一种分布式入侵检测系统的实现

韩仲祥[1]，史浩山[1]，杜华桦[2]
(1.西北工业大学 电子信息学院，陕西 西安 710072;2.空军工程大学 电讯工程学院，陕西 西安 710077)

摘　要：由于TCP/IP协议是一个开放的协议，因此网络极易受到攻击。为了能够有效地检测到入侵行为，提出了一种基于部件的分布式入侵检测系统，并结合网管软件系统的开发，在Linux环境下进行了实现。系统主要由控制台、分析系统、存储系统、响应系统、网络引擎和主机代理构成。通过协同工作并采用改进了的Boyer－Moore算法，检测网络入侵行为，有效地维护了信息网络的安全。

关键词：入侵检测；网络引擎；网络安全
中图分类号：TN915　　**文献标识码**：A　　**文章编号**：1009－3516(2004)05－0085－04

随着Internet的迅猛发展，网络信息系统的安全问题变得越来越严峻，防火墙技术通常是被人们所采用的第一道防线，但防火墙能力有限，只能过滤外来部分非法的数据包，对内部网络的非法操作等无能为力。而入侵检测系统(Intrusion Detect System，IDS)是继防火墙之后的第二道防线，与防火墙配合使用能有效地提高网络的安全等级。

根据定义[1]，入侵检测识别任何一组企图破坏系统的完整性、秘密和资源的访问权限。但笔者认为，IDS在检测入侵活动时，应尽量减少对计算机和网络系统的影响，对入侵活动最好是实时检测，从而保证合法用户的合法权利。

通常，入侵检测系统应具有监视分析用户和系统的行为、审计系统配置和漏洞、评估敏感系统和数据的完整性、识别攻击行为、对异常行为进行统计、跟踪和识别违反安全法规的行为等功能，目的是使系统管理员可以较有效地监视、审计自己的系统。入侵检测通常分为两大类[2]：

1)异常检测(Anomaly Detection)：检测使用系统的异常行为和对资源的异常使用，并对异常活动进行标识。

2)滥用检测(Misuse Detection)：对已有的入侵行为进行标识，定义成一系列的确定模式，将检测到的入侵行为与之匹配，从而实现入侵检测的目的。

入侵检测系统的核心功能是分析各种事件，从中发现违反安全策略的行为，通常一个好的入侵检测系统应满足实时性、可扩展性、适应性、安全性、可用性、有效性等几方面的要求。本文结合教育训练网网络管理软件系统，开发出了一种分布式入侵检测系统(DIDS)。

1　体系结构

1.1　系统模块

如图1所示，安全系统的主要部件包括网络引擎(Network Engine)、主机代理(Host Agent)、存储系统(Storage System)、分析系统(analyzer)、响应系统(Response System)、控制台(Manager Console)。

网络引擎和主机代理部件的作用是从整个计算环境中获得要分析的数据。前者截获网络中的原始数据

收稿日期：2004－05－10
基金项目：国家高技术发展计划(863)基金资助项目(2002A143020)
作者简介：韩仲祥(1971－)，男，山东莒南人，博士生，主要从事计算机网络安全、网络管理技术研究；
史浩山(1946－)，男，陕西西安人，教授，博士生导师，主要从事数据通信与计算机网络技术研究.

包,并从其中寻找可能的入侵信息或其它敏感信息。后者通过所在主机收集各种信息,包括分析日志、监视用户行为、分析系统调用、分析该主机的网络通信等。两个部件具有一定的数据分析功能,采用模式匹配的方法来检测已知的一些简单攻击。

存储系统是用来存贮捕获的原始数据、分析结果等重要的数据。储存的原始数据对发现入侵者进行法律制裁时提供确凿证据。存储系统也是不同部件之间数据处理的共享数据库,为系统不同部件提供各自感兴趣的数据。存储系统采用 MySQL 数据库,提供灵活的数据维护、处理和查询服务。

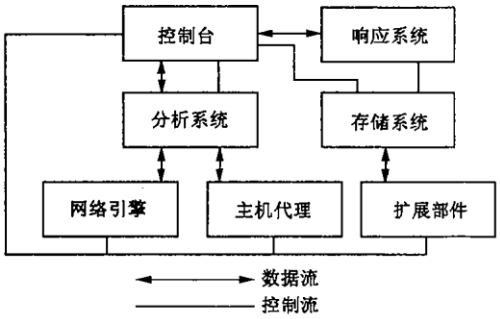

图 1 分布式入侵检测系统结构

分析系统的作用是对捕获的原始信息、其它部件提供的可疑信息进行统一分析和处理。一般采用统计方式、主要面向高层次的分析,同时负责对分布式攻击进行检测。分析系统是安全系统的核心。

响应系统是对确认的入侵行为采取相应措施的子系统。响应包括消极的措施,如给管理员发电子邮件、消息、传呼等;也可以采取保护性措施,如切断入侵者的 TCP 连接、修改路由器的访问控制策略等;根据需要甚至可以采取主动的反击策略,对攻击者进行如 DoS 攻击。

控制台是安全系统和用户交互的界面,该界面集成于网络管理与安全子系统中。用户可以提供控制台配置系统中的各个部件,也通过控制台了解各部件的运行情况。

1.2 系统部署

在安全系统中采用了 2 级分析结构,即防火墙内外都设有检测器(如图 2 所示)。

在图 2 中,入侵检测器 *A* 放置在防火墙外,属于第一级分析结构,强调实时检测能力。检测器 *A* 可以捕获所有与 Internet 交换的数据流,因此可以检测站点和防火墙暴露在多少种攻击之下。

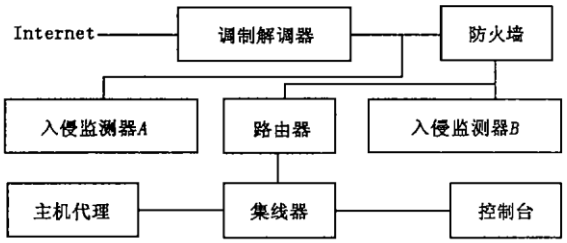

图 2 系统部署

入侵检测器 *B* 放在防火墙内部,属于第二级分析结构,深入分析数据的潜在威胁。同时,设置良好的防火墙能够阻止绝大部分简单攻击,这样检测器 *B* 不用将大部分注意力分散在这类攻击上。

通过对检测器 *A* 和检测器 *B* 采集的数据进行对比,安全系统可以很明显地获得有关渗透过防火墙的攻击信息,检测来自网络内部和外部的攻击,并检测出由于设置有问题而无法通过防火墙的内部系统。同时分级的分析结构能够使得多种分析方法同时存在于系统之中,充分发挥各种检测方法的优点。

另外,安全系统支持多于 2 个的检测器,这样可以根据需要对具体的网段进行保护。

2 网络引擎的设计与实现

网络引擎通过对网络上传输数据包的分析,得到可能入侵的信息。它不单是一个产生和传输数据的工具,同时也具有一定的分析能力。在功能上接近于一个完整的基于网络的入侵检测系统。

2.1 网络引擎的设计

网络引擎可分为以下几部分:数据包截获、协议分析、数据分析、引擎管理和安全通信(如图 3 所示)。

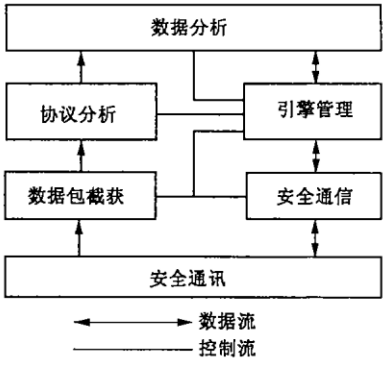

图 3 网络引擎结构

数据包截获:数据包截获模块将网络接口设置为混杂模式,将接收到网络上传输的数据包截取下来,供协议分析模块使用。

为提高效率,数据包过滤应该在系统内核里来实现。安全系统采用了 Linux 的 LIPCAP 来实现这模块,开发包中内置的内核层实现的 BDF 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。

协议分析的作用是辨别数据包的协议类型,以便使用相应的数据分析程序来检测数据包。可以把所有的协议构成1棵协议树,1个特定的协议是该树结构中的1个结点,可以用1棵2叉树来表示。1个网络数据包的分析就是1条从根到某个叶子的路径。在程序中动态地维护和配置此树结构即可实现灵活的协议分析功能。

在该树结构中可以加入自定义的协议结点,如在HTTP协议中可以把请求URL列入该树中作为1个结点,再将URL中不同的方法作为子节点,这样可以细化分析数据,提高检测效率。

数据分析模块的作用是分析某一特定协议的数据,得出是否关注该主机的结论。一个数据分析函数一般可以检查一种协议的1种入侵方式,这样可以方便的进行配置。数据分析函数不仅仅由数据包触发,也可以是系统定义的某1个事件来触发。如时间、特定的数据包到来、管理员启动、某种数据分析的结果、网络上其它入侵检测系统发送来数据等都可以触发数据分析函数。

数据分析的方法是入侵检测系统的核心,主要使用了快速的模式匹配算法,所有的攻击方法被表示为模式信号存放在入侵特征数据库中,当前的数据如果和数据库中某种特征匹配,就指出入侵行为的类型。

安全通信部分负责网络引擎中各部分间和引擎与其它系统部件间通信的信息安全。

代理管理部分负责网络引擎中各部分的协调和配置。

2.2　网络引擎实现

安全系统中的网络引擎是在Linux平台上使用php和gcc编程实现的。系统使用模式匹配方法对网络数据包进行实时检测。

网络引擎的关键部分是数据分析模块。该模块中涉及到2个问题:首先是如何描述入侵行为,其次是使用什么算法来快速检测入侵行为的存在。

在实现中,我们使用了与Snort兼容的检测规则来描述入侵行为,使用Boyer - Moore匹配算法来检测。

1)检测规则

在安全系统中,采用了Snort的入侵行为描述方法。Snort是一个开放源代码的轻量级基于网络的入侵检测系统。这种描述方法简单、易于实现,能够描述绝大多数的入侵行为。由于其简单,虽然Snort中包含的规则非常多,但检测速度仍然比较快。

每条规则分为规则头部和规则选项2部分。规则头部包含规则的操作、协议、源IP地址和目标IP地址及其网络掩码和端口。规则选项包括报警信息及需要检测模式信息。

2)匹配算法的改进

匹配算法是检测引擎的关键,它直接影响系统的实时性能。在网络数据包搜索入侵特征时,需要1个有效的字符串搜索算法。

字符串搜索算法中,最著名的是KMP算法(Knuth - Morris - Pratt)和BM算法(Boyer - Moore)。2个算法在最坏情况下均具有线性的搜索时间。但是在实用上,KMP算法并不比最简单的c库函数strstr()快多少,而BM算法则往往比KMP算法要快。但是BM算法也有需要改进的地方[8],例如要在"substring searching algorithm"中搜索"search",刚开始时,把子串"search"中的"s"与"substring"中"s"对齐。

第一次匹配结果是在第二个字符处发现不匹配时,要把子串往后移动。但是该移动多少呢?最简单的做法是移动一个字符位置。KMP是利用已经匹配部分的信息来移动;BM算法是做反向比较,并根据已经匹配的部分来确定移动量。Boyer - Moore - Horspool算法根据被比较串对齐的最后一个字符("r")来决定位移量的多少。

我们的方法是根据紧跟在当前子串之后的那个字符(上图中的"i")获得位移量。

显然,由于上一次匹配的失败,移动是必然的,因此,设移动步数为N,则$N \geq 1$。但N的最大值是多少了?如果这个字符在模式串中,显然应该根据模式串的位置来决定。如果它在模式串中就没有出现,显然连它自己也不用比较量,因此可以移动到该字符的下一个字符开始比较。

以上面的例子,子串"search"中并不存在"i",则说明可以直接跳过一大片,从"i"之后的那个字符开始作下一步的比较,如下:

```
substring searching algorithm
        search^
```

比较的结果,第一个字符又不匹配,再看子串后面的那个字符,是"r",它在子串中出现在倒数第三位,

于是把子串向前移动 3 位,使 2 个"r"对齐,如下:

substring searching algorithm

search

整个过程,我们只移动了两次子串就找到了匹配位置,可以看出,用这个算法,每一步的移动量都比 BMH 算法要大,所以肯定比 BM 算法更快。我们用类封装实现了这一算法。

3 总结

网络管理与安全在不断完善中,在大量的检测中发现安全系统中的 IDS 能够满足分布式环境下对入侵检测的要求,具有较好的可扩展性和准确性,由于使用与 Snort 兼容的入侵描述方法,使得模式库的更新更加快捷、及时,使用协议分析和模式匹配相结合的检测方法提高了检测的效率和准确性。

参考文献:

[1] Tidwell T, Larson R, Fitch K, et at. Modeling Internet Attacks[A]. Proceedings of The 2001 IEEE Workshop on Information Assurance and Security[C]. 2001. 54 - 59.

[2] Guy Gary Helmer. Intelligent Muiti - Angent System for Intrusion Detection and Countermeasures [D]. PhD thesis, Iowa State University, 2000.

[3] Denning A. An intrusion Detection Mmodel[J]. IEEE Transaction on Software Engineering, 1987, 13(2): 222 - 232.

[4] 朱 杰. 入侵检测中的快速过滤算法[J]. 计算机工程, 2003, 29(16): 109 - 110.

[5] 范西昆, 郑连清, 樊昌周, 等. 一种基于移动代理的入侵检测系统[J]. 空军工程大学学报(自然科学版), 2001, 2(6): 78 - 81.

(编辑:门向生)

The Implementation of a Distributed Intrusion Detection System

HAN Zhong - xiang[1], SHI Hao - shan[1], DU Hua - hua[2]

(1. Electronic Information College, Northwestern Polytechnical University, Xi'an, Shaanxi 710072, China; 2. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: Because of the open structure of TCP / IP, the network is vulnerable to attack. In order to availably detect the intrusion, an intrusion detection system based on components is presented, and the implementation of it in Linux environment is made in combination with the development of NMS software. The system consists of manager console, analyzer, storage system, response system, network engine and host agent. By operating cooperatively and using the improved Boyer - Moore algorithm, the network intruding acts can be detected effectively and the information network security is defended.

Key words: intrusion detection; network engine; network security