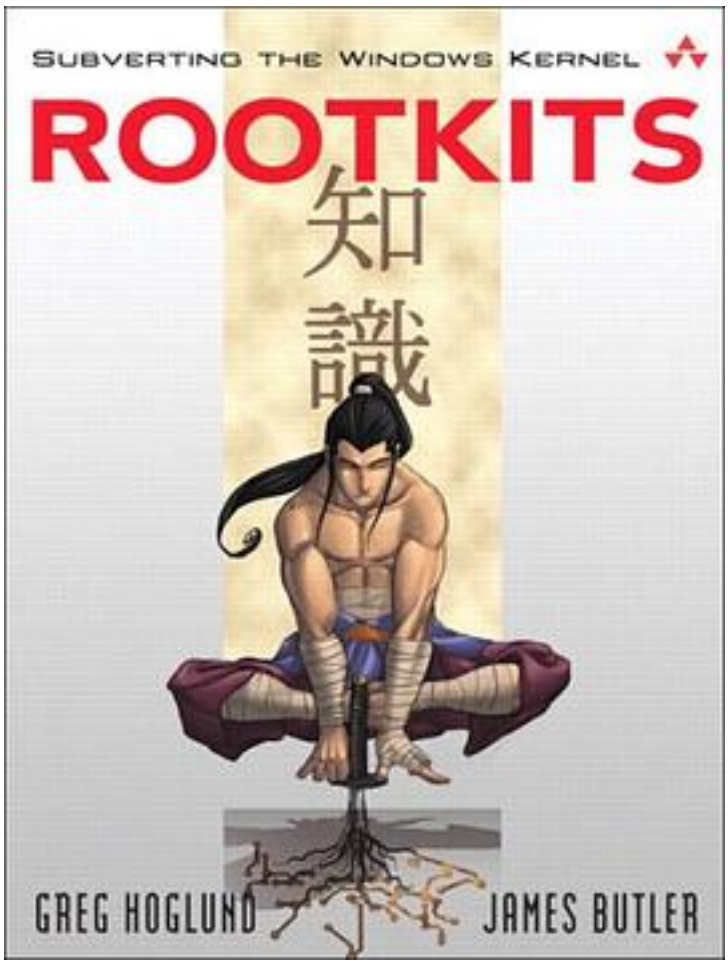
Rootkits



Rootkits_下载链接1_

著者:Greg Hoglund

出版者:Addison-Wesley Professional

出版时间:2005-8-1

装帧:Paperback

isbn:9780321294319

"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. Using extensive downloadable examples, 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 Visit rootkit.com for code and programs from this book. The site also contains enhancements to the book's text, such as up-to-the-minute information on rootkits available nowhere else.

作者介绍:

目录:

Rootkits_下载链接1_

标签

rootkit

kernel

计算机

安全

网络安全

Security

混口饭吃

计算机科学

评论

这本书现在来看有点老了，这几年SP，CCS的新方向太多了

内核级的，很多没看懂

Rootkits_下载链接1_

书评

书是好书,选题很好,但是,翻译就真的有问题,只能说差强人意,以这个篇幅来介绍rookits,而且基本上都说清楚了,有人可能觉得rookits这么高深的课题讲得还远远不够,须知道,这种课题只能点到为止,对于某些专业人士来说,缺的只是那么一点儿提示,不是技术细节,这个领域重要的是想像力,...

在卓越上买的，订单后看了一下英文版的，发现没必要买纸质书了，但是货已经发出来了…… 英文版的用的都是很简单的单词，很容易看懂，觉得买中文版有点亏了……
清华大学出版社，能不能把纸张弄好一点啊！

书不厚，但是内容的分量很足，并且不是普通的读者就能立刻上手的。它不像Windows核心编程一书那样详实，但在关键之处毫不含糊。这从它给出的示例就能看出来。这本书的作者已经假设读者有了很强的程序设计背景，在内核驱动编程，Windows内存管理，PE文件格式等这些系统程序...

个人觉得写的很不错，有人说翻译的不是很好，可读到现在觉得翻译的还是可以的，只是有些地方知识跨度可能会影响理解，不过多读两遍觉得翻译的还是不错的。
---个人见解

不知道是谁设计的封面，书的英文标题都弄错了，正确的标题应该是：rootkits:subverting the windows kernel,结果这本书封面上方的标题成了：rootkits:subvering the windows kernel，少了一个t，也太不负责任了吧。

不知大家看了这么久有没有发现书中的错误，个人感觉第四章的隐藏进程函数有问题，书上说可以过滤掉以_root_开头的所有进程，不过你仔细看82页下方的函数就会发现它函数写的有问题，比如说我系统中有一个_root_进程，ok那么没问题，完全可以过滤，但是如果我系统有多个_root_进...

Rootkits_下载链接1_