

图书基本信息

书名：<<主机防火墙设计技术及Tdifw源代码分析>>

13位ISBN编号：9787302300694

10位ISBN编号：7302300690

出版时间：2012-11

出版时间：清华大学出版社

作者：伍红兵，胡勇强，俞海英 著

页数：399

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>

## 内容概要

《主机防火墙设计技术及Tdifw源代码分析》以开源项目Tdifw为素材，详细分析了主机防火墙设计技术及实现。

《主机防火墙设计技术及Tdifw源代码分析》的目的是帮助读者学习和掌握防火墙设计技术与实现方法。

主机防火墙一般采用“服务+驱动”的系统构架，能够控制哪个用户运行的哪个进程能够访问哪个远程主机的哪个端口。

相应地，主机防火墙开发者首先需要具备Windows安全模型、服务应用程序设计、内核驱动程序设计、网络体系结构等方面的知识，然后需要掌握如何运用这些技术开发主机防火墙。

围绕这些内容，《主机防火墙设计技术及Tdifw源代码分析》分为以下几个部分：Windows安全模型；服务与事件日志；内核驱动程序设计；Windows网络体系结构；Tdifw防火墙设计技术与源代码分析。

本书适合大专院校计算机专业的学生、Windows程序员、Windows内核程序员、信息安全领域的程序员以及对Windows防火墙设计感兴趣的编程爱好者使用。

阅读本书需要有C语言、Windows操作系统和计算机网络的基础知识。

## 书籍目录

第1章Windows安全模型 1.1受保护的對象 1.2對象安全模型 1.3安全标识符 1.4访问令牌 1.4.1模仿 1.4.2受限制的令牌 1.5安全描述符 1.5.1 ACL分配 1.5.2访问控制检查 1.6账户权限和特权 1.6.1账户权限 1.6.2账户特权 1.7 Windows安全性组件 1.8一个不容易理解的问题 1.8.1登录会话 1.8.2会话 1.8.3窗口站和桌面 1.8.4小结 第2章服务与事件日志 2.1 Windows服务概览 2.1.1服务相关组件 2.1.2服务相关注册表项 2.2服务程序工作原理 2.2.1进程入口函数 2.2.2服务入口函数 2.2.3服务控制处理器 2.2.4控制码和状态报告 2.3服务控制程序 2.3.1打开SCM 2.3.2安装服务 2.3.3删除服务 2.3.4启动与控制服务 2.3.5重新配置服务 2.3.6锁定SCM数据库 2.4服务调试 2.5事件日志 2.5.1报告事件 2.5.2消息文件 2.5.3事件日志体系结构和开发流程 2.5.4创建消息文件 2.5.5编译消息 2.5.6资源文件 2.6 Windows服务举例——ServiceFramework 2.6.1安装服务 InstallService 2.6.2服务程序 MyService 2.6.3客户端程序 MyClient 第3章 内核驱动程序设计 3.1基本驱动程序示例 3.1.1基本的NT驱动BaseNT 3.1.2基本的WDM驱动 3.2设备驱动程序基本概念 3.2.1系统I/O组件 3.2.2驱动程序基本结构与工作模型 3.2.3驱动程序分类 3.2.4 WDM驱动程序与设备栈 3.2.5设备栈的建立 3.2.6 IRP在设备栈中的传递 3.2.7分层的驱动程序 3.2.8注册表中的驱动程序信息 3.2.9设备枚举 3.2.10驱动程序加载顺序 3.3关键数据结构 3.3.1驱动对象 3.3.2设备对象 3.3.3文件对象 3.3.4 I/O请求包IRP 3.3.5 I/O栈单元 3.4驱动程序编译 3.4.1使用WDK的编译环境编译驱动程序 3.4.2使用Visual Studio编译驱动程序 3.5驱动程序调试 3.5.1调试环境设置 3.5.2结合WRK对项目调试 3.6驱动程序安装 3.6.1设备安装组件 3.6.2 PNP设备安装举例 3.6.3 INF文件 3.7 Toaster示例分析 3.7.1 目录和文件说明 3.7.2编译方法 3.7.3驱动安装 3.7.4运行示例 3.7.5过滤驱动 3.7.6设备栈 第4章Windows网络体系结构 4.1 网络API 4.2 WinSock 4.2.1 SPI 4.3传输驱动程序接口TDI 4.4网络驱动程序接口规范NDIS 4.5 Windows平台下的防火墙方案 4.5.1用户级的实现方法 4.5.2核心级的实现方法 4.5.3各种拦截方案比较 4.6对传输驱动接口TDI的讨论 4.6.1传输驱动程序接口(TDI) 4.6.2 TDI设备对象 4.6.3 TDI文件对象 4.6.4 TDI传输驱动程序例程 4.6.5 TDI内核模式客户交互 4.6.6 TDI请求及事件 第5章Tdifw防火墙设计技术与源代码分析 5.1 Tdifw安装与使用 5.1.1 Tdifw体系结构 5.1.2系统文件说明 5.1.3安装 5.1.4配置文件Tdifw.conf 5.2分析环境构建 5.2.1 Tdifw移植到Visual Studio 2010要点 5.2.2 Tdifw项目调试 5.2.3增加输出错误信息的可读性 5.3 Tdifw安装程序tdi\_install.C 5.3.1 Tdifw过滤驱动在系统中的位置 5.3.2 install.exe使用方法 5.3.3 tdi\_install.c注释 5.4 SVC项目 5.4.1 SVC项目中的内存泄露检测——CRT调试堆 5.4.2 main.C文件 5.4.3 SVC项目的错误信息输出 5.4.4 Tdifw服务线程service\_main 5.4.5 start函数 5.4.6 stop函数 5.4.7加载配置文件 5.4.8服务程序响应驱动程序请求 5.4.9处理驱动程序请求 5.4.10其他函数的解释 5.4.11 Tdifw服务中的消息文件 5.5 drv驱动项目 5.5.1 drv项目中的内存泄露检测 5.5.2驱动入口DriverEntry 5.5.3 ot—init 5.5.4 filter\_init 5.5.5 conn\_state\_init 5.5.6 c\_n\_a\_device 5.5.7 OnUnload 5.5.8 d\_n\_d\_device 5.5.9分发例程DeviceDispatch 5.5.10 tdi\_create 5.5.11 tdi\_dispatch\_complete 5.5.12处理IRP\_MJ\_INTERNAL\_DEVICE\_CONTROL请求的函数 参考文献

## 章节摘录

版权页：插图：2.6.2 服务程序MyService 服务程序只是一个框架，没有完成什么有意义的工作，需要理解框架的结构，知道如果要增加有意义的工作应该在什么位置增加代码。

代码主要流程为：（1）定义服务表项SERVICE\_TABLE\_ENTRY；（2）调用StartServiceCtrlDispatcher函数启动服务线程；（3）服务线程入口函数service\_main注册服务控制处理器函数service\_ctrl，然后调用服务的主体函数ServiceSpecific；（4）ServiceSpecific函数完成服务的主要工作：加载自定义的注册表项中的配置信息；创建命名管道以准备与客户端程序通信；启动线程PipeThread专门用于通过命名管道与客户端程序通信；启动一个while循环，完成服务的主体工作，本例只是完成一些测试工作：将一些信息写入自定义的文本格式的日志文件中、将一些信息写入标准的Windows事件日志中。

（5）service\_ctrl函数接收SCM的控制请求，其中最重要的工作是处理SERVICECONTROL\_STOP控制请求、停止服务，停止的方法很简单，将控制服务是否停止的全局变量g\_shutDown设为TRUE，ServiceSpecific函数中的while循环会判断该全局变量以决定是否退出循环，一旦退出循环，ServiceSpecific函数就会返回，接着service\_main函数也会返回，服务线程终止，最后StartServiceCtrlDispatcher函数也结束，主线程终止，从而整个服务也就停止了。

（6）在以上过程中适当的地方调用ReportStatusToSCMMgr函数报告服务的运行状态。

下面对其中的重要函数做一个说明。

1.main（）函数 这是服务应用程序的主线程入口函数，一般情况下由SCM负责加载。

主要工作就是定义服务表项SERVICE\_TABLE\_ENTRY，然后调用StartServiceCtrlDispatcher函数启动服务线程。

其中加了一个调试功能，如果在命令行直接输入：则程序由系统的SHELL加载，而不是由SCM加载，也不会调用StartServiceCtrlDispatcher函数，而是直接调用服务的主体函数ServiceSpecific：从而整个程序就像一个普通的控制台程序，在ServiceSpecific函数中设置断点，可以调试服务的主体功能。

编辑推荐

《主机防火墙设计技术及Tdifw源代码分析》适合大专院校计算机专业的学生、Windows程序员、Windows内核程序员、信息安全领域的程序员以及对Windows防火墙设计感兴趣的编程爱好者使用。

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>