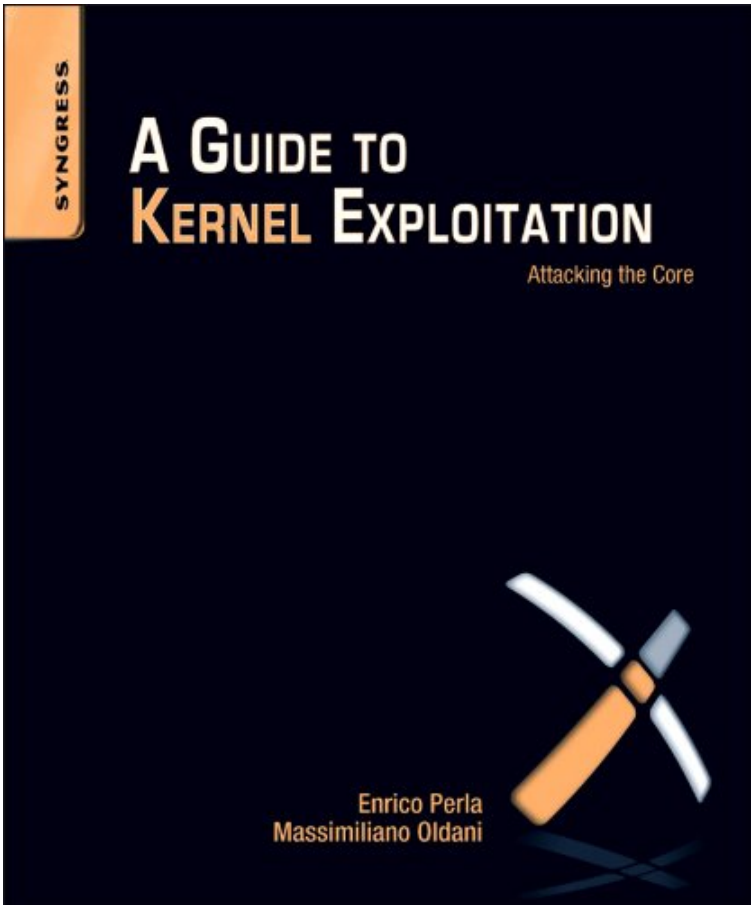
A Guide to Kernel Exploitation: Attacking the Core

Enrico Perla, Massimiliano Oldani
*audiobook | *ebooks | Download PDF | ePub | DOC*



#707181 in eBooks 2010-10-28 2010-10-28File Name: B004FGMSFK | File size: 24.Mb

Enrico Perla, Massimiliano Oldani : A Guide to Kernel Exploitation: Attacking the Core before purchasing it in order to gage whether or not it would be worth my time, and all praised A Guide to Kernel Exploitation: Attacking the Core:

8 of 9 people found the following review helpful. An excellent book on kernel exploitationBy BlakeI bought this book in hopes of finding an informative and thought provoking look at kernel exploitation - I was not disappointed. Aside from a few minor typos, I found this book to be one of the most well written books on exploitation that I have read. I have recommended it to some fellow students and a professor (I am a graduate student in computer science). I highly recommend this book for anybody that is interested in kernel exploitation. In my opinion, this book is currently the best source of information on exploiting the kernel since Phrack #64 file 6.1 of 2 people found the following review helpful. This book is the best book I've ever readBy DuderinoThis book is the best book I've ever read. No, but seriously, its like the keys to the kingdom. The authors do a great job of giving you a foundation in the starting chapters (however, it is very helpful if you have a coding background and have some knowledge of how and kernel/processor works, generally). I'm about half way through the book and I have learned so much about exploitation - this book is priceless.2 of 4 people found the following review helpful. Easy readingBy T. EmmertThis

was the first kernel related book I've read and it was very approachable an easy to understand.Each section breaks the necessary information down into understandable pieces. The background info provided is very useful for someone with no kernel background. However the amount of general kernel information was 50% of the book. For people who have some kernel background this book would most likely bore them to death.

A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerabilitya bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold.Covers a range of operating system families mdash; UNIX derivatives, Mac OS X, WindowsDetails common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditionsDelivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks

"A very interesting book that not only exposes readers to kernel exploitation techniques, but also deeply motivates the study of operating systems internals, moving such study far beyond simple curiosity."--Golden G. Richard III, Ph.D., Professor of Computer Science, University of New Orleans and CTO, Digital Forensics Solutions, LLCFrom the Back CoverThe number of security countermeasures against user-land exploitation is on the rise. Because of this, kernel exploitation is becoming much more popular among exploit writers and attackers. Playing with the heart of the operating system can be a dangerous game: This book covers the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits and applies them to different operating systems (Linux, Solaris, Mac OS X, and Windows). Kernel exploits require both art and science to achieve. Every OS has its quirks and so every exploit must be molded to fully exploit its target. This book discusses the most popular OS familiesUNIX derivatives, Mac OS X, and Windowsand how to gain complete control over them. Concepts and tactics are presented categorically so that even when a specifically detailed exploit has been patched, the foundational information that you have read will help you to write a newer, better attack or a more concrete design and defensive structure.About the AuthorEnrico Perla currently works as a kernel programmer at Oracle. He received his B.Sc. in Computer Science from the University of Torino, and his M.Sc. in Computer Science from Trinity College Dublin. His interests range from low-level system programming to low-level system attacking, exploiting, and exploit countermeasures.Massimiliano Oldani currently works as a Security Consultant at Emaze Networks. His main research topics include operating system security and kernel vulnerabilities.