<<Windows内核安全编程从入门到实>>

图书基本信息

书名：<<Windows内核安全编程从入门到实践>>

13位ISBN编号：9787121160981

10位ISBN编号：7121160986

出版时间：2012-4

出版时间：电子工业出版社

作者：《黑客防线》编辑部　组编

页数：424

前言

前言　　记得第一次在内核中简单调用DbgPrint函数输出“ helloworld ”时兴奋得手舞足蹈，也记得之后开发ARP防火墙时遭遇无数次蓝屏而无限接近崩溃的状态。
时至今日，接触Windows内核安全编程已有三年时间了，期间断断续续地写了一些小程序，直到偶然一天收到《黑客防线》杂志的邀请而萌生了写一本书记录自己一路走来经历的想法，对于和我一样正走在学习Windows内核安全编程之路上的菜鸟们来说，有很大的阅读价值，尤其对于那些正准备上路或者刚刚上路的新晋菜鸟而言，通过阅读本书，可以少走很多无谓的弯路。

本书的结构　　本书共包括10章，其中：　　第1～3章为基础篇，介绍基于Windows编程的基础知识；　　第4～8章为提升篇，通过具体示例介绍各Windows组件相关的编程方法；　　第9～10章为辅助篇，简单介绍安全编码及逆向与调试程序的方法。

本书的理论部分主要以WDK文档作为支撑，全书关于理论介绍的知识绝大部分来源于WDK，另外一小部分知识直接或间接来源于其他文档（如Windbg文档等）、书籍（如WindowsInternal4等）、网络及个人经验等。

本书的实践部分来源于WDK提供的例子及个人项目，建议读者在虚拟机中运行示例。

本书的阅读说明　　读者可以根据需要选择阅读感兴趣的章节，也可以从头至尾完整地阅读全书。

除了特别说明适用于Windows7或其他系统的内容除外，本书所有的内容默认适用于WindowsXP系统。

每章提供的示例建议在虚拟机环境下运行。
由于本人能力和时间有限，并没有在真机环境中测试过，不能保证所提供的示例程序稳定运行在各种环境下，若直接运行于真机环境中，可能会对您的计算机财产造成不必要的损害。

致谢　　感谢赵跃华教授对我的悉心培养；感谢张翼（xyzreg）学长对我多年的指导和照顾；感谢全体535实验室的师弟师妹们对本书的文字修正；感谢黑客防线在合作过程中的细致帮助；最后，感谢我的父母对我无尽的给予。

如果您在阅读过程中发现本书的技术性错误，或者有好的建议，欢迎致信ifsecurity588@gmail.com。

作者　　2011/12/28ax

内容概要

本书详细介绍了Windows平台下的内核安全编程知识。
首先简单介绍了驱动编程的基本方法；然后详细介绍了Windows各个系统组件的工作原理，如文件系统、网络系统自上而下的执行流程。
同时还介绍了各个组件涉及的安全问题，如文件隐藏、键盘记录等，并通过工程项目让读者从代码层级了解这些信息安全问题及解决方法；最后介绍了驱动编程本身的安全问题，如安全编码的注意事项和脆弱代码的检测手段。
另外本书还介绍了简单的调试和逆向技术，帮助解决开发过程中遇到的技术难题。
通过阅读本书，可以帮助读者更深层次的了解内核态下的信息安全知识。

本书适合大专院校计算机系的学生、windows程序员、从事信息安全行业的工程师以及所有对windows内核安全编程感兴趣的爱好者使用。

书籍目录

章节摘录

编辑推荐

《网络安全入门与提高：Windows内核安全编程从入门到实践》适合大专院校计算机系的学生、Windows程序员、从事信息安全行业的工程师以及所有对Windows内核安全编程感兴趣的爱好者使用。

版权说明