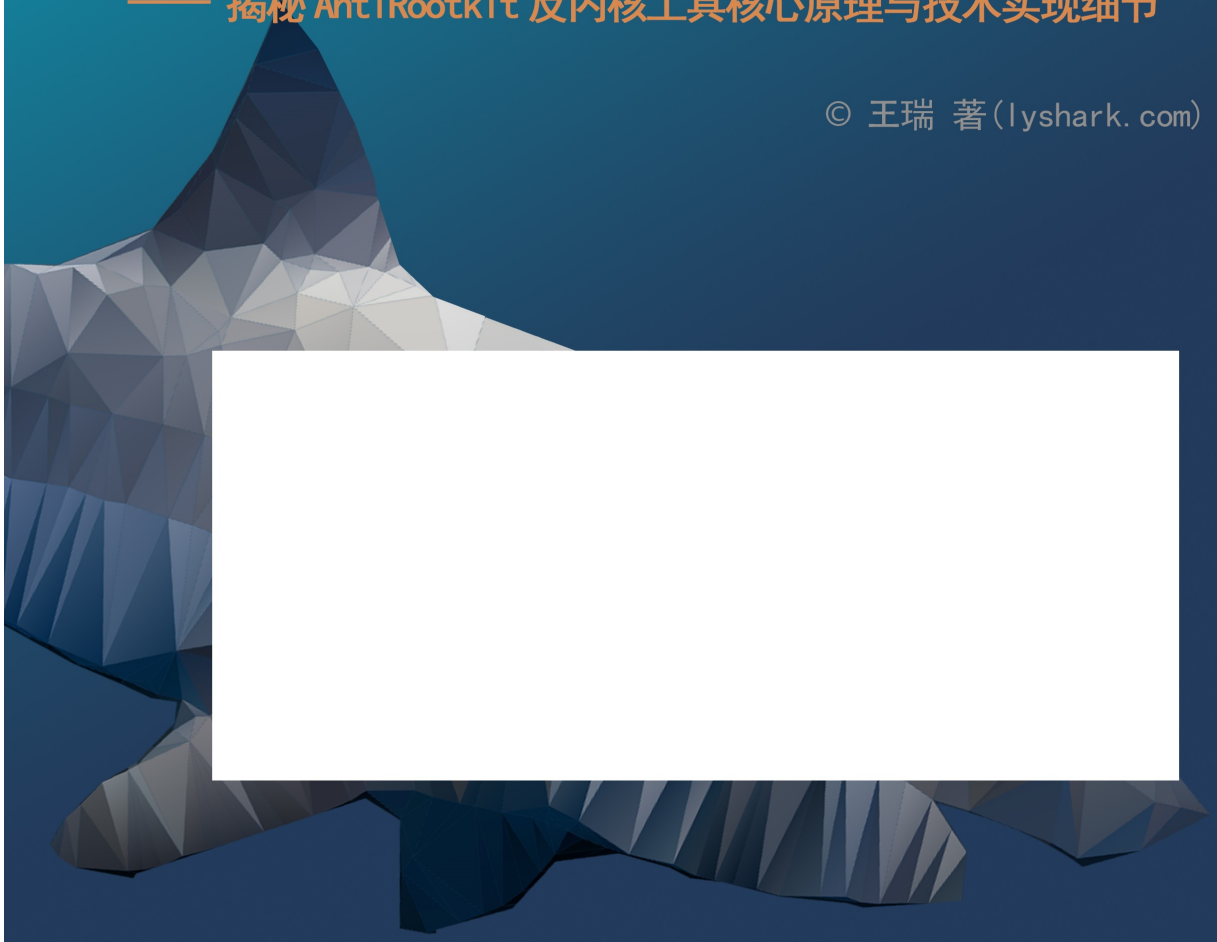
预览版，正在编写

Windows 内核安全编程技术实践（第二版）

—— 揭秘 AntiRootkit 反内核工具核心原理与技术实现细节

© 王瑞 著(lyshark.com)



◆方法独特，提炼核心技术　◆以实战角度出发，学以致用　◆图文并茂，涵盖ARK核心实现细节

前言

作者： 王瑞
页数： 800页
开本： 16开
装帧： 平装
兼容系统： Windows 10 Build 18362.19h1（x64 bit）
所属分类： 信息安全/软件安全/内核安全编程
作者邮箱： me@lyshark.com

书籍概述

《Windows 内核安全编程技术实践（第二版）》是2023年申请（国著）登记的内核安全开发系列PDF电子书，作者是王瑞。本书图文并茂、深入浅出、案例丰富，是Windows内核开发工程师的参考资料，也可供信息安全，软件工程等相关专业本科及以上在校生学习参考。本书是近年来少见的关于揭秘AntiRootkit反内核工具实现细节的相关书籍。

内容简介

这是一本`Windows`内核安全编程系列丛书（纯64位），由作者多年技术积累编写而成，该书由浅入深、循序渐进地介绍了`Windows`内核程序的开发方法与调试技巧。书如其名揭秘`Anti Rootkit`反内核工具核心原理与技术实现细节，本书最大的特色在于每一节的例子都是经过精挑细选的，具有很强的针对性。不同于市面上的多数`内核开发`系列丛书，本书是以内核安全角度为切入点，以实战角度出发，力求让读者通过亲自动手实验，掌握各类`Windows`内核安全编程的相关技巧，学到尽可能多的`Windows`底层知识。 本书适用于中、高级系统安全工程师，同时也可用做高校计算机专业操作系统开发实验课的补充教材。

作者简介

王瑞，LyShark 门户创始人，毕业于中国海洋大学（计算机科学与技术）专业，曾就职于中国联通（北京），二进制安全专家，持有红帽认证RHCE工程师，华为认证HCIP网络安全高级工程师，Oracle甲骨文认证数据库专家，软考信息安全工程师，软考系统架构设计师。自幼便对计算机产生了浓厚兴趣，自学二进制安全方向十余年，常在互联网博客平台分享安全技术研究经验及成果，对网络安全，安全运维，渗透测试，安全开发，软件逆向分析，计算机反病毒，等技术都具有浓厚的兴趣。

作者曾荣获 CSDN-博客专家认证，51CTO博客-专家博主，华为云-云享专家，阿里云-专家博主，开源中国-推荐博主，CSDN-全栈领域优质创作者，CSDN-2022年度博客之星Top5，InfoQ中国-签约作者，博客园Top500总阅读量600余万，腾讯云-2022年度优秀作者奖。

作者自述

在正式开始阅读此书之前我还是希望您能阅读一下这段自述，首先非常感谢多年以来一直关心和支持我的朋友们，同时也非常感谢那些不停的鞭策我勇往直前的批评者，嘲讽者们，是你们给了我力量让我能继续坚持下去。

2010年，13岁的我正式开始了自学计算机编程之路，光阴易逝，转眼间13年过去了，我依靠完全自学，从一个不会打字的新手变成了一名二进制安全专家，在自学的道路上我经历了太多的无奈，太多的嘲讽，我在一个完全不适合学习技术的环境中硬生生地将自己变成了一名专业技术人才，自学道路中总有孤独与我相伴，我在孤独与寂寞中慢慢的爬行。

如果你要问我不抛弃不放弃的含义，那么我可以告诉你，当所有人包括你的父母，都认为你只有死路一条的时候，而你却能够起死回生，解决所有困难力挽狂澜，甚至还会让他们觉得你是个天才，这就是不抛弃不放弃的含义，正所谓厚德载物，自强不息，水到绝境是风景，人到绝境是重生。

有些朋友想要知道 LyShark 的含义，其含义是从开始到结束我都是孤独的，不论是在网络里还是现实中我都是孤独的，至于鲨鱼，它是海洋里的霸主，独自掠食，在孤独中体会自己热爱的技术，我会带着自己的这份热忱独自一人游向深蓝。来日方长，未来可期，我将义无反顾坚守初心，自我成就！

回到正题中，目前国内有不计其数的计算机专业毕业生，但是真正合格的程序员却少之又少，甚至大学毕业了都只学到了皮毛。业内的很多人其实都知道原因。大学缺乏合格的计算机专业老师，只会照本宣科、没有工程实践的老师永远也教不出合格的程序员。而真正经验丰富、适合做老师的程序员又没有教书育人的机会。

目前对于市面上内核开发系列书籍，普遍都存在一个共同弊端。本质上来说内核开发都是计算机行业的高大上代名词（在程序员眼中研究内核开发的也都是鼻祖级别的存在），学习内核开发的开发者理应具备计算机领域专业知识。市面上的内核开发系列书籍多数都较为专业并不适合新手入门学习，而高手则更嫌浪费时间阅读太多的废话。新手看不懂，高手嫌啰嗦，这就是内核开发系列图书的现状。

为了规避上述问题，本书在编写时就考虑到了两者的利弊，并想要在这其中找到一种平衡，让新手可以尽可能看懂，让高手也可以更容易地得到所需要的代码片段，书如其名，突出技术实践性，将关键代码中的关键内容进行精讲，将无关紧要的知识体系进行一定程度的跳过，重在实现功能，以及对功能的灵活运用上，让内核开发不再那么"高大上"，让新手也可以"快速入门"，我认为这就是这本书的价值所在。

在阅读此书时，读者需要具备以下几个方面的基础知识。

口 扎实的 C/C++ 开发能力
口 扎实的 Windows 汇编开发能力
口 熟练使用 Visual Studio 2013
口 熟练使用 VMware Workstation

具备了如上这些知识体系，就能根据自己的实际需求来学习本书的内容。如果你是一位优秀的应用层开发工程师，又或是高等院校计算机相关专业的学生(本科或本科以上)，内核开发技术将会给你带来崭新的职业发展空间，使你有足够的技术竞争力面对软件研发行业。同时，信息安全（二进制安全）行业也会是你新的求职方向。

王瑞

2023年12月22日 于 北京

书籍目录