<<主机防火墙设计技术及Tdifw源 >

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

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“服务十驱动”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。

<<主机防火墙设计技术及Tdifw源　>

书籍目录

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ReportStatusToSCMgr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