基于层次模型的分布式入侵检测系统的研究与实现

Research and Implementation of Distributed Intrusion Detection System Based on the Hierarchy Model

梁　根　(茂名学院 信息与网络中心 广东 茂名 525000)

摘　要：讨论了防火墙和传统集中式入侵检测系统的不足,提出一种层次型分布式入侵检测系统的模型和逻辑结构,并基于 Snort 软件实现了该系统,通过实验证明,该分布式入侵检测系统有较好的性能和安全性。

关键字：入侵检测系统 分布式 层次模型 Snort

1 引言

大多数企业、单位与政府部门都在组建和发展自己的网络,为了保证网络资源的安全,一般采用防火墙作为安全保障体系的第一道防线,通过访问控制,防御黑客攻击,提供静态防护[1]。但是随着越来越多的系统本身漏洞以及应用系统的漏洞被发现,以及攻击者的入侵方式更加隐蔽,新的攻击方式层出不穷,所以单纯的依靠防火墙已经无法完全防御不断变化的入侵攻击的发生。

传统的防火墙主要有以下的不足:防火墙作为访问控制设备,无法检测或拦截嵌入到普通流量中的恶意攻击代码,比如针对 WEB 服务的注入攻击等;防火墙无法发现内部网络中的攻击行为。由于防火墙具有以上一些缺陷,所以部署了防火墙的安全保障体系还有进一步完善的需要[2]。

入侵检测系统(Intrusion Detection system,简称为IDS),是指对入侵行为的发现。它通过在计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行分析,从而判断网络或系统中是否有违反安全策略的行为和存在被攻击的迹象[3]。入侵检测被认为是继防火墙之后的第二道安全闸门,它对系统的运行状态进行监视,发现各种攻击征兆、攻击行为或者攻击结果,以保证系统资源的机密性、完整性和可用性。入侵检测的主要功能是:监控网络和系统、发现入侵事实、异常现象甚至是入侵企图、征兆,从而进行实时报警和主动响应等任务。入侵检测技术是动态安全技术的最核心技术之一。

2 相关研究

2.1 集中式入侵检测系统存在的缺陷

集中式的入侵检测系统具有的缺点主要有[4]:检测速度跟不上网络速度的发展、攻击特征库更新不及时、检测方法简单单一、不同入侵检测系统之间不能互操作、不能和其他网络安全产品互操作、结构不合理、系统可伸缩性差、难于向系统中添加新的功能或对系统重新进行配置等问题。所以它只适合结构简单的小型网络,当其面对规模较大、异构的网络环境以及应对分布式协同攻击时显得力不从心,一是因为中央控制分析器的工作负荷过大,并且由于网络传输的延迟,探测器传输给中央处理器的网络数据不及时;二是因为异构网络平台也给分析系统带来了处理上的极大困难。

2.2 分布式入侵检测的优缺点

综上所述,现有的传统入侵检测系统,即通过在网络中放置多个探测器,以收集网络数据,然后把这些数据送到一个中央控制分析器进行分析处理的技术,存在诸多问题,已经不适应攻击技术的分布化、协作化趋势,更不能满足结构互异、规模庞大、高带宽网络的安全需求,迫切需求有效的基于分布式的入侵检测系统[5]。

分布式入侵检测系统不同于集中式入侵检测系统,它具有以下几个方面的优势:攻击模式库更新快;

检测精度高；检测效率高；检测更大范围的攻击行为；能进行协同响应。

现有的分布式系统虽然在检测性能上已经远远超过了集中式的入侵检测系统，但是还不完善，主要存在以下几个方面的问题：监视器存在单点失效；复杂的多层结构存在时延；不易配置或配置复杂；商业产品价格高昂。

3 基于层次型的分布式入侵检测系统

3.1 基于 Snort 的入侵检测系统

Snort 能够进行协议分析，内容的搜索、匹配。现在 Snort 能够分析的协议有 IP、TCP、UDP 和 ICMP。将来的版本，将提供对 ARP、ICRP、GRE、OSPF、RIP、ERIP、IPX、APPLEX 等协议的支持。它能够检测多种方式的攻击和探测，例如：缓冲区溢出，CGI 攻击，SMB 检测，探测操作系统质问特征的企图等等。

Snort 还有很强的系统防护能力。如：利用其 IPtables、IPFilter 插件可以使入侵检测主机与防火墙联动，通过 FlexResP 可使其有 IPs 功能，snort 能够命令防火墙主动短开恶意连接。

Snort 支持插件，可以使用具有特定功能的报告，检测子系统插件对其功能进行扩展。Snort 当前支持的插件包括：数据库日志输出插件，破碎数据包检测插件，断口扫描检测插件，HTTP URI 插件，XML 网页生成等插件。

Snort 有四种运行模式[6]：数据包嗅探（Sniffer）数据包嗅探仅仅是从网络上读取数据包并连续不断地显示在终端上；数据包记录（packet logger）数据包记录是把数据包记录到硬盘上；网络入侵检测（NIDS Network Intrusion Detection System）网络入侵检测是最复杂的，而且是可配置的。网络入侵预测（Inline，即 Intrusion Prevention System（IPS））而网络入侵防预是通过 Iptables 库获取包，根据 snort 规则利用新的规则类型配合防火墙进行网络防预的。

3.2 分布式入侵检测系统的模块结构

分布式入侵检测系统的模块结构主要由 4 个重要的子系统构成[7]：

（1）数据包捕获和解码子系统；

该子系统数据包捕获和解码子系统该子系统的功能是为捕获网络的传输数据并按照 TCP/IP 协议的不同层次将数据包进行解析。

（2）检测引擎；

检测引擎是分布式入侵检测系统的核心。为了能够快速准确地进行检测，我们将检测规则利用链表的形式进行组织，分为两部分：规则头和规则选项。前者是所有规则共有的包括 IP 地址、端口号等，后者根据不同规则包括相应的字段关键字。

检测引擎采用模块化设计结构，具有很好的可扩展性[8]。引擎包含的功能模块有包捕获模块、虚拟机模块、攻击特征库、过滤器模块、智能分析模块、记录器模块、报警模块、磁盘管理模块等。

（3）日志/报警子系统；

日志子系统允许你将包解码收集到的信息以可读的格式或以 tcpdump 格式记录下来。报警子系统使其将报警信息发送到 syslog、用户指定的文件、Unix 套接字或数据库中。

（4）预处理器。

分布式入侵检测系统预处理器是介于解码器与检测引擎之间的可插入模块，作用是对当前截获的数据包进行预先处理，以便后续处理模块对数据包的处理操作。

3.3 层次型入侵检测系统的逻辑结构

分布式入侵检测系统中，分析节点分为三个（或更多）抽象层次[9]，低层分析结点完成对原始数据的预处理、过滤和提炼工作，并将初步的分析结果提交给上层分析结点。上层结点综合分析来自于低层分析节点上报的结果，做出上层判断或将本层的分析结果再上报它的上层分析节点，如图 1 所示。

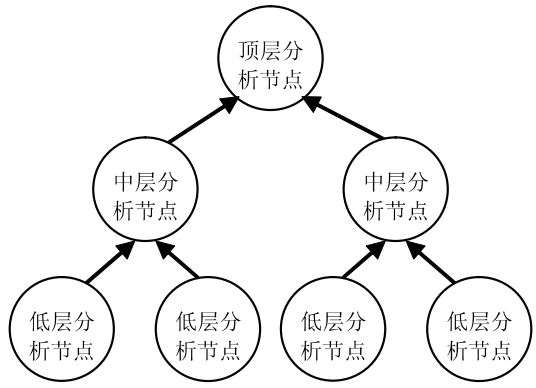

图 1　层次化的分布式入侵检测系统

表 1　测试入侵事件类型

攻击大类	攻击子类	攻击描述及示例
拒绝服务攻击	与 ICMP 有关的攻击	利用 ICMP 包的 DoS 攻击，如 ping flood，ping of death 攻击等
	Win IGMP 攻击	利用 IGMP 协议的攻击，如 IGMP，Asking 攻击等
	SYN flooding	SYN 洪水式攻击，如 synflooder，melnuke 等
	UDP flooding	利用 UDP 包的洪水式攻击，如 mstream，trinoo 等
预攻击探测	端口扫描	如各种基本的扫描方法
	扫描—ICMP	利用 ICMP 包进行的扫描，如 L3retriever ping 以及 webtrends 扫描器的扫描。
	扫描探测—TCP	利用 TCP 包进行的扫描，如 christmas 扫描，空扫描等
	FTP 口令猜测	FTP 口令猜测，如 ftpcrack
可疑活动	包含病毒的邮件（POP3，Part1）	取回携带病毒的邮件，如 triplesix 蠕虫，newapt 蠕虫等
	利用 WEB 服务进行的可疑活动	利用 http 服务漏洞实现 ping of death，如 cxjnuke2，3 等
未授权的尝试访问	利用 HTTP 服务的弱点	利用 IIS Unicode 漏洞的各种攻击，如 unicode 等
	缓存溢出	各种缓存溢出攻击，如针对 X86 linux imapd4，imapd5 等的攻击
	WEB—IIS 存取企图	利用或针对 IIS 服务器的攻击，如_vti_inf，carbo. dll 等
	Backdoor	各种后门的检测，如 netbus，backorifice 等

从图中看出，两个模型色差范围分布形态基本一致，但是查找表模型中色块的色差的色差值较 系统主要由多个分布在网络中关键结点上的分析节点构成[10]，每个分析节点可以独立地工作，当拓扑结构中的分析节点的数量小于等于一时，通信模块和控制模块就处于休眠状态，而每个分析结点此时可以单独运行。每个分析结点的主要部件由 Snort 网络检测引擎模块、通信模块、过滤器模块和控制器模块四部分组成。每个分析结点构成一种对等的分布式检测系统。每个分析结点的逻辑结构如图 2 所示。

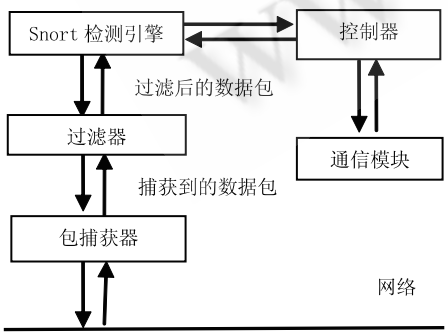

图 2　分析结点逻辑结构

Snort 网络入侵检测引擎是整个系统中的核心部件，它主要被部署在受保护网络内不同的网段上。基于 Snort 的分布式入侵检测系统可以部署在负载较轻的主机上，亦可部署在单独配置的机器上。

通信模块与 Snort 检测引擎部署在同一位置，它的主要作用是在分布式系统中与其他检测分析节点进行信息交换和通信。

为了减轻检测引擎的检测负荷，并保证在高流量的网络中基于 Snort 的分布式入侵检测系统尽量做到不漏报和误报，我们对已被 Snort 捕获并经过协议解析的数据包，进行过滤处理，抛弃无需检测分析的大量数据包，这样就能直接提高系统的检测效率。

控制器模块是每个主机与外部交流的界面。控制器模块的主要工作主要有以下两部分：控制 Snort 检测引擎、通信模块和过滤器模块启动或终止工作；控制 Snort 检测引擎、通信模块和过滤器模块处于何种工作模式。

基于 Snort 的分布式入侵检测系统能适应大规模的高速的网络环境，能实时检测出多种常见的入侵、攻击手段，并可借助第三方软件，以屏幕消息或电子邮件告警等方式及时报警。

4　系统实现与测试

4.1 实验环境

本实验在茂名学院校园网上对分布式入侵检测进行了大量的实验，该校园网共有约 1.5 万用户，实验所在的网络环境共有 4 个链路出口，分别为中国电信 400M，中国网通 200M，中国联通 100M，教育网 100M，核心交换设备为 AVAYA P882 和 Cisco Catalyst 6509。本文的测试环境由十一台主机组成，四台作为攻击端主机，安装攻击工具软件，另外七台主机作为检测主机，OS 为 Redhat Enterprise Linux Advanced Server 4。

4.2 测试方案

我们把网络入侵事件划分为以下 4 大类：拒绝服务攻击，预攻击探测，可疑活动，非授权访问尝试，每一大类又分为若干子类，具体如表 1，然后分别进行测试。

测试时我们对以下指标进行了记录，主要包括：

1. 漏报率：系统在检测时出现漏报的概率。漏报：系统未能识别出入侵行为，将其作为正常行为放过。

2. 误报率：系统在检测时出现误报的概率。误报包括将正常行为判断为攻击而产生报警；将一种攻击错误的判断为另一种攻击而报警。

3. 事件库：也叫特征库。系统能够匹配检测的攻击种类数量的大小，能够横向体现系统检测能力。

4. 延迟时间：从攻击发生到系统检测到攻击的时间。延迟时间的长短直接关系到攻击破坏的程度。

5. 资源占用：系统工作时对资源的消耗情况。

6. 自身安全性：又称健壮性。系统对直接以自身为攻击目标的攻击的抵抗能力。

4.3 实验结果与分析

其他测试条件不变的情况下，负载低于 50% 时，漏报率都低于 4%；当系统负载增大到 70% 时，漏报率增至 21%；当系统负载陡增至 90% 时，漏报率就已经大于 70%，结果如图 3 所示。

实验结果显示，负载加大，包长不变的情况下，嗅探网卡抓包数也在加大，同时系统需要处理的包数也在增大；从现象中能够看到，系统在负载达到 80% 后性能降低厉害，可能是系统资源被占用过多引起；查看系统的 CPU 占用情况和内存使用情况，发现负载达到 60% 后，内存占用率急剧升高，在负载超过 90% 时，系统处于不响应状态。

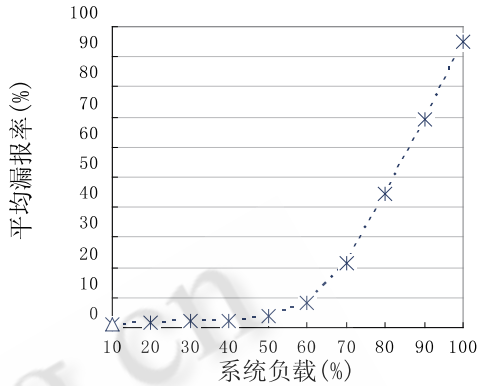

图 3　系统负载与漏报率比较图

5　结论

分布式 IDS 解决了许多传统 IDS 未能解决的问题，如减轻网络负载、灵活性、可扩展性等。本文在针对防火墙和集中式 IDS 的不足的基础上提出了一种层次化的分布式 IDS 的模型和逻辑结构，简单介绍了 Snort 的基本功能，并基于 Snort 软件实现了该分布式 IDS，通过实验证明，该分布式 IDS 有较好的性能和安全性。

参考文献

1　Steve Suehring. Linux 防火墙. 何泾沙译. 3 版. 北京：机械工业出版社，2006，1：39 – 62.

2　Philip H. Integrated security and network management remain elusive. Network Security，2004，10(6)：15 – 16.

3　王军，熊伟，肖德宝. 基于 SNMP 的入侵检测系统的设计与实现. 计算机工程与应用，2003，39(17)：177 – 180.

4　李昀，李伟华. 分布式入侵检测系统的研究与实现. 计算机工程与应用，2003，39(4)：1 – 3，8.

5　连一峰，戴英侠，胡艳，许一凡. 分布式入侵检测模型研究. 计算机研究与发展，2003，40(8)：23 – 24.

6　潘玲，黄云森，张凡. 一种基于 Snort 的入侵防御系统. 计算机系统应用，2005，14(6)：29 – 31.

7　康松林，费洪晓，施荣华. 网络应用软件监控系统监控模块的设计与实现. 中南大学学报：自然科学版，2004，35(6)：993 – 997.

8　唐谦，张大方. 基于 Snort 的入侵检测引擎比较分析. 计算机工程与设计，2005，26(11)：2884 – 2886.

9　董晓梅，于戈. 分布式入侵检测与响应协作模型研究. 计算机工程，2006，32(6)：151 – 153.

10　陈传波，周晓军. 一种基于移动代理的分布式 IDS 模型的研究. 计算机工程与科学，2006，32(6)：231 – 235.