第一图书网, tushu007.com

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

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

第一部分 基础篇
第1章 前置要求与环境搭建
1.1 驱动编程的语言
1.2 开发环境搭建
1.2.1 Visual Studio 2005/2008的安装与配置
1.2.2 WDK的安装与配置
1.2.3 VisualDDK的安装与配置
1.3 常用工具介绍
第2章 内核编程基础知识
2.1 Windows主要系统组件
2.1.1 对象管理器
2.1.2 内存管理器
2.1.3 进程和线程管理器
2.1.4 I/O管理器
2.1.5 PnP管理器
2.1.6 电源管理器
2.1.7 配置管理器
2.1.8 安全引用监视器
2.2 常见名词解释
2.2.1 内核名词
2.2.2 文件名词
2.2.3 网络名词
2.3 常见内核数据结构
2.3.1 驱动框架常见数据结构
2.3.2 进程与线程数据结构
2.3.3 存储系统数据结构
2.3.4 网络数据结构
2.3.5 其他一些常见的数据结构
第3章 基本编程方法
3.1 简单的NT式驱动模型
3.1.1 驱动模型的选择
3.1.2 NT式驱动程序基本结构
3.1.3 编译驱动程序
3.1.4 加载驱动及查看输出信息
3.2 应用层与内核的通信方法
3.2.1 访问数据的I/O方式
3.2.2 读写驱动程序
3.2.3 发送I/O控制码
3.2.4 内存共享
3.3 同步技术
3.3.1 事件对象
3.3.2 信号灯对象
3.3.3 互斥体对象
3.3.4 定时器对象
3.3.5 自旋锁

3.3.6 回调对象
3.3.7 原子操作
3.4 IRP处理
3.4.1 简单的IRP流动图
3.4.2 IRP的创建
3.4.3 IRP的发送
3.4.4 为IRP设置完成函数
3.4.5 IRP的完成
3.4.6 多种典型的 IRP处理示例
3.5 字符串操作
3.5.1 STRING、ANSI_STRING和UNICODE_STRING
3.5.2 初始化和销毁
3.5.3 复制和添加
3.5.4 比较
3.5.5 转换
3.6 内存管理
3.6.1 分配系统空间内存
3.6.2 运行时库管理函数
3.6.3 使用内核栈
3.6.4 使用Lookaside快速链表
3.6.5 访问用户空间内存
3.6.6 内存区对象和视图
3.6.7 MDL的使用
3.7 注册表编程
3.7.1 注册表对象管理函数
3.7.2 注册表运行时库函数
3.7.3 注册表调用过滤
3.8 文件编程
3.8.1 打开文件句柄
3.8.2 执行相关文件操作
3.9 其他
3.9.1 本地系统服务函数的Nt和Zw版本
3.9.2 NTSTATUS返回值
3.9.3 双向链表的使用
3.9.4 异常处理
第二部分 提升篇
第4章 进程
4.1 进程监控实现原理
4.2 Windows 7系统下的进程
监控软件实例
4.2.1 内核模块程序实现
4.2.2 用户模式程序实现
4.3 安装与使用
第5章 磁盘
5.1 存储驱动体系结构
5.2 设备树示例
5.3 diskperf磁盘过滤驱动

5.3.1 diskperf介绍
5.3.2 diskperf的过滤框架
5.3.3 diskperf的PnP支持
5.3.4 diskperf的硬盘访问监控和性能数据捕获
5.3.5 diskperf的电源支持
5.3.6 diskperf的安装与测试
第6章 键盘
6.1 原理跟踪
6.1.1 自下而上的过程
6.1.2 自上而下的过程
6.2 几种常见的键盘记录行为
6.2.1 应用层的消息钩子
6.2.2 键盘过滤驱动
6.2.3 键盘类驱动的分发函数Hook
6.2.4 DKOM技术
6.2.5 其他方法
6.3 反键盘记录
6.3.1 实现原理
6.3.2 反键盘记录示例
第7章 文件
7.1 原理跟踪
7.1.1 Windows存储栈
7.1.2 不涉及缓存的数据存储
7.1.3 涉及缓存的数据存储
7.2 简单的文件隐藏
7.2.1 文件隐藏的原理
7.2.2 文件隐藏的实现
7.3 scanner扫描程序
7.3.1 过滤管理器与微过滤驱动概念
7.3.2 使用过滤管理模型的优势
7.3.3 微过滤驱动的加载和卸载
7.3.4 用户模式和内核模式的交互
7.3.5 scanner介绍
7.3.6 scanner驱动程序
7.3.7 scanner应用层程序
7.3.8 scanner的安装与使用
第8章 网络
8.1 原理跟踪
8.2 NDIS协议驱动
8.2.1 DriverEntry
8.2.2 绑定
8.2.3 数据发送
8.2.4 数据接收
8.2.5 数据流动总结
8.3 OPEN_BLOCK的展示
8.3.1 原理知识
8.3.2 相关代码

第三部分 辅助篇
第9章 安全编码
9.1 蓝屏的概念
9.2 创建可靠的驱动程序
9.2.1 验证设备对象
9.2.2 使用安全字符串
9.2.3 验证对象句柄
9.2.4 支持多CPU
9.2.5 确认驱动状态
9.2.6 IRP安全检查
9.3 使用驱动验证程序
9.3.1 驱动验证程序的测试选项
9.3.2 使用驱动验证程序
第10章 调试与逆向
10.1 静态调试
10.1.1 静态调试驱动程序
10.1.2 静态调试应用程序
10.2 动态调试
10.2.1 双机调试的基本方法
10.2.2 WinDbg的常用命令
10.2.3 WinDbg的使用技巧
10.3 逆向与调试相结合
10.3.1 示例

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

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com