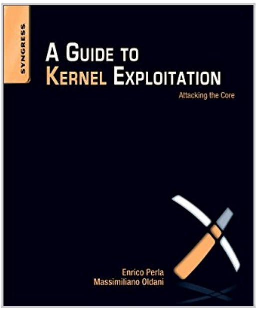

A Guide to Kernel Exploitation: Attacking the Core

By Enrico Perla, Massimiliano Oldani

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani

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 — UNIX derivatives, Mac OS X, Windows
- Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions
- Delivers 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 Guide to Kernel Exploitation: Attacking the Core

By Enrico Perla, Massimiliano Oldani

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani

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 — UNIX derivatives, Mac OS X, Windows
- Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions
- Delivers 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 Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani Bibliography

- Sales Rank: #684312 in eBooks
- Published on: 2010-10-28
- Released on: 2010-10-28
- Format: Kindle eBook

Editorial Review

Review

"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, LLC**

From the Back Cover

The 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 families?UNIX derivatives, Mac OS X, and Windows?and 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 Author
Enrico 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.

Users Review

From reader reviews:

Aimee Nguyen:

Here thing why this particular A Guide to Kernel Exploitation: Attacking the Core are different and reliable to be yours. First of all looking at a book is good but it depends in the content of it which is the content is as delicious as food or not. A Guide to Kernel Exploitation: Attacking the Core giving you information deeper and different ways, you can find any e-book out there but there is no reserve that similar with A Guide to Kernel Exploitation: Attacking the Core. It gives you thrill reading through journey, its open up your current eyes about the thing in which happened in the world which is probably can be happened around you. You can easily bring everywhere like in park, café, or even in your approach home by train. For anyone who is having difficulties in bringing the imprinted book maybe the form of A Guide to Kernel Exploitation:

Attacking the Core in e-book can be your alternative.

Krystal Wilson:

Do you certainly one of people who can't read gratifying if the sentence chained in the straightway, hold on guys this kind of aren't like that. This A Guide to Kernel Exploitation: Attacking the Core book is readable simply by you who hate the perfect word style. You will find the info here are arrange for enjoyable looking at experience without leaving even decrease the knowledge that want to provide to you. The writer regarding A Guide to Kernel Exploitation: Attacking the Core content conveys prospect easily to understand by many people. The printed and e-book are not different in the information but it just different in the form of it. So , do you nevertheless thinking A Guide to Kernel Exploitation: Attacking the Core is not loveable to be your top collection reading book?

Jacqueline Morrison:

Nowadays reading books become more than want or need but also work as a life style. This reading routine give you lot of advantages. The advantages you got of course the knowledge your information inside the book that improve your knowledge and information. The details you get based on what kind of book you read, if you want have more knowledge just go with education books but if you want really feel happy read one along with theme for entertaining like comic or novel. The actual A Guide to Kernel Exploitation: Attacking the Core is kind of reserve which is giving the reader capricious experience.

Vicky Gamez:

As a college student exactly feel bored in order to reading. If their teacher inquired them to go to the library or to make summary for some book, they are complained. Just tiny students that has reading's spirit or real their pastime. They just do what the educator want, like asked to the library. They go to presently there but nothing reading really. Any students feel that studying is not important, boring and also can't see colorful images on there. Yeah, it is to get complicated. Book is very important to suit your needs. As we know that on this period of time, many ways to get whatever you want. Likewise word says, ways to reach Chinese's country. Therefore this A Guide to Kernel Exploitation: Attacking the Core can make you truly feel more interested to read.

Download and Read Online A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani #FN4R3JB85V7

Read A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani for online ebook

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani 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 A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani books to read online.

Online A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani ebook PDF download

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani Doc

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani Mobipocket

A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani EPub

FN4R3JB85V7: A Guide to Kernel Exploitation: Attacking the Core By Enrico Perla, Massimiliano Oldani