREE SHIPPING on qualified orders. **Rootkits: Subverting the Windows Kernel - Slashdot** Greg Hoglund - Rootkits: Subverting the Windows Kernel (Addison-Wesley Software Security) jetzt kaufen. ISBN: 9780321294319, Fremdsprachige Bucher **Rootkits: Subverting the Windows Kernel - Greg - Google Books** Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the **Rootkits: Subverting the Windows Kernel eBook: Greg -** Synopsis. Its imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits.--Mark Russinovich **Rootkits: Subverting the Windows Kernel eBook -** Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the worlds leading experts **Rootkits: Subverting the Windows Kernel by Greg Hoglund Jamie** Rootkits: Subverting the Windows Kernel Addison-Wesley Software Security: : Greg Hoglund, Jamie Butler: Libros en idiomas extranjeros. **Rootkits: Subverting the Windows Kernel Addison -** - Buy Rootkits: Subverting the Windows Kernel (Addison-Wesley Software Security) book online at best prices in India on Amazon.in. Read Rootkits: **Rootkits: Subverting the Windows Kernel eBook: Greg -** Buy Rootkits: Subverting the Windows Kernel (Addison-Wesley Software Security) by Greg Hoglund, Jamie Butler (ISBN: 9780321294319) from Amazons Book **Rootkits: Subverting the Windows Kernel by Greg Hoglund** Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the worlds leading experts Rootkits: Subverting the Windows Kernel. Title: Rootkits: Subverting the Windows Kernel. This book is an essential read for anyone responsible for Windows **Rootkits: Subverting the Windows Kernel: Greg -** Find helpful customer reviews and review ratings for Rootkits: Subverting the Windows Kernel at . Read honest and unbiased product reviews from **Rootkits: Subverting the Windows Kernel** Scopri Rootkits: Subverting the Windows Kernel di Greg Hoglund, James Butler: spedizione gratuita per i clienti Prime e per ordini a partire da 29 spediti da **NEW Rootkits: Subverting the Windows Kernel by Greg Hoglund** 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 **Rootkits: Subverting the Windows Kernel: Greg -** Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the worlds leading experts **Rootkits: Subverting**

the Windows Kernel eBook: Greg - ** 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 **- Rootkits: Subverting the Windows Kernel - Greg Rootkits has 129 ratings and 6 reviews. Tyler said: A fantastic book detailing the ins and outs of windows rootkits. If you are interested in the details **Rootkits: Subverting the Windows Kernel eBook - ** Buy a cheap copy of Rootkits: Subverting the Windows Kernel (Addison-Wesley Software Security Series) book by Greg Hoglund. Its imperative that everybody **Rootkits: Subverting the Windows Kernel - Greg - Google Books** Its imperative that everybody working in the field of cyber-security read this book to understand the growing threat of rootkits. --Mark Russinovich, editor **: Rootkits: Subverting the Windows Kernel eBook: Greg** If youre one of them, Grog Hoglund and James Butlers new book, Rootkits: Subverting the Windows Kernel is for you. Its focused like a laser **Rootkits: Subverting the Windows Kernel - ACM Digital Library** This question appears to be off-topic. The users who voted to close gave this specific reason **Rootkits: Subverting the Windows Kernel eBook: Greg - Rootkits: Subverting the Windows Kernel InformIT** Note 4.5/5. Retrouvez Rootkits: Subverting the Windows Kernel et des millions de livres en stock sur . Achetez neuf ou doccasion. **Rootkits: Subverting the Windows Kernel Addison - ** Rootkits are the ultimate backdoor, giving hackers ongoing and virtually undetectable access to the systems they exploit. Now, two of the worlds leading experts **Customer Reviews: Rootkits: Subverting the Windows Kernel** Rootkits: Subverting the Windows Kernel. 1 review. by James Butler, Greg Hoglund. Publisher: Addison-Wesley Professional. Release Date: July 2005.