第7卷第4期　　空 军 工 程 大 学 学 报(自然科学版)　　Vol.7 No.4
2006年8月　　JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION)　　Aug.2006

基于 MIB II 的 IDS 实现研究

韩仲祥[1,2]，　史浩山[1]，　庄绪春[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:讨论了 IDS 和网络安全管理的状况,给出了 ID 和 NM 相结合的异常入侵检测模型,即分布式和分等级的 ID 技术和 NMS 共存,充分利用 NMS 中 MIB II 的信息,提出的分等级相关结构可以提高检测的准确率,识别协同入侵,尤其对 DDoS 这样的宏泛攻击很有效,这种技术在 IDS 和 NMS 的整合环境中可以发挥重要作用。

关键词:IDS;NMS;MIB II;DDoS
中图分类号: TN915　　**文献标识码**:A　　**文章编号**:1009-3516(2006)04-0055-05

当前 IDS 一个变化就是攻击策略和攻击工具的复杂化,攻击试图躲避检测,如 DDoS 等多阶段的攻击,是最困难检测的攻击,也是威胁性最大的攻击。这些攻击分布操作而又协调一致最终达到目的。当前 IDS 系统在多区域中缺乏对安全事件的关联性分析,因此不能有效地检测到此类攻击,全局性的入侵检测就显得非常有意义,并且也是非常重要的研究课题[1-3]。

在网络管理系统中,用于分析的数据来源主要是 MIB(管理信息库),但是仅仅依靠 MIB 的信息用于入侵检测是不够的。例如 IP 数据包头部的链接信息用于检测某些攻击是很重要的,当然,仅用 MIB 数据来分析攻击是不完善的[4]。现在人们在网络中加载 IDS 和 NMS 时它们是独立的,本文研究的目的就是如何将 ID 和 NM 在审计数据、分析技术、系统结构和配置策略等方面整合在一起,并建立异常入侵检测的模型。

1　系统结构

现在的网络环境,由于网络拓扑变得越来越复杂、攻击手段越来越多样,对 IDS 来说仅仅监视和分析网络中一个点的数据,想提高效率是很困难的。由于 IDS 是被动的监视而不象防火墙那样主动过滤,IDS 越有效越好,在高速和大流量的网络中,黑客通过过载 IDS 一段时间而导致 IDS 延时很容易入侵。

一个较好的网络入侵检测处理策略就是在网络中放置多个轻量级的代理—ID 代理,试验表明一个 IDS 无法准确而及时地发现网络中所有的入侵,特别是在高速网络中。多个 ID 代理中每一个代理检测特定层次的入侵,在我们的框架结构中如基于主机的 ID 代理能够分析 BSM 审计数据、系统追踪及用户命令信息流,以此来监视主机上的应用和用户行为。对于网络 ID 代理,它们主要负责检测针对网络协议薄弱环节的攻击如 DDoS 攻击。ID 代理的数量和配置策略取决于企业安全规划。例如可以在特定服务器上安装基于主机的 ID 代理来保护黑客的侵入,基于网络的 ID 代理可以配置在路由器或者交换机上来检测通过这些设备的网络信息流。

另外还采用了分布式配置,如图 1 所示,系统保护级分为本地分析,区域分析和全局分析。

配置在本地的 ID 代理用来检测网络设备和服务器的入侵行为,它们的工作范围通常是一个子网(如某一个部门的网络),每一个 ID 相关器管理几个本地 ID 代理,它将本地 ID 代理传送来的安全事件或者警告信息综合起来,相关处理本区域的入侵警告。ID 相关器管理覆盖范围内的所有安全行为并负责向 ID 管理器

收稿日期:2005-10-20
基金项目:教育部博士点基金资助项目(20050699037)
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研究.

报告情况。ID 管理器主要负责整个网络如校园网的入侵检测,它接收来自多个区域的 ID 相关器的信息作全局的入侵分析,完整而复杂的攻击分析就是由 ID 管理器来完成的。ID 管理器发出最后的入侵检测报告给网络管理员—全网的管理者,以供决策。

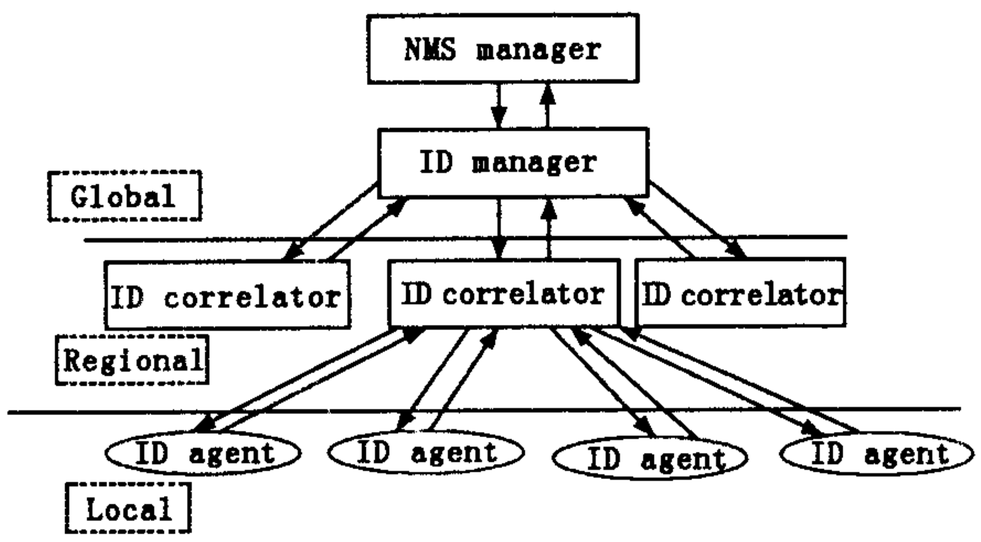

图 1 分级 ID 结构图

1.1 ID 代理

如前所述,一个 ID 代理主要负责某一特定类型的入侵,图 2 表明了一个 ID 代理的组成部分。

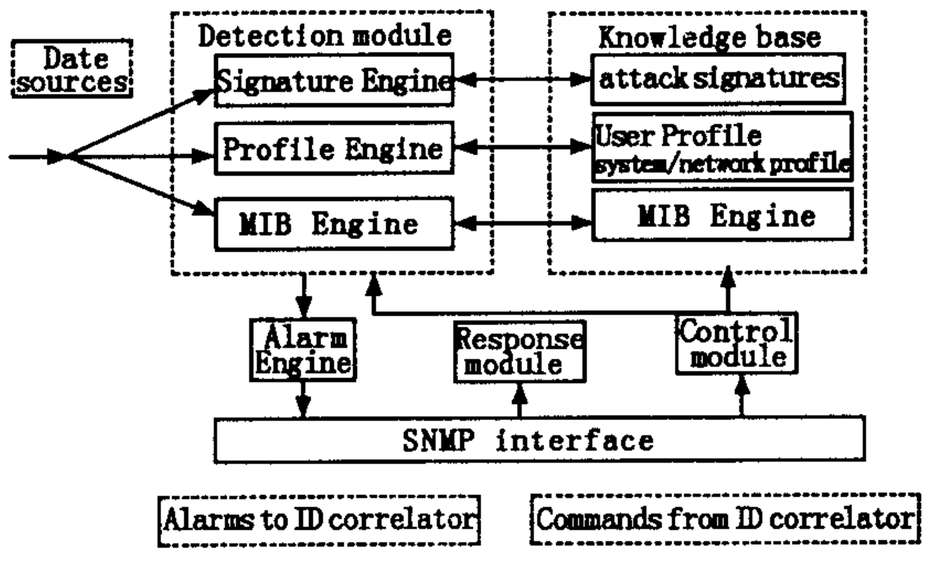

图 2 ID 代理组成图

该模型主要包括:

1)检测模型:它主要分析接收到的数据包、BSM 记录及 MIB 数值等,同时还要与检测模型或者正常轮廓匹配。检测模型有 3 个引擎:特征引擎、轮廓引擎和 MIB 引擎。特征引擎通过入侵特征集中检测已知类型的入侵,轮廓引擎主要负责网络或用户基于正常轮廓的异常检测,这两个引擎利用如 BSM 或者传统的 ID 数据源。MIB 引擎检查 MIB 对象的值并与常规的 MIB 轮廓比较以检测入侵。不同的 ID 代理根据他们检测角色的不同可以是 3 种检测引擎的一种引擎或者是一种检测引擎的部分,例如一个 ID 代理可以是特征引擎,以便快速而有效地检测已知的入侵。3 种引擎的结合可以大大提高 ID 代理的效率。通过控制模块中的模块,ID 相关器可以改进轮廓和攻击特征。

2)知识库:它存储攻击特征、用于检测的用户或者系统的轮廓和 MIB 轮廓,同时也存储规则设置和攻击模型。知识库包含各领域知识和分析工具的分析结果。

3)响应模块:它采取各种响应动作,例如拒绝某一可疑源的连接请求。响应动作的实施是根据 ID 相关器传送过来的入侵命令而定。

4)控制模块:控制模块根据 ID 相关器送来的控制信息调整知识库和相关引擎。例如当网络拓扑结构发生变化时,新拓扑结构信息通过 ID 相关器发送到控制模块以更新知识库。检测引擎的攻击特征和规则设置也会相应地更新。

5)告警引擎:它向 ID 相关器发送警报。

6)SNMP 界面:它是 ID 代理和 ID 相关器的通信平台。ID 代理传来的警报信息和 ID 相关器传来的控制信息将被封装成 SNMP 包。这样做的优势是整个系统就是 NMS,警报信息就成为 MIB 的对象。

1.2 ID 相关器

ID 相关器是结构中重要的组成部分(如图 3 所示)。ID 相关器的主要职责是:①相关处理 ID 代理传送来的警报信息以识别入侵的特征,预测入侵种类阻止可能发生的入侵;②传送告警信息给 ID 管理器以便作进一步的入侵分析;③采取适当的动作响应入侵,如关闭某些网络设施,给 ID 代理发送响应命令等。ID 相关器中主要有警报搜集和安全相关引擎两大模块。警报搜集接收 ID 代理送来的告警事件;安全相关引擎将 ID 代理传送来的告警信息与相关模型匹配,解释其相关性,并预测入侵的目的。它除了向 ID 管理器发送告警信息外,还能根据入侵状况产生行为代码并送往 ID 代理。

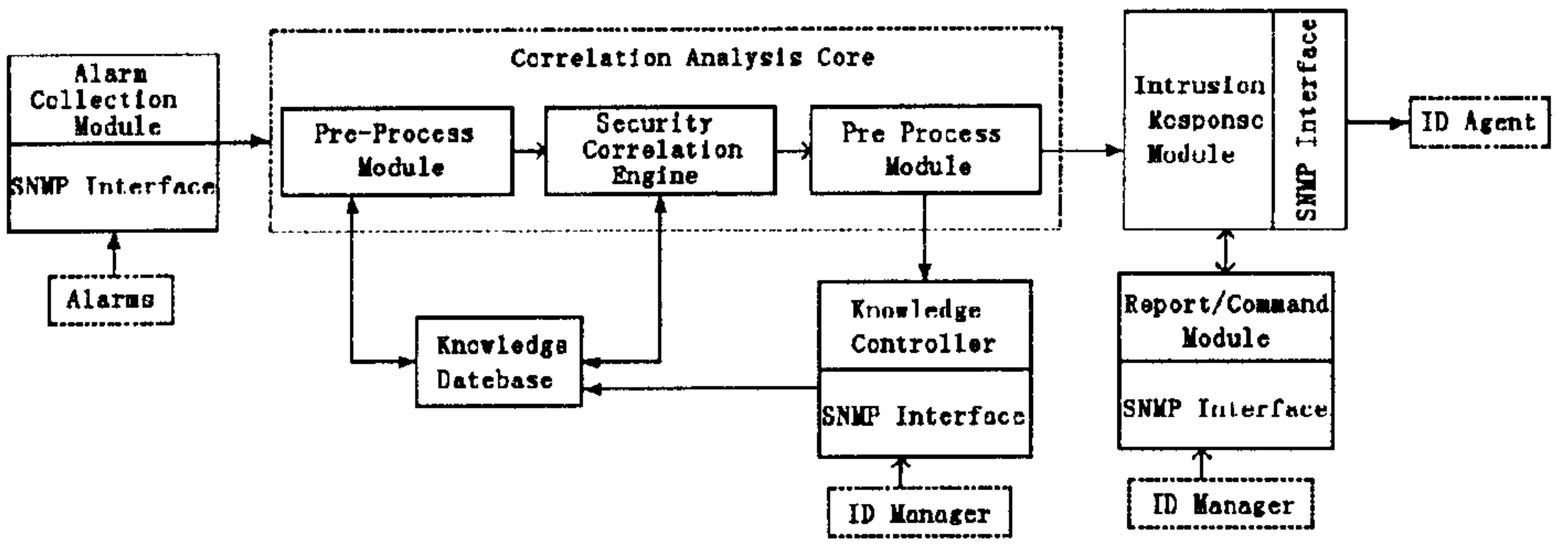

图 3 ID 相关器组成图

如图4所示,安全相关引擎由以下几个重要部分组成。

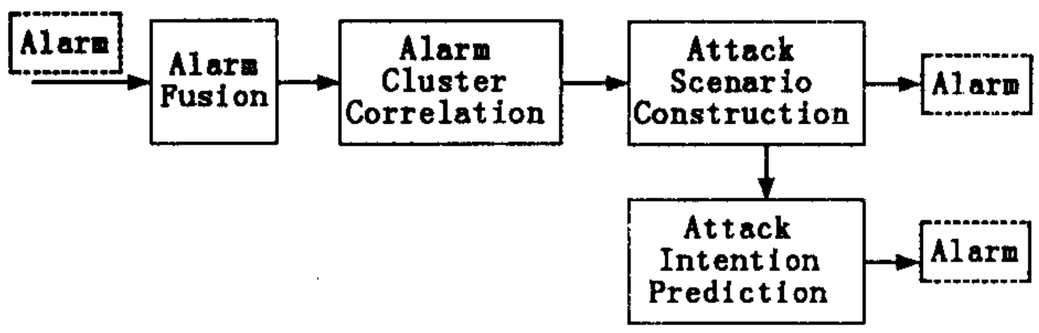

图4　安全相关引擎组成图

1)报融合:搜集并融合不同 ID 代理送来的警报信息,对同一入侵产生大量警报,并按照警报串进行分类。

2)报串相关器:在不同类别中比较警报信息,充分显示入侵的特性,这样对攻击检测描绘的更准确、详细。同时为将来的攻击分析提供信息。

3)攻击模拟装置:在已有相关输出的前提下构造攻击过程。一个攻击过程就是一系列相关的攻击步骤。攻击模拟装置的目的就是推想发生了什么和即将发生什么。

4)攻击目的预测:分清攻击目的并预测下一步即将发生什么,对多步骤的入侵分析,给出可以采取的行动。

5)知识库:存储诸如网络拓扑、网络部件等网络知识,相关引擎所用的相关技术也会被存放在其中,例如,如果相关引擎利用基于规则的推理方法,规则设置就会存放到知识库中。与入侵相关的知识如入侵细节、入侵特征也要存放到知识库中。另外,还存放安全策略及入侵响应,入侵响应由 ID 管理器更新。

6)入侵响应模块:按照 ID 相关器覆盖区域的安全策略给 ID 代理发送入侵响应命令,如果对入侵没有可利用的响应知识,ID 相关器就将信息传递给 ID 管理器,ID 管理器就把响应加到知识库中以备将来之用。

7)知识控制器:构造、管理、更新知识库。例如,当一种新的情况发生,该模块要处理并把它加到知识库中以备将来利用,ID 管理器通过该部分也可以添加更新存放在知识库中的安全策略。

1.3　分析

这种分布式分等级的系统在高速环境中可以工作得很好,因为分析工作分布在 ID 代理中。

在 ID 和 NM 的整合系统中有两级相关处理过程,在低级,需要相关处理送到 ID 代理的许多源信息并检测本地的入侵,在高级,ID 相关器和 ID 管理器分析攻击的细节并协同检测分布式攻击。基于这种全局协同检测我们可以知道下一步什么时间、在哪儿将要发生什么,及采取相应的阻止措施。这种混合一体化的结构所具有的特点是:低误报率和高检测率;入侵趋势预测和入侵确定,特别是对狡猾的协同攻击。

多渠道信息的整合是 IDS 的关键,尤其是对能够穿越多个主机、子网、区域和坚持较长时间的狡猾攻击。对于 IDS 来说,导致高误报率的一个主要因素就是缺乏足够的信息。由于不同操作系统采用的网络协议不同,IDS 监视并分析网络数据包,能够区分来许多自目的主机的信息。如果网络数据包仅仅来自一个可利用的数据源,IDS 发现可疑的数据流而实际上破坏并不大就会产生虚警。本文 IDS 结构中,ID 代理相关处理来自不同的检测引擎的警报信息,以检测异常的信息是否是真正的入侵,并向 ID 相关器递交最终的警报。这种模型可以综合处理多渠道的异常信息并最终确定一个异常情况是否是入侵是可信的。

为了提高入侵检测的效率,ID 代理中的 MIB 检测模块是必需的。例如象基于流量的 DoS 等攻击,入侵检测必需正确统计好信息流。然而目前多数的 IDS 系统是利用原始的数据包进行检测的,为了检测到异常的信息流,IDS 引擎需要对原始的数据包大量的统计计算。另外,选择并建立用于检测大范围的攻击的统计特性是不断变化的。对于异常检测,NMS 已经为我们提供了大量有用的网络信息,例如,MIB II 有许多用于描述网络信息流的信息和主机的配置信息。既然 MIB 可以在 SNMP 代理中获得有用的信息,就可以把它们用于入侵检测。

将 MIB 的信息用于入侵检测可以增强 NMS 的管理和分析网络操作的能力,特别是安全管理领域。在实用中,作为网络管理的代理和入侵检测的 ID 代理就可以合在一起,将 ID 和 NM 整合在一起使得操作方便有效,提高了使用的简单性。

在 ID 和 NM 的整合系统中,有两级搜集器,在低级搜集器中需要收集很多的源信息发到 ID 代理中,以便确定本地是否有入侵发生。高级的搜集器,ID Correlator 和 ID Manager 进一步确定是否有攻击存在。基于这种全局的相关器处理,就可以确定下一步什么时间,什么地点将会发生什么,采取措施有效防止。这种方法可以降低误报率,提高检测速度,特别适用于复杂的协同式的攻击,更是有效。

这种复杂的攻击可以穿越多个主机、子网关和域,并能持续很长的一段时间,从多个地方搜集信息是这种 IDS 检测的关键。高的误报率就是缺少有效的信息。IDS 监视并分析来自不同操作系统的网络数据包,

可以发现不同的信息,但是,如果数据包是唯一可用的信息,当发现值得怀疑的信息流就报警,就有可能造成误报。我们设计的 IDS 系统对异常的举动可以进一步判断看是否是真的入侵,并产生一个警报送往 ID Correlator,比较适用于检测异常的入侵。

为了提高入侵检测的效率,ID 代理中的 MIB 检测模型很有必要,比如象 DoS 这样的信息流攻击,检测攻击靠正确统计数据流。现在多数 IDS 系统都要利用原始的数据包去检测入侵,IDS 检测引擎需要对数据包作大量的统计工作以检测异常的入侵。这是比较有效的直接方法。另外,选择并构造统计特征以检测大范围的攻击很有意义。NMS 系统已经提供了大量的网络状态信息,这些信息有利于进行异常检测。例如 MIBII 中就有许多对象,能够反映网络和主机中的流信息和特征。既然 MIB 已经安装在 SNMP 的代理中,就可以用来进行入侵检测用。

IDS 的入侵检测信息能增强 NMS 的网络管理和分析能力,尤其在安全管理领域中。

实用中,ID 代理中的网络管理和安全管理就可以结合在一起,同时将 ID 和 NM 结合在一起,由于界面统一、操作标准而变得方便有效。

2 MIB 检测引擎

2.1 模型设计

MIB II 有 IP、ICMP 和 TCP 组,收集不同层和协议的信息。MIB II 的每一组能提供关于系统配置、网络信息流、控制和错误统计等有用信息,也就是说 MIB II 中的对象能给我们提供一个审计源,借此可以了解被管元素和网络的操作状况。

本文在基于异常 ID 模型的 MIB II 中,有 81 个监视对象,它们均和网络流、错误统计及配置信息有关,并被安排在 IP、ICMP、UDP、TCP 和 SNMP 组中。

为了能够监视整个网络状态,将这 81 个 MIB 变化参数按照所属协议层分配到 18 个子模型中,这种结构是按照 MIB II 定义对象所在协议层次进行设计的。

应用这种异常检测模型,所有子模块均被利用,一旦有异常,子模块会发送警告信息,当这一警告信息被其中的一个协议 ID 子模块选中,就可以假定该协议层中有异常。异常检测中,并不预先准备关于入侵的知识,每种协议中利用 ID 子模块,就可以很好的检测到异常入侵,甚至可以知道在哪种协议层中。

异常检测模型中利用了分级技术。利用测试对象去接近每一个 MIB 对象中的异常检测模型结构,尤其是对每一个 MIB 对象,根据该对象以前的参数值可以预测即将出现的数值。即:利用 $O_{t-n}, O_{t-(n-1)}, \cdots, O_{t-2}, O_{t-1}$ 来预测 O_t。在正常情况下,对象之间有一个可以预测的关系,当有异常入侵发生时这种关系就会被打乱,训练 ID 模型学习维持正常的关系就可以检测潜在的入侵。

2.2 试验与仿真

评测 ID 模型时,利用 DDoS(分布式拒绝攻击)进行攻击,MIB II 搜集目标数据,系统运行速率和没有入侵时的速率基本相同,实验中设置容忍极限参数 α 为 30%。表 1 为 ID 模型运行结果统计。

表 1 基于 MIB II 的 ID 模型入侵检测样值

入侵的类型	准确率(%)	误判率(%)	检测的 ID 子模型
Ping Flood	95.48	0.217	IP_In,ICMP_In,ICMP_Out
Syn Flood	96.15	0.767	IP_In,TCP_In
UDP Flood	97.95	0.412	IP_In, UDP_ In,UDP_ In_Error
TearDrop	60.78	0.327	IP_In, IP_Other

结果表明基于子模块的 ID 模型能检测到每一种入侵。同时在检测象 Ping Flood, Syn Flood, UDP Flood 等攻击有较高的准确率和相对较低的误报率,表明按照协议设置检测子模块能够实现正确的入侵检测。例如,在 Ping Flood 攻击中,攻击者发送了大量的 icmp 回应信息到目标主机,目标主机不但接收了大量的 icmp 信息,而且也发送了大量的 icmp 回应信息。我们希望子模块 ICMP In 和 ICMP Out 去检测异常行为,结果表明,这两个子模块成功地检测到了 Ping Flood 攻击。在 TearDrop 攻击中检测速率没有其它的高,原因是 ID 模型的抽样速率,通常,当网络中发生入侵时,MIB 检测数据会有一个延迟,原因是入侵响应要有一个入侵构建过程。当然相对高的抽样速率,对于 TearDrop 攻击来说,响应时间就小,检测效率就高。

试验表明,基于 MIB II 的 ID 模型能够有效的检测很多象 DDoS 这样的数据流攻击。但是由于 MIB II 对象个数有限,ID 模型现在还不能检测非数据流的攻击,象 illegal - remote - root - access 攻击,它一般不依靠大量数据流去攻击目标主机。

虽然本文的 ID 模型有一定的局限性,但优越性显而易见。首要的是这种 ID 模型能够提高入侵检测的效率。正象前面所述,MIB II 给我们提供了大量的有关网络活动的信息和统计数据,它们对异常检测非常重要,既然这些信息是由 NMS 提供,IDS 工作起来显然就更加有效。

基于 MIB II 的 ID 模型另外一个潜在的应用就是能够检测象 DDoS 这样的攻击。可以在附属主机上安装这种代理模型,以检测攻击该附属主机的异常行为。当附属主机发出警告信息,ID 模型在攻击者攻击目标主机之前将警告信息发到主机以便采取相应措施阻止攻击者。

3　结论

本文讨论了现在 IDS 和网络安全的状况。提出了 ID 和 NM 相结合的技术,即分布式和分等级的 ID 技术和 NMS 共存,提出分等级的相关结构可以提高检测的准确率,识别协同入侵。这种将 ID 和 NM 技术结合起来的构思将会改变 ID 技术并明显提高检测效率。

同时也给出了基于 MIB II 的异常检测模型,试验结果告诉表明该 ID 模型对检测象 DoS 这样的宏泛攻击很有效,同时也说明这样的 ID 模型在 IDS 和 NMS 整合中发挥着重要作用。

参考文献:

[1] 韩仲祥. 实时入侵检测的优化问题研究[J]. 计算机工程与应用 ,2004,29:38 - 42.

[2] 秦　拯. 基于神经网络的实时入侵检测模型的研究[D]. 重庆: 重庆大学,2001.

[3] Samuel Patton, William Yurcik, David Doss. An Achilles Heel in Signature - Based IDS: Squealing False Positives in SNORT [A]. Proceedings of the Fourth International Symposium on Recent Advances [C]. 2001,10 - 12.

[4] Lee W, Xiang D. Information - Theroetic Measures for Anomaly Detection[A]. Proceedings of the 2001 IEEE Symposium on Security and Privacy[C]. 2001.

[5] 韩仲祥,史浩山,杜华桦,等. 一种分布式入侵检测系统的实现研究[J]. 空军工程大学学报(自然科学版),2004,5(5): 85 - 91.

(编辑:门向生)

Implementation of IDS Based on MIB II

HAN Zhong - xiang[1,2], SHI Hao - shan[1], ZHUANG Xu - chun[2]

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

Abstract: This paper analyzes the challenges in current IDS and network security management, proposes an anomaly intrusion detection module with integrating NM by making full use of information in MIB II. The experiment results show that the model performs well in detecting some traffic - based intrusion such as DDoS. This technology can play an important role in the integration of the IDS and NMS.

Key words: IDS; NMS; MIB II; DDoS