



计算机专业人员书库

朱雁辉 编著
朱雁冰 审校

Windows 防火墙与 网络封包截获技术



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

计算机专业人员书库

Windows 防火墙与网络封包 截获技术

朱雁辉 编著

朱雁冰 审校

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书首先论述了各种常用的网络封包截获方法,包括传输层过滤驱动程序、NDIS 中间驱动程序和 Winsock 2 SPI。然后以 Xfilter 个人防火墙为实例,从功能分析、模块设计、文件结构定义、界面设计到编码、制作帮助文件及制作安装盘,完整地介绍了软件开发的全过程。因此,从本书中不仅可以学到较为全面的封包截获技术,而且可以借鉴工程化的方法制作自己的软件。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

Windows 防火墙与网络封包截获技术/朱雁辉编著. —北京:电子工业出版社,2002.7

(计算机专业人员书库)

ISBN 7-5053-7717-5

I. W… II. 朱… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2002)第 040949 号

责任编辑:黄志瑜

特约编辑:李建森

印 刷:北京东光印刷厂

出版发行:电子工业出版社 <http://www.phei.com.cn>

北京市海淀区万寿路 173 信箱 邮编 100036

经 销:各地新华书店

开 本:787×1092 1/16 印张:38.5 字数:985.6 千字 附光盘 1 张

版 次:2002 年 7 月第 1 版 2002 年 7 月第 1 次印刷

印 数:6 000 册 定价:62.00 元(含光盘)

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。

联系电话:(010)68279077

前言

随着网络的普及，安全问题正威胁着每一个网络用户。由于黑客攻击和信息泄漏等安全问题并不像病毒那样直截了当地对系统进行破坏，而是故意隐藏自己的行动，所以往往不能引起人们的重视。但是，一旦网络安全问题发生，通常会带来严重的后果。因此，必须加强安全意识，并及早防范。目前最常用的网络安全防范工具是防火墙，相信不用多久，防火墙软件就会像防病毒软件那样安装在每一个人的计算机上。这将产生一个巨大的网络安全市场。作为软件开发者的程序员更要抓住这个机遇，掌握这门专业技术，为自己创造更多的机会。

由于网络安全技术涉及到太多的机密问题，所以这项技术总是以原理的形式出现，具体实现方法很少有人提及。因此，网络安全技术的发展受到了很大阻碍，能够掌握这门技术的专业极人才也非常匮乏。本书首次公开了完整的防火墙源程序和文档，并对关键技术和程序进行了详细的说明。另外，本书的网站 <http://www.xfilt.com> 作为在线平台会及时地对技术进行跟进和更新，因此本书是学习防火墙和网络编程的理想选择。

主要内容

本书首先论述了常用的各种网络封包截获方法，包括传输层过滤驱动程序、NDIS 中间驱动程序、Winsock 2 SPI。然后以 Xfilter 个人防火墙为实例，从功能分析、模块设计、文件结构定义、界面设计到编码、制作帮助文件及制作安装盘，完整地介绍了软件开发的全过程。因此，从本书中不仅可以学到较为全面的封包截获技术，而且可以借鉴工程化的方法制作自己的软件。

本书的特色

本书从需求分析到打包发布，详尽地介绍了一个软件产品的生产全过程。这些一向被认为是商业机密的资料被首次公开。

本书所使用的实例，是一个精心设计的、完整的个人防火墙软件产品 Xfilter，此外，还有许多精巧实用的实例。Xfilter 是一个具有典型功能的防火墙产品，它最具意义的是公开了完整的源代码。网络安全产品一向以技术含量高、保密性强而著称；公开防火墙的源代码，无疑会给黑客提供更好的机会去创造攻击手段。但是事物总有两面性，事实上，它有更好的一面。它可以帮助广大程序员掌握这门核心技术，以编写更安全的防火墙软件。

本书对示例的讲解有一个显著的特点就是“完整”。为适应基础不同的读者的需要，本书在对示例论述的时候，尽量做到使过程描述完整。

本书的读者

本书适于以下类型的读者阅读。

- (1) 需要用到网络封包截获技术的读者，这本书能给予很大的帮助。
- (2) 做网络安全软件开发的读者。有关这方面内容的实例性图书，市面上不多见，这本书是他们所渴望得到的。
- (3) 刚学了一点 VC 基础，正愁着没有项目试验的读者。这本书不仅可以让你由浅入深地掌握防火墙的开发技术，而且可以成为熟练的 VC 程序员。
- (4) 需要提高系统分析能力的读者。理解并消化好书里的例子，将增进系统分析经验，提高系统分析的能力。
- (5) 做软件驱动程序开发的读者。掌握了书中的最小化示例，做驱动程序就像编写“Hello World”一样简单。
- (6) 计算机专业的同学们，如果你正找不到系统分析的参考资料来做毕业论文，这里面对你想要的资料。

如何阅读本书

本书分为 3 大部分：

第一部分，网络封包截获技术。除了介绍常用的网络封包截获技术外，还加入了 Windows 的网络架构和构建编程环境的相关内容。

第二部分，Xfilter 个人防火墙实例剖析。这一部分包括 Xfilter 个人防火墙的系统设计、代码分析、帮助文件制作、安装盘制作和测试文档等内容。

第三部分，附录。这一部分给出了 Winsock 2 传输服务提供者的 31 个函数的解释以及 Xfilter 使用的宏代码、全局变量和结构类型的说明。

如果想系统地了解各种封包截获方法和实际应用，可以从头到尾地阅读本书，由浅入深地掌握核心技术和实战经验。另外，本书的一些章节有很高的独立性，所以也可以按照需求跳跃式地阅读感兴趣的章节。

(1) 如果对 Windows 的核心架构不太了解，建议阅读第 1 章。

(2) 如果只对驱动程序截获网络封包感兴趣，可以直接阅读第 3 章和第 4 章。如果在阅读过程中还想创建自己的编程环境来做实验，可以回过头阅读第 2 章。

(3) 如果对 Xfilter 的核心技术 Winsock 2 SPI 感兴趣，建议从第 5 章开始顺序阅读。第 5 章是对 Winsock 2 SPI 的基础论述，并且有较为简单的示例，可以作为入门章节。第 6 章是一个完整的 SPI 示例，介绍了如何用 Winsock 2 SPI 技术截获网络封包。第 8 章、第 9 章和第 10 章讲述了 Xfilter 如何利用 Winsock 2 SPI 来完成对网络封包的截获、分析和控管。

(4) 如果想知道 Xfilter 的系统设计，则可以直接阅读第 7 章。

(5) 如果想整体地把握 Xfilter 技术，最好的办法是完整地阅读 Xfilter 的源代码。在阅读的过程中可充分利用本书的系统分析文档和函数说明，以使用最短的时间掌握最多的知识。

(6) 如果只对帮助文件制作感兴趣，则可以直接阅读第 16 章。

(7) 如果只对安装盘制作感兴趣，则可以直接阅读第 17 章。

(8) 如果已经掌握了 Winsock 2 SPI 技术，只是在实际编程过程中需要实时查阅函数资料，则可以查阅附录 A。

致谢

感谢我的父母，他们不辞劳苦地工作，为我创造了一个温暖而又稳定的环境，让我可以无忧无虑地写作。感谢我的弟弟朱雁冰，他除了帮我搜集资料和校稿外，还为 Xfilter 写了一部分代码。没有他们的帮助就没有这本书的出版，在此向他们表示深深的谢意！另外更要感谢我的好友余超，他为本书提出的真知灼见非常难能可贵。

如果有什么意见或建议，请发送电子邮件到 xstudio@371.net 或 xstudio@xfilt.com。

配套光盘包括的内容

Winsock 2 SPI 相关示例：

(1) MinWinsockSpi

最小化的基础服务提供者及安装例程。

(2) MinLSP

最小化的分层服务提供者及安装例程。

(3) PacketCapture

截获网络封包的基础服务提供者及安装例程。

(4) GuiDesign (VB)

Xfilter 个人防火墙的界面设计。

(5) Xfilter

提供 Xfilter 个人防火墙 1.0.2 版的完整代码。另外，还包含帮助文件制作的源文件、安装程序制作的源文件及完整的安装程序。

DDK 相关的示例：

(1) MinDriver

最小化的驱动程序。

(2) MinDriverInVc

在 VC 中编译最小化的驱动程序。

(3) FilterTdiDriver

截获网络封包的传输层过滤驱动程序。

(4) xpassthru

截获网络封包的 NDIS 中间驱动程序。

相关工具 (tools)：

DumpSpi.exe

枚举出系统所有 Winsock 2 SPI 传输服务提供者的网络协议结构和路径信息。

另外，学习中一定要有一个调试信息的监视软件。本书没有附带这样的工具，但很容易从网站上获得。例如常见的 DbgView.exe，网址是：www.sysinternals.com。也可以任意选用其他的 Debug View 工具软件。本书以 DbgView.exe 为例进行讲述。

目 录

第一部分 Windows 网络封包的截获技术

第 1 章	Windows 网络协议架构	(3)
1.1	Windows 网络协议的实现	(3)
1.2	Windows 操作系统的总体架构	(3)
1.3	网络 7 层协议在 Windows 中的实现	(5)
1.4	TCP/IP 协议的架构	(7)
1.5	TCP/IP 协议在 Windows 中的实现	(9)
第 2 章	编程环境的构建	(10)
2.1	硬件需求	(10)
2.2	软件需求	(11)
2.3	软件安装	(11)
2.4	VC6 IDE 环境的设置	(11)
2.5	编译并测试 Winsock 示例程序	(13)
2.6	编译并测试 DDK 示例程序	(15)
2.6.1	测试驱动程序示例程序	(15)
2.6.2	编译驱动程序示例程序	(16)
2.6.3	在 VC 环境下编译驱动程序	(17)
第 3 章	用传输层过滤驱动程序截获网络封包	(21)
3.1	一个最小化的驱动程序	(21)
3.1.1	MinDriver.h 代码清单	(21)
3.1.2	MinDriver.c 代码清单	(22)
3.2	过滤驱动程序的特性	(23)
3.3	传输层过滤驱动程序实例	(24)
3.3.1	在 Packet.h 里定义的宏和结构类型	(24)
3.3.2	FilterTdiDriver 入口函数 DriverEntry	(26)
3.3.3	用来绑定过滤驱动程序的函数 TCPFilter_Attach	(27)
3.3.4	卸载驱动程序的函数 DriverUnload	(30)
3.3.5	解除挂接的函数 TCPFilter_Detach	(32)
3.3.6	用来分发 IRP 请求的函数 PacketDispatch	(33)
3.3.7	IRP 处理完成后的回调函数 PacketCompletion	(37)
3.3.8	工程文件 Source	(38)
第 4 章	用 NDIS 中间驱动程序截获网络封包	(39)
4.1	NDIS 简介	(39)

4.2	中间驱动程序的特性	(39)
4.3	编译、安装和测试 xpass thru	(41)
4.4	xpass thru 的架构	(43)
4.5	xpass thru 使用的宏、结构和全局变量	(44)
4.6	xpass thru 的入口函数 DriverEntry	(47)
4.7	注册 Miniport 设备的函数 MPRegisterAsMiniport	(49)
4.8	注册 Protocol 设备的函数 MPRegisterAsMiniport	(50)
4.9	Miniport 接口函数	(52)
4.10	Protocol 接口函数	(54)
4.11	发送封包的函数	(58)
4.11.1	MPSend	(58)
4.11.2	MPSendOnePacket	(59)
4.11.3	MPSendPackets	(61)
4.11.4	PtSendComplete	(62)
4.11.5	MPTransferData	(63)
4.11.6	PtTransferDataComplete	(64)
4.12	接收封包的函数	(65)
4.12.1	PtReceive	(65)
4.12.2	PtReceiveComplete	(69)
4.12.3	PtReceivePacket	(70)
4.12.4	MPReturnPacket	(72)
4.13	得到封包属性的函数	(73)
4.14	source 内容清单	(75)
第 5 章	Winsock 2 SPI 编程技术	(77)
5.1	Winsock 2 SPI 基础	(77)
5.1.1	Winsock API 与 SPI 的对应关系	(78)
5.2	传输服务提供者	(79)
5.2.1	最小化的基础服务提供者例程	(84)
5.2.2	最小化的分层服务提供者例程	(90)
第 6 章	用 Winsock 2 SPI 截获网络封包	(106)
6.1	运行程序	(106)
6.1.1	建立截获封包的 DLL 工程	(107)
6.1.2	建立用来安装的 EXE 工程	(108)
6.2	编写安装程序	(109)
6.2.1	输出调试信息的宏	(110)
6.2.2	安装程序代码	(111)
6.2.3	CXInstall 类	(114)
6.2.4	构造完整的安装程序	(127)
6.3	编写截获 TCP/IP 封包的 DLL 程序	(129)

6.3.1 全局变量	(129)
6.3.2 DllMain	(130)
6.3.3 WSPStartup	(132)
6.3.4 截获的服务提供者函数	(135)
6.3.5 工程配置文件 TcpIpDog.Def	(148)
6.3.6 设置、编译和测试 TcpIpDog	(149)

第二部分 Xfilter 个人防火墙实例剖析

第 7 章 Xfilter 个人防火墙系统设计	(153)
7.1 Xfilter 的核心功能分析	(153)
7.2 程序工作流程图	(155)
7.3 Xfilter 的主体功能	(156)
7.4 模块划分	(157)
7.4.1 模块划分原则	(158)
7.4.2 模块结构图	(158)
7.4.3 模块接口定义	(162)
7.4.4 制定测试方法	(163)
7.5 控管规则文件结构设计	(164)
7.5.1 控管规则文件需要存储的内容	(164)
7.5.2 控管规则文件结构	(167)
7.5.3 日志文件需要存储的内容	(170)
7.5.4 日志文件结构	(170)
7.6 网络命令结构	(172)
7.7 界面设计	(173)
7.7.1 制定界面风格	(173)
7.7.2 界面设计工具选择	(173)
7.7.3 界面设计文档	(174)
7.8 选择开发工具和制定编码规则	(179)
7.8.1 选择开发工具	(179)
7.8.2 编码规则	(180)
第 8 章 Xfilter.dll 的封包截获	(182)
8.1 封包截获相关代码分析	(182)
8.1.1 Xfilter.dll 的入口函数 DllMain	(182)
8.1.2 服务提供者入口函数	(184)
8.1.3 截获的服务提供者函数	(189)
8.1.4 与 Xfilter.exe 的接口函数 XfloControl	(201)
8.1.5 询问是否放行的函数 QueryAccess	(203)
8.2 相关知识点说明	(207)

8.2.1	在不同的进程间共享数据	(207)
8.2.2	全局变量的临界操作	(208)
8.2.3	Win9x 与 WinNT/2000 不同的 DLL 调用方式	(208)
8.2.4	在 DLL 中向进程发送消息完成通信	(209)
第 9 章	Xfilter.dll 的访问控管	(210)
9.1	CCheckAcl 类的原型	(210)
9.2	CCheckAcl 类的成员变量和函数	(212)
9.3	对服务提供者函数做管制的函数	(213)
9.3.1	CheckStartup	(213)
9.3.2	CheckSocket	(214)
9.3.3	CheckCloseSocket	(215)
9.3.4	CheckConnect	(216)
9.3.5	CheckAccept	(217)
9.3.6	CheckSend	(218)
9.3.7	CheckSendTo	(219)
9.3.8	CheckRecv	(220)
9.3.9	CheckRecvFrom	(221)
9.4	封包处理函数	(223)
9.4.1	InitializeSession	(223)
9.4.2	CreateSession	(224)
9.4.3	DeleteSession	(225)
9.4.4	FindSession	(227)
9.4.5	SetSession	(227)
9.4.6	SetSessionEx	(229)
9.4.7	FinallySession	(230)
9.4.8	SendSessionToApp	(231)
9.4.9	GetSessionAndSetSessionNull	(232)
9.5	管制函数	(232)
9.5.1	IsLocalIP	(232)
9.5.2	GetAccessInfo	(234)
9.5.3	GetAccessFromWorkMode	(234)
9.5.4	GetAccessFromAcl	(235)
9.5.5	FindAcl	(240)
9.5.6	FindTime	(240)
9.5.7	FindIP	(242)
9.6	初始化和清理函数	(244)
9.6.1	CCheckAcl	(244)
9.6.2	~CCheckAcl	(244)
9.6.3	SetWindowsVersion	(244)

9.7	设置函数	(246)
9.7.1	IsWin9x	(246)
9.7.2	SetGuiProcessName	(246)
9.7.3	SetGuiWnd	(247)
9.7.4	GetGuiWnd	(247)
9.7.5	SetWorkMode	(247)
9.7.6	GetWorkMode	(248)
9.7.7	SetAcl	(248)
9.7.8	SetAclToChangedMode	(249)
9.8	相关知识点说明	(250)
9.8.1	类的构造函数和析构函数	(250)
9.8.2	全局变量的定义和使用	(251)
9.8.3	用指针实现动态数组	(251)
第 10 章	Xfilter.dll 的协议解析和公用函数分析	(252)
10.1	典型的协议封包数据	(252)
10.1.1	HTTP 协议包头实例	(252)
10.1.2	FTP 下载/上传文件封包实例	(252)
10.1.3	SMTP 发送邮件封包实例	(253)
10.1.4	POP3 接收邮件封包实例	(254)
10.2	CProtocolInfo 类原型	(257)
10.3	CProtocolInfo 类的成员函数列表	(258)
10.4	供外部调用的公共函数	(258)
10.4.1	GetProtocolInfo	(258)
10.5	类内部调用的私有函数	(259)
10.5.1	GetFromSend	(259)
10.5.2	GetFromRecv	(260)
10.5.3	GetFtp	(260)
10.5.4	GetHttp	(262)
10.5.5	GetSmtp	(264)
10.5.6	GetPop3BySend	(265)
10.5.7	GetPop3	(266)
10.6	公共模块 CXCommon 类	(268)
10.6.1	CXCommon 类的原型	(268)
10.6.2	CXCommon 类的成员函数列表	(268)
10.6.3	DIPToSIP	(269)
10.6.4	GetBit	(269)
10.6.5	SetBit	(270)
10.6.6	GetAppPath	(270)
10.6.7	GetPath	(272)

10.6.8	GetName	(272)
10.7	生成 Xfilter.dll 的工程文件 (LspServ.def)	(273)
10.8	小结	(274)
第 11 章	Xfilter.exe 与 Xfilter.dll 的接口	(275)
11.1	建立界面工程	(275)
11.2	主应用程序类 CPropertyApp	(277)
11.2.1	CPropertyApp 类的原型	(278)
11.2.2	CPropertyApp 类的变量	(279)
11.2.3	初始化函数	(280)
11.2.4	退出函数	(287)
11.2.5	菜单函数	(291)
11.2.6	其他函数	(295)
11.3	隐藏的主窗口类 CMainFrame	(298)
11.3.1	CMainFrame 类的原型	(298)
11.3.2	CMainFrame 类的变量列表	(299)
11.3.3	CMainFrame 类的自定义消息处理函数	(300)
11.3.4	CMainFrame 类使用的线程函数	(304)
11.3.5	CMainFrame 类的其他成员函数	(306)
11.4	在任务栏上显示图标的类 CSystemTray	(310)
11.4.1	CSystemTray 类的原型	(310)
11.4.2	CSystemTray 类的成员变量	(311)
11.4.3	CSystemTray 类的成员函数	(311)
11.5	小结	(320)
第 12 章	Xfilter.exe 的文件操作	(321)
12.1	控管规则文件操作类 CAclFile	(321)
12.1.1	CAclFile 类的原型	(321)
12.1.2	CAclFile 类的成员变量	(322)
12.1.3	CAclFile 类的构造和析构函数	(323)
12.1.4	CAclFile 类的公有函数	(324)
12.1.5	CAclFile 类的私有函数	(333)
12.2	日志文件操作类 CXLogFile	(347)
12.2.1	CXLogFile 类的原型	(347)
12.2.2	CXLogFile 类的成员变量	(348)
12.2.3	CXLogFile 类的构造和析构函数	(348)
12.2.4	CXLogFile 类的公有函数	(349)
12.2.5	CXLogFile 类的私有函数	(355)
第 13 章	用户注册和下载网络命令	(360)
13.1	用户注册窗口类 CRegister	(360)
13.1.1	CRegister 类的原型	(360)

13.1.2	CRegister 类的成员变量	(362)
13.1.3	VC 中界面元素对象与变量的绑定	(362)
13.1.4	CRegister 类的成员函数	(363)
13.2	用户注册和下载网络命令类 CHttpRequest	(367)
13.2.1	CHttpRequest 类的原型	(368)
13.2.2	CHttpRequest 类的变量	(369)
13.2.3	构造和析构函数	(369)
13.2.4	网络请求函数	(370)
13.2.5	用户注册函数	(377)
13.2.6	下载网络命令函数	(382)
13.3	模拟超级链接类 CHyperLink	(390)
13.3.1	CHyperLink 类的原型	(390)
13.3.2	CHyperLink 类的成员变量	(391)
13.3.3	CHyperLink 类的成员函数	(392)
13.4	可以更改字体颜色的标签类 CColorStatic	(399)
13.4.1	CColorStatic 类的原型	(399)
13.4.2	CColorStatic 类的成员变量	(399)
13.4.3	CColorStatic 类的成员函数	(399)
第 14 章	Xfilter.exe 的属性页界面	(401)
14.1	属性页总窗口类 CMainSheet	(401)
14.1.1	CMainSheet 类的原型	(401)
14.1.2	CMainSheet 类的变量	(403)
14.1.3	CMainSheet 类的成员函数	(403)
14.2	封包监视窗口类 CPacketMonitor	(412)
14.2.1	CPacketMonitor 类的原型	(412)
14.2.2	CPacketMonitor 类的成员变量	(414)
14.2.3	CPacketMonitor 类的成员函数	(414)
14.3	日志查询窗口类 CLogQuery	(420)
14.3.1	CLogQuery 类的原型	(420)
14.3.2	CLogQuery 类的成员变量	(422)
14.3.3	CLogQuery 类的成员函数	(422)
14.4	控管规则窗口类 CAcl	(431)
14.4.1	CAcl 类的原型	(432)
14.4.2	CAcl 类的成员变量	(434)
14.4.3	CAcl 类成员函数	(434)
14.5	系统设置窗口类 CSystemSet	(446)
14.5.1	CSystemSet 类的原型	(447)
14.5.2	CSystemSet 类的成员变量	(448)
14.5.3	CSystemSet 类的成员函数	(449)

14.6	关于窗口类 CAbout	(451)
14.7	增加欢迎画面	(452)
第 15 章	Xfilter.exe 的控管规则设置	(454)
15.1	控管规则设置窗口类 CAclSet	(454)
15.1.1	CAclSet 类的原型	(454)
15.1.2	CAclSet 类的成员变量	(456)
15.1.3	CAclSet 类的成员函数	(456)
15.2	网络/时间设置窗口类 CNetTimeSheet	(468)
15.2.1	CNetTimeSheet 类的原型	(469)
15.2.2	CNetTimeSheet 类使用的全局变量	(470)
15.2.3	CNetTimeSheet 类的成员函数	(470)
15.3	时间设置窗口类 CSetTime	(475)
15.3.1	CSetTime 类的原型	(475)
15.3.2	CSetTime 类的成员变量	(477)
15.3.3	CSetTime 类的成员函数	(477)
15.4	网络设置窗口类 CSetNet	(486)
15.4.1	CSetNet 类的原型	(486)
15.4.2	CSetNet 类的成员变量	(488)
15.4.3	CSetNet 类的成员函数	(488)
15.5	IP 地址段设置窗口类 CNetIParia	(501)
15.5.1	CNetIParia 类的原型	(501)
15.5.2	CNetIParia 类的成员变量	(503)
15.5.3	CNetIParia 类的成员函数	(503)
15.6	小结	(504)
第 16 章	联机帮助的实现	(505)
16.1	帮助文件制作方法简介	(505)
16.1.1	选择工具	(505)
16.1.2	制作方法	(505)
16.2	在帮助文件中使用 API 主题映射	(512)
16.3	将帮助文件应用到程序中	(514)
第 17 章	打包与测试	(516)
17.1	安装程序的制作	(516)
17.2	测试	(523)
17.3	Xfilter 的部分测试文档	(524)
17.4	小结	(532)

第三部分 附 录

附录 A	传输服务提供者函数	(535)
------	-----------------	-------

A.1	WSPAccept	(535)
A.2	WSPAddressToString	(537)
A.3	WSPAsyncSelect	(538)
A.4	WSPBind	(539)
A.5	WSPCancelBlockingCall	(540)
A.6	WSPCleanup	(541)
A.7	WSPCloseSocket	(541)
A.8	WSPConnect	(542)
A.9	WSPDuplicateSocket	(545)
A.10	WSPEnumNetworkEvents	(546)
A.11	WSPEventSelect	(547)
A.12	WSPGetOverlappedResult	(547)
A.13	WSPGetPeerName	(549)
A.14	WSPGetQOSByName	(550)
A.15	WSPGetSockName	(551)
A.16	WSPGetSockOpt	(552)
A.17	WSPIoctl	(553)
A.18	WSPJoinLeaf	(555)
A.19	WSPListen	(557)
A.20	WSPRecv	(559)
A.21	WSPRecvDisconnect	(561)
A.22	WSPRecvFrom	(562)
A.23	WSPSelect	(565)
A.24	WSPSend	(567)
A.25	WSPSendDisconnect	(569)
A.26	WSPSendTo	(570)
A.27	WSPSetSockOpt	(574)
A.28	WSPShutdown	(575)
A.29	WSPSocket	(576)
A.30	WSPStartup	(578)
A.31	WSPStringToAddress	(579)
附录 B	Xfilter 宏代码	(581)
B.1	最大值代码	(581)
B.2	网络命令代码	(581)
B.3	用户注册代码	(581)
B.4	日志文件相关代码	(582)
B.5	自定义消息代码	(582)
B.6	控管规则文件相关代码	(582)
B.7	错误代码	(583)

B.8	控制代码	(584)
B.9	访问权限控制代码	(585)
B.10	其他控管规则的相关代码	(585)
附录 C	Xfilter 结构类型	(587)
C.1	Internet 结构类型	(587)
C.1.1	XUSER_INFO	(587)
C.1.2	XNET_COMMAND_HEADER	(588)
C.2	控管规则结构类型	(589)
C.2.1	XACL_HEADER	(589)
C.2.2	XACL	(591)
C.2.3	XACL_IP	(591)
C.2.4	XACL_TIME	(592)
C.2.5	XACL_FILE	(592)
C.3	封包结构类型	(593)
C.3.1	SESSION	(593)
C.3.2	QUERY_SESSION	(594)
C.4	控制结构类型	(594)
C.4.1	XFILTER_IO_CONTROL	(594)
C.5	日志文件结构类型	(595)
C.5.1	LOG_HEADER	(595)
C.5.2	LOG_FIND	(595)
附录 D	Xfilter 全局变量	(597)
D.1	Xfilter.dll 使用的全局变量列表	(597)
D.2	Xfilter.exe 使用的全局变量列表	(598)

第 一 部 分

Windows 网络封包的截获技术