基于代理的分布式入侵检测系统中网络代理的相关技术研究*

Network Agent Techniques in Agent-Based on Distributed Intrusion Detection System

刘辉兰,李陶深,葛志辉

Liu Huilan, Li Taoshen, Ge Zhihui

(广西大学计算机与电子信息学院,广西南宁 530004)

(School of Comp. and Elec. Info., Guangxi Univ., Nanning, Guangxi, 530004, China)

摘要:介绍一个基于代理的分布式入侵检测系统的模型框架及其网络代理的结构设计,研究在Windows的环境下,利用网络代理技术的入侵检测方法,讨论网络代理的通信、网络数据采集与解析、协议分析等模块的相关实现技术。

关键词:入侵检测系统 分布式 网络代理 代理

中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2005)04-0232-04

Abstract: The framework model of an agent-based on distributed intrusion detection system and the architecture design of its network agent are introduced. The intrusion detection method through network agent techniques is analyzed. The relevant techniques about the communication between network agents, network data collection and analysis model, protocol analysis model are discussed.

Key words: intrusion detection system, distributed, network agent, agent

随着互联网的迅速扩张和电子商务的兴起,计算机网络的安全问题成为人们关注的热点。入侵检测系统作为一种主动的安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵,可以为电子商务等网络应用提供可靠服务。本文介绍基于代理的分布式入侵检测系统和网络代理结构设计,研究和探讨网络代理、数据采集、协议分析等模块的实现技术。

1 基于代理的分布式入侵检测系统

1.1 基于代理的分布式入侵检测系统

文献[1]在通用入侵检测框架CIDF模型[2,3]的基础上,提出了一个基于代理的分布式入侵检测系统(Agent Based Distributed Intrusion Detection System,简称ADIDS)的模型框架,该模型结合基于网络和基于主机的入侵检测方法,使用代理技术在分布式环境下对入侵进行检测。ADIDS系统有六个部分组成:(1)中央控制台。它是整个入侵检测系统和用户交互的界面,负责接收各个代理发送的报警信息,并在入侵与日志数据库中进行记录,同时还负责协调代理之间的协作;(2)基于主机代理。其检测目标是主机系统和系统本地用户,通常安装在受保护的主机上,实时检测被保护主机的安全;(3)基于网络代理。它主要用于实时监控网络关键路径的信息,保护整个网段的安全;(4)入侵响应代理。它是对入侵行为做出反应的措施,如记录入侵行为数据以作为日后法庭上的证据,给控制中心发送告警消息,对攻击进行追踪和诱导及反击,甚至可以切断本次连接的方式来实现系统的安全;(5)入侵与日志数据库。其作用是用来存贮网络数据引擎模块捕获的原始数据、分析模块产生的分析结果和入侵响应模块操作日志等;(6)规则知识库。它用来存放特征模式或者异常模式,提供必要的数据信息支持,例如用户历史档案,或者检测规则集等,入侵检测系统将用户的行为特征和它进行比较判断,看是否有入侵行为。

1.2 网络代理的结构设计

ADIDS中基于网络代理结构如图1所示,主要

收稿日期:2005-06-24

作者简介:刘辉兰(1982-),男,本科生。

*广西科技攻关项目(桂科攻0385001)和广西留学回国人员科学基金项目(桂科回0342001)联合资助。

由数据采集模块、协议分析模块、检测引擎模块以及网络代理总控制台、规则知识库、入侵与日志数据库等组成。检测方法有误用检测和异常检测两种方法。数据采集模块从网络上捕获数据包，然后将捕获的数据包按照 TCP/IP 协议的不同层次将数据包进行解析，存入相应的数据结构。协议分析模块利用网络协议高度有效化的特点来快速检测攻击，可保证高速的包捕获率和低的丢包率。检测引擎模块运用误用检测、和异常检测方法进行入侵检测。控制中心负责协调各模块之间的协作，用户可以通过中央控制台配置系统中的规则知识库，也可以通过控制中心对入侵与日志数据库中的数据进行统计分析，以更合理的方式来配置整个系统。当检测到攻击行为的时候，则产生报警信息。

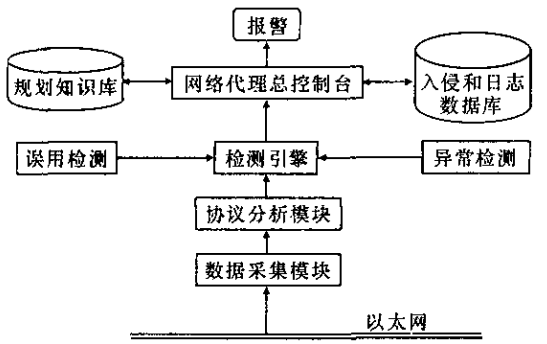

图1 网络代理结构

2 相关实现技术研究

2.1 网络代理的实现

基于 Agent 的入侵检测系统中，科学合理地构造 Agent 是首要问题。为了提高系统的入侵检测能力，网络 Agent 必须协同主机代理共同进行监视及处理。然而，要实现这种协作，必须解决基于 Agent 的入侵检测系统的通信问题，系统的通信包括控制台与 Agent、Agent 与 Agent 的通信。对于控制台与 Agent 之间的通信，主要涉及以下内容。

(1)Agent 向控制台注册。当 Agent 程序在运行主机上初次被安装时，Agent 必须向控制台进行注册，将本 Agent 所在机器的 IP 地址、网络掩码等信息提供给控制台。

(2)控制台轮询 Agent。控制台为保证了解 Agent 的工作状态，每隔一定的时间便向各个 Agent 发出询问信息，检查 Agent 是否处于工作状态。当 Agent 接受到控制中心的询问信息后，立即向控制台发出应答信息。

(3)控制中心对各个 Agent 进行配置。为了使 Agent 能根据要求进行工作，管理员必须对代理进行有效的配置，使每一个 Agent 都能根据网络系统的要求及时高效地完成自己的任务。

(4)入侵信息传输过程。当 Agent 检测到入侵时，必须及时将入侵信息以报文的形式发送到管理控制台。

(5)发送其他报文。为了使 Agent 和控制台能很好的通信，还必须有一种控制报文对两者进行协调。使用控制报文，控制台可以对 Agent 的状态进行控制。

至于 Agent 之间的通信，由于在 ADIDS 系统中只有一个控制中心，如果控制台由于某种原因瘫痪或者失效，那么整个系统将处于瘫痪状态，这是非常严重的。因此，为了使系统在没有控制台的状态下能够工作，各个 Agent 必须能够在异常情况下担负起控制中心的任务。也就是说，每一个 Agent 都带有一个控制中心模块，该模块在控制台正常工作时关闭。当 Agent 检测到控制台异常时，Agent 之间进行确认，当确认控制台失效时，则按照已设计的方法，将其中某一个 Agent 自动升级为控制台，担负起管理系统的任务。因此，Agent 之间的通信过程也是很重要的。

ADIDS 系统中，Agent 是一种可以用各种语言编写的实体。只要它提供与外部统一的接口，各种 Agent 就可以协同工作。各 Agent 的继承关系如图 2 所示，其中主机代理类、网络代理类和响应代理类都是由一个代理基类继承下来的，并扩展了相应的功能[4]。因为 JAVA 语言的无关性和移动 Agent 的移动性正好符合，并使得 Agent 的实际应用成为可能，我们采用 JAVA 作为代理的开发平台。

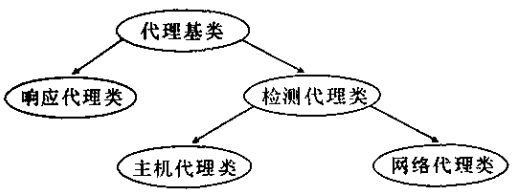

图2 各代理的继承关系

2.2 数据采集模块的实现

数据采集模块从网络上捕获数据包，然后将捕获的数据包按照 TCP/IP 协议的不同层次将数据包进行解析并存入相应的数据结构。在现有的计算机系统网卡中，一般有普通和混杂两种工作模式[5]。普通模式受数据包由的 MAC 地址决定，数据被发送到目的主机；混杂模式中所有可以被检测到的信息均被主机接收，而不管实际上数据的目的地址是不是本机。网络代理的数据采集的过程如图 3 所示。

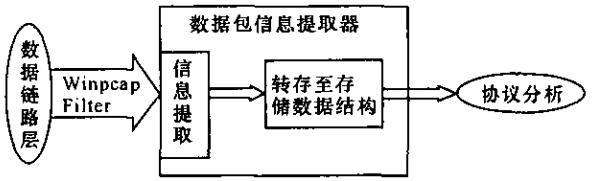

图3 数据采集流程

进行网络数据采集时，首先将网络接口设置为混杂模式，将到达网络上传输的数据包全部截取下来，供协议分析模块使用。由于效率的需要，有时要根据设置来过滤网络上的一些数据包，如特定协议的数据包。网络监听模块的过滤功能是该网络监听的关键，因为对于网络上的每一数据包都会使用该模块过滤，判断是否符合过滤条件，为提高效率，数据包过滤应该在系统内核中实现。

我们主要利用WinPcap开发包中Packet.dll和Wpcap.dll提供的API函数来实现网络数据采集模块，该开发包内置的内核层实现的过滤机制和许多接口函数不但能够提高监听部分的效率，也降低了开发的难度。WinPcap是一个与平台无关、采用分组捕获机制的分组捕获函数库，可用于访问数据链路层。这个库为不同的平台提供了一致的编程接口。在WinPcap的平台上，以WinPcap为接口的程序可以自由地跨平台使用。

程序的运行过程大致是：首先得到网络适配器的设备句柄，根据设备句柄打开网卡并将其置为混杂接收模式，这样网卡就可以收到任何在网络中传输的数据包；在接收数据包之前，还应该开辟一个用户缓冲区用来存放接收到的原始数据包，并将其初始化为数据包结构体；接收数据包时，由于需要监听网络中传输的所有数据包，可不设置对数据包的过滤参数；接收到数据包后，可根据网络协议中定义的各种类型数据包的格式对数据包进行拆分或重组；停止接收过程后，首先释放接收缓冲区，再将网卡恢复为正常接收状态，释放网卡设备句柄。

监听程序接收到的数据包都是原始数据包，它们的格式一般是以以太网数据帧的头部作为开始部分，接着是ARP或IP数据包的头部，IP数据包头部的后面是TCP或UDP、ICMP的头部，最后才是真正要传输的数据。因此，在拆分IP数据包时，先提取以太网数据帧的头部，再取IP数据包的头部，然后分析TCP或UDP、ICMP数据包的头部。最后，从数据包中取出需要的数据。数据获取过程如图4所示。

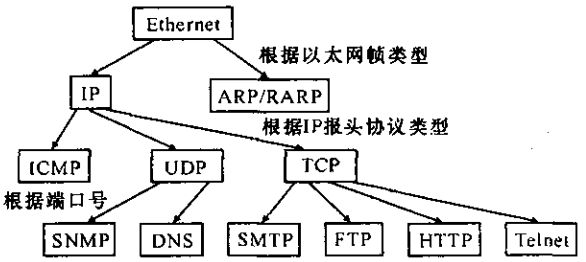

图4 数据包分层获取过程

2.3 协议分析模块的实现

用于协议分析的技术很多，最常用的是协议分析检测技术。该技术根据协议规范分析网络数据包，确认数据包的协议类型，以便使用相应的命令解析程序来检测数据包，这种方法利用了网络协议高度有效化的特点来快速检测攻击，有效地利用了网络协议的层次性和相关协议的知识。

根据以太网帧结构的定义，在以太帧的第13字节处包含了2个字节的第三层协议标识，0800为IP协议，0806为ARP协议。在IP数据包的格式定义中，第10个字节为第四层协议标识，如：TCP为06，UDP为11，ICMP为01等。而TCP数据包的第3、第74个字节为应用层协议标识（端口号）。如80为HTTP协议，21为FTP协议，23为TELNET协议等。对以太网帧的检测步骤如下：

步骤1：分析它的上层协议是IP协议、ARP协议还是RARP协议。TCP/IP协议规定一个以太网的数据包在第13字节处包含标识第三层协议的两字节。协议分析器直接到13字节处读2字节的协议标示符，如果读出的值是0800，则表示其上层协议为IP协议，应交于IP协议处理部分处理；若值为0806，则交于ARP协议处理部分处理；若为8035，则交于RARP协议处理部分处理。

步骤2：在15字节处读4bit的IP协议版本字段信息，如为04，则IP为IPv4；如为06，则IP为IPv6。IPv4协议规定IP报头的协议字段是传输层的协议标识，该位在第24字节处，协议分析器直接到第24字节处读第四层协议标示符的一个字节。IPv6协议的下一协议头部字段标识传输层协议的类型，该位在21字节处，协议分析器直接到第21字节处读第四层协议标示符的一个字节。如果这个值是01，则IP包的数据域所携带的协议为ICMP；若为06，那么，IP包的数据域所携带的协议传输控制协议为TCP；若为17，则表示这个数据包是UDP协议的数据包。在确定是TCP数据报、UDP数据报、ICMP数据报还是IGMP数据报后，就可以调用相应的协议处理部

分进行分析处理。

步骤3:TCP协议规定在第35字节处包含一对两字节的应用层协议标示符(端口号)。跳到35bit处,读一对端口号。如果两个端口号中的一个是0080,那么TCP消息的数据域携带的协议是HTTP。同样可以对UDP数据包、ICMP数据包加以分析。

步骤4:协议规则规定HTTP位于TCP之上,URL开始于第55bit处。协议分析器55bit处读统一资源定位器(URL),这个URL字符串将被输入到HTTP命令解析器,并在它被允许通过网络服务器之前分析攻击行为。

步骤5:将获得的此特征值与特征库内容比较,如与特征吻合,则访问被判断为攻击行为,产生报警,并采取相应措施。

步骤3和步骤4是对IPv4而言,如是IPv6则需把跳转的位置加上20字节。可以看出,协议分析的分析过程就是一条从根到某个节点或叶子的路径,而每个叶子、节点是某一种攻击类型的分析机。在分析机中,再采用模式匹配的算法来检测攻击,因此大大减少了计算量,提高了算法的效率。

本文在协议分析模块中利用网络协议高度有效化的特点来快速检测攻击,极大地减少所需的计算量,可保证高速的包捕获率和低的丢包率,即便在高负载的网络上也可以完全探测出各种攻击,并对其进行更详细的分析也不会丢包。

3 结束语

本文介绍了网络代理的结构设计,以及网络代理、数据采集模块、协议分析模块的实现技术。该模型框架具有良好的集成性、适应性、扩展性和协调性,可改善单点失效,保证较高的检测效率,适应于大规模、分布式系统的要求。今后我们将进一步完善系统的功能,投入实际应用后对系统的实用性和有效性作进一步的论证。

参考文献:

[1] 葛志辉. 基于代理的分布式入侵检测系统的设计与实现[D]. 南宁:广西大学,2004.

[2] Huang Mingyuh, Robert J Jasper, Thomas M Wicks. A large scale distributed intrusion detection framework based on attack strategy analysis [J]. Computer Networks, 1999, 31(23-24): 2465-2475.

[3] 连一峰,戴英侠,胡 艳,等. 分布式入侵检测模型研究[J]. 计算机研究与发展,2003,40(8):1195-1202.

[4] 赵 萍,殷肖川,王 峰. 入侵检测系统中多代理技术的应用[J]. 计算机应用,2001,21(12):42-46.

[5] 蔡立斌,高兴锁,梅苏文. 基于NIDS入侵检测模型的研究和探讨[J]. 网络纵横,2003,2:36-39.

(责任编辑:黎贞崇)