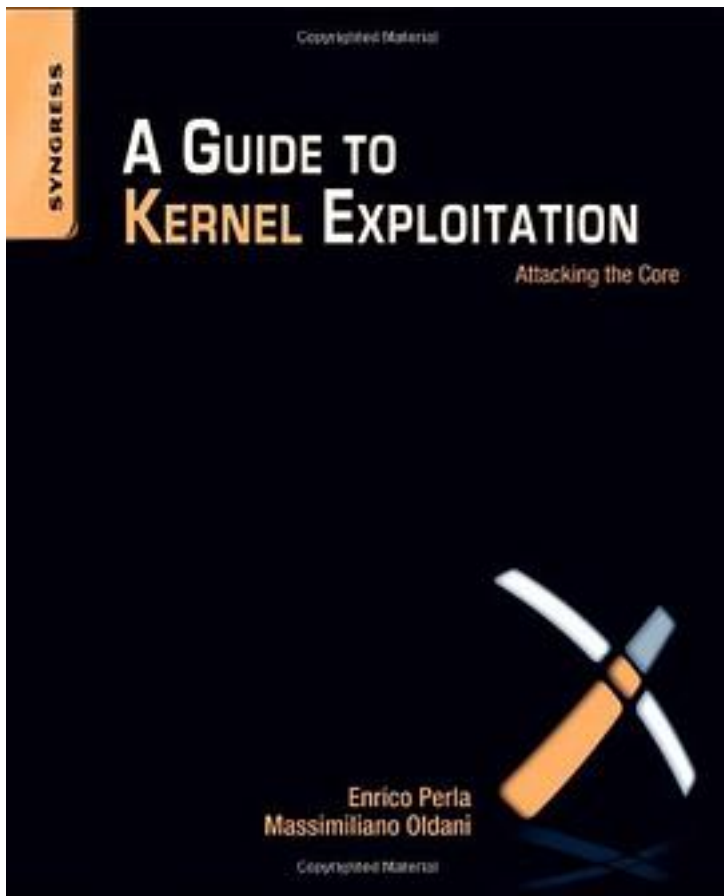# A Guide to Kernel Exploitation

[A Guide to Kernel Exploitation_下载链接1_](#)

著者:Enrico Perla B.Sc. Computer Science University of Torino M.Sc. Computer Science Trinity College Dublin

出版者:Syngress

出版时间:2010-9-15

装帧:Paperback

isbn:9781597494861

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.

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

作者介绍:

目录:

[A Guide to Kernel Exploitation_下载链接1_](#)

标签

kernel

计算机

信息安全

Kernel

security

安全

黑客

计算机科学

评论

漏洞还是那些漏洞，而防御已经不可同日而语。

估计没时间看完。不过这本书读起来非常过瘾。喜欢折腾kernel的人一定会喜欢这本书。

A Guide to Kernel Exploitation_下载链接1_

书评

A Guide to Kernel Exploitation_下载链接1_