侍伟敏 （焦作工学院计算机系 454000）

A Study on Composite Intrusion Detection System

混合式入侵检测系统的研究

摘要：本文介绍了基于网络的和基于主机的入侵检测系统各自的特点，分析了这两种入侵检测系统存在的问题，给出了一种混合式入侵检测系统的解决方案，并对混合式入侵检测系统的组成及其功能进行了详细的分析研究，最后对本系统的特点作了简单的总结。

关键词：网络安全　入侵检测系统　混合式

1 引言

随着网络技术的发展，特别是Internet的深入发展，网络本身的安全性问题也就显得更为重要。目前的网络安全措施主要是采用防火墙，然而，随着黑客攻击技术的发展，系统的已知的漏洞越来越多，防火墙的局限性使其对很多攻击无能为力，尤其是对来自内部的攻击，更是束手无策。因此，把入侵检测(IDS)系统作为防火墙以后的第二道安全防线，通过动态检测与跟踪技术，对入侵攻击行为进行实时检测、动态分析与告警无疑对网络安全具有特别重要的意义。

入侵检测系统按功能可以分为基于主机的入侵检测系统和网络入侵检测系统两大类。基于主机的入侵检测系统通过对系统日志、审计记录进行分析来检测入侵行为，重点放在对文件操作、进程状态改变、用户行为等系统事件的分析与处理上；网络入侵检测系统通过将截取的网络数据包的包头或负载内容与已知的网络攻击特征进行匹配，从而实时地检测出入侵行为。这两种入侵检测系统都有它们各自的特点，基于主机的入侵检测系统主要监视系统的活动，能精确地报告入侵行为的结果，与具体的操作系统相关，而与主机的物理位置无关。网络入侵检测系统针对网络数据包的某些属性，如IP地址、端口号、SYN标志等进行分析匹配，必要时在TCP层或IP层对数据包进行还原，与具体的操作系统无关，一般情况下，一个网络入侵检测系统能够对整个子网上的网络数据包进行实时的检测，而且入侵的记录不会被入侵者删除。例如，基于主机的入侵检测系统能够检测出系统核心文件的更改或覆盖，以及特洛依木马的安装、运行，而这对网络入侵检测系统来说是很困难的。但是对于网络扫描、拒绝服务（DOS）等基本的网络入侵手段，主机系统无能为力了。无论是基于主机的还是基于网络的入侵检测系统都有其不足，只有将两者有机的结合在一起，才能发挥各自的特点，弥补各自的不足，这就是混合式入侵检测系统所要解决的问题。

2 系统模型

2.1 系统总体结构

整个系统主要有三大部分组成，分别为网络检测系统、主机代理检测系统、应急中心。其系统的总体结构如图1所示：

其整个系统的实现过程如下：网络检测系统不断的扫描主机的端口，一旦发现有数据包发送给主机，就立即捕获，然后对这些数据包进行规则化处理后，再与攻击事件特征库相匹配，如发现有相同的事件描述，即时的通告应急中心。同时，主机实时的监视特权进程的系统调用序列和日志的信息，收集一些审计的事件发送给主机代理检测系统。当主机代理检测系统被设置为正常状态下时，通过把这些正常的审计事件与正常库相匹配，来不断的更新正常库。当系统为监控状态时，同样的把这些被视为异常的

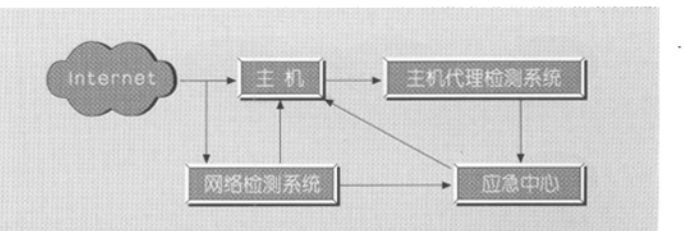

图1 系统的总体结构

事件与正常库相匹配，如发现有偏离正常库的，则立即通知应急中心。应急中心对分别来自网络检测系统和主机代理检测系统的异常信息进行综合管理，并分析这些信息，采取相应的安全措施。

2.2 系统组件

2.2.1 网络检测系统

从体系结构上，网络检测系统分为六个部分，即网络捕捉器、网络协议解码器、规则解释器、事件检测器、数据包存储器和攻击特征库。此体系结构的各个组成部分相对独立，自成体系。任何一部分的改动与扩充都不影响整体结构。其结构如图2所示：

各模块的功能说明如下：

(1) 网络捕捉器。不断的扫描主机端口，并且获取发往主机的数据包，为入侵检测系统提供从物理网络（网络接口卡）直接收集数据链路层网络

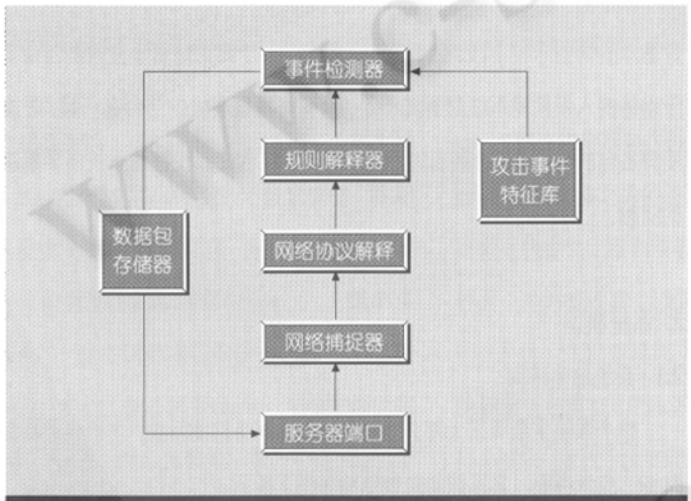

图2 网络入侵检测系统

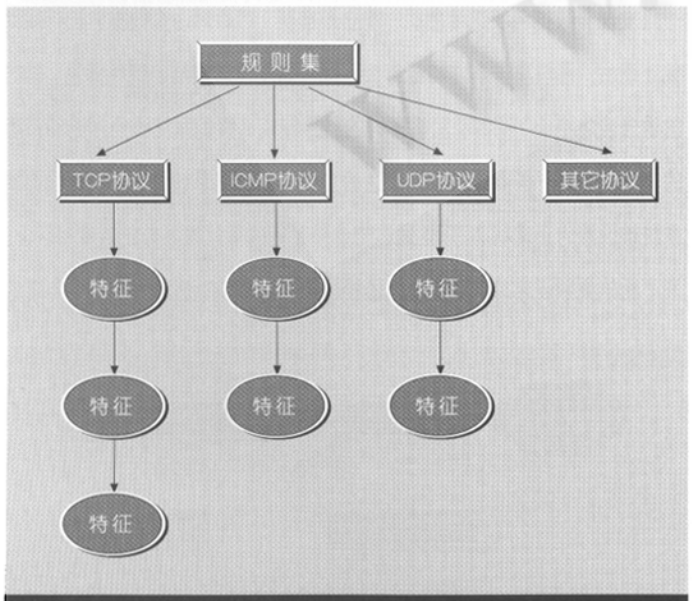

图3 特征链表的结构

原始信息的能力，网络捕捉器根据实现的机制，可以对收集到的数据包进行初处理，根据报文的类型（如源或目标端口，TCP报文的标志位信息），报文的长度等决定是否将该报文传递给网络协议解码器，进行规则化处理。这样使网络协议解码器免于处理大量无用报文，提高了整个系统的效率。概括说来，网络捕捉器的主要功能有两个：一个是获取发送给主机的网络数据包；二是对数据进行有针对性的过滤。

(2) 网络协议解码器。该部分的功能相当于一个网络协议分析仪，用于把“网络捕捉器”获得的原始网络信息，根据不同的网络协议进行解码并分别存储于不同的协议链表中。通过对常见攻击手段的分析，我们发现绝大多数的攻击集中于IP协议之上的TCP、ICMP、UDP协议，其中以TCP协议为最多。因此，特征链表着重对以上三种协议进行详细的描述，特征链表的结构如下：

(3) 规则解释器。首先从规则库中读取规则，然后将“网络协议解码器”分组后的信息依据规则转换为二维链表的形式。这一功能的实现主要依赖于规则库文件所描述的规则进行转化。

(4) 特征库。是用来存储已攻击事件的模式，这些事件的存储方式与规则库中规定的方式相同。

(5) 事件检测器。它是实现网络检测系统的核心部件。其功能主要有两个：其一：事件检测器首先从攻击事件特征库中读取对每种攻击事件的特征描述，然后接受“规则解释器”对数据进行规则化处理后的事件。对待检测的事件与攻击特征库中事件进行匹配，一旦发现相应的攻击手段，根据“攻击事件特征库”文件中相应攻击手段描述语句中所指定的响应种类做出相应的反应。

其二：根据响应的种类，如果是正常的事件（即数据包）发送给数据存储器，否则丢弃数据包。

(6) 数据包的存储器，接受经过事件检测器检测后的数据包，并且不断的发往服务器。

2.2.2 主机

主要是为服务器代理检测系统提供被检测的事件，服务器的系统结构主要有两大部分，一个是审计事件的收集器，另一个是控制器。其结构如图4所示：

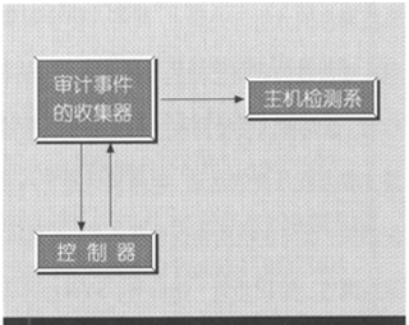

图4 主机的系统结构

这两部分的功能如下：

(1) 审计事件的收集器：是用来负责实时地收集与系统安全有关的审计事件，在定义审计事件的时候对一些关键的系统调用进行了扩充在它的参数中，除了包含有它自身的参数外，还增加了用户的一些信息，比如，用户登录系统的时间，用户名，成功与否等信息。此外，还为一些特权命令和关键的程序建立了相应的审计事件。

(2) 控制器：依据系统时钟来控制服务器代理检测系统是处于正常状态还是监控状态。

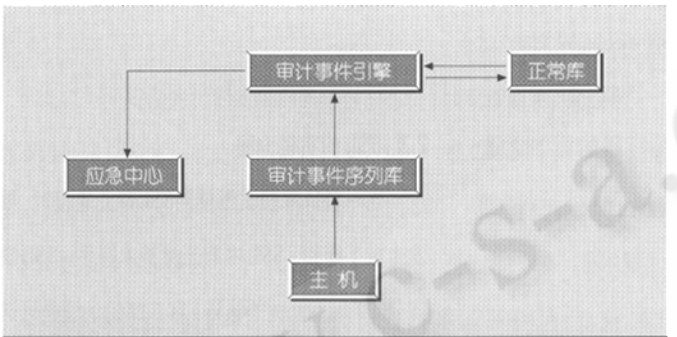

图5 服务器代理检测系统

2.2.3 主机代理检测系统

对于整个系统来说，主机代理检测系统是最重要的部分，其实质它是主机的一个代理机构。

主要是为减轻主机的负担，避免主机系统的性能降低。整个系统主要有三部分组成，分别为：审计事件序列库、审计事件引擎和正常库。其中审计事件引擎和正常库是本系统的核心部分。系统结构如图5所示：

系统的实现过程

审计事件序列首先接受来自主机的所有审计事件序列，并保存这些事件序列。然后审计事件引擎每次读取一个审计事件序列时，都要判断一下来自主机中的控制器所发送的控制信息是要求本系统处于正常状态还是监控状态。如果设置为正常态，审计事件引擎将审计事件序列库中的事件序列与正常库中的事件序列相匹配，发现有不同的事件序列时，则把此事件序列追加到正常库中，以此来不断的更新正常库。另外，如果系统被设置为监控状态时，同样，审计事件引擎也需要将审计事件序列库中的事件序列与正常库中的事件序列相匹配，当发现与正常库中有不同的事件时，则立即通知应急中心，并采取相应的安全措施。

各部件的功能如下：

(1) 审计事件序列库：主要是用来存储来自服务器的审计事件序列，并对审计事件引擎提供审计的数据。

(2) 审计事件引擎：它是本系统最核心的部件，主要有两个作用：

其一：当系统处于正常状态下，通过对审计序列的事件与正常库中的事件进行匹配，来不断的更新正常库。另外，当系统处于监控状态下，通过对待审计事件与正常库中的事件相匹配，来实时的检测系统的异常的事件。

其二：如果发现有异常事件，及时的通告应急中心。

(3) 正常库：建立系统正常库的过程就是对系统正常状态的一个学习过程，就是在系统正常状态下对特权程序进行监控，以收集正常状态下的审计事件序列，而正常库就是存储这些审计事件序列的单元。

2.2.4 应急中心

对分别来自网络检测系统和服务器代理检测系统的异常信息进行综合管理，通过分析这些信息，采用相应的安全措施。比如丢弃数据包，隔离子网，对主机进行报警等。

3 结束语

随着网络安全问题的日益突出，IDS在网络安全系统中所起的作用愈来愈重要，而且日趋复杂的网络结构对入侵检测系统的可扩展性、可管理性、适应性提出了新的要求，本论文提出了基于服务器一个混合式的入侵，即把基于主机的和基于网络的入侵检测有机的结合起来，为了减轻因服务器上检测负荷过重，造成服务器的效率降低，而采用了代理机制。此外，在实现待审计事件与正常库进行模式匹配时，新增加了索引库，从而提高了匹配的效率，而且正常库和特征库都可以智能的升级，论文中所设计的这种混合式的入侵检测系统是一种实时的入侵检测，即发现异常现象，能及时的报警，采用相应的措施来保护服务器不受攻击。

参考文献

1 王飞、李信满、赵宏，分布式入侵检测系统的设计与实现，中国计算机学会信息保密专业委员会学术会议2000。

2 李斌，基于网络的入侵检测系统[硕士论文]，北京理工大学，2001。

3 郭巍、吴承荣、金晓耿、张世永，入侵检测方法概述，信息安全国际会议论文，1999.10 Vol.25。

4 吴承荣、廖键、张世永，网络安全审计系统的设计和实现，信息安全国际会议论文，1999.10 Vol.25。