国 防 科 技 大 学 学 报
第23卷 第5期 JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY Vol.23 No.5 2001

文章编号:1001-2486(2001)05-0098-05

分布式网络攻击检测系统(DIDS)*

张权,张森强,高峰

(国防科技大学电子科学与工程学院,湖南 长沙 410073)

摘 要:介绍了网络攻击检测系统(IDS)的运作机理,分析了IDS的优缺点。针对传统IDS的问题提出了分布式IDS(DIDS)的概念,比较了DIDS的设计目标与目前一些IDS产品的性能。最后从功能模块设计、攻击特征的获取和更新、提高攻击行为的检测和反应速度、攻击行为关联性分析和更加主动的反应策略五个方面详细阐述了DIDS的具体设计思路,为进一步完善网络攻击检测系统的性能提供了可行的解决方案。

关键词:IDS/DIDS;分布式检测分析;集中式管理维护

中图分类号:TP393.06 文献标识码:A

Distributed Intrusion Detection System (DIDS)

ZHANG Quan, ZHANG Sen-qiang, GAO Feng

(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: The principle of intrusion detection system (DIDS) is introduced, and its advantages and disadvantages are analyzed. Hence, we bring out the concept of Distributed IDS, comparing the design goal with the performance of some IDS products. In the end, the designation of DIDS is discussed in detail in regard to the aspects of the functionality module designation, the retrieve and update of attack characteristics, the enhancing of the attack detection and reactivity, the correlated attack analysis, and the more active reaction policy.

Key words: IDS/DIDS; distributed detection analysis; centralized management and maintenance

随着互联网络的普及,信息安全问题成为各界关注的焦点问题。各国政府,各相关行业和部门以及一些科研机构也愈来愈重视网络安全与网络防攻击技术。计算机网络攻击检测[1,2,3](Computer Network Intrusion Detection)是最近几年才兴起的一种网络安全增强技术,它的出现有助于网络安全专家把精力集中到那些新的真正具有较大危险性的网络攻击行为上,很大程度上改变了专家们疲于应付各种攻击行为的被动局面;同时攻击检测提供了自动检测和响应机制,使安全专家彻底摆脱了手工分析和反应的不利局面。为此,许多专家认为攻击检测是解决网络安全问题最具价值和潜力的技术之一[2]。

本文介绍了IDS的运作机理,分析了IDS的优缺点,然后针对传统IDS的问题提出了分布式IDS(Distributed Intrusion Detection System,简称DIDS)的概念,比较了DIDS的设计目标与目前一些现有IDS系统的性能;最后从功能模块设计、攻击特征的获取和更新、提高攻击行为的检测和反应速度、攻击行为关联性分析和更加主动的反应策略等几个方面阐述了DIDS的具体设计问题。

1 IDS原理

1.1 IDS工作机制

攻击检测(Intrusion Detection)是一种自动识别对于计算机和网络资源的恶意行为并采取相应的保护措施以避免系统遭到侵害或进行适当的记录,以便在遭到侵害后快速恢复系统功能的过程。图1给出了一个通用的攻击检测模型,该模型包括事件产生器、活动记录单元、规则集和检查引擎等几部分。其中,事件产生器是模型中提供系统活动信息的部分。事件来源于系统审计记录、网络通信或者防火墙等应用子系统。规则集的定义来源于专家系统,用来决定是否发生攻击事件的检查引擎。活动记录是按照系统状态机模型建立的系统运行参数集,实时改变系统的状态参数,它根据从规则集中检查出的行

* 收稿日期:2001-03-17
基金项目:国家863基金资助项目(863-307-7-5)
作者简介:张权(1974-),男,博士生。

为创建新的状态记录。活动记录和规则集的反馈表示系统的学习机制,学习规则可以采用人工智能的方法,使系统实现自学,也可以人工干预进行微调;一般两种方法联合使用。

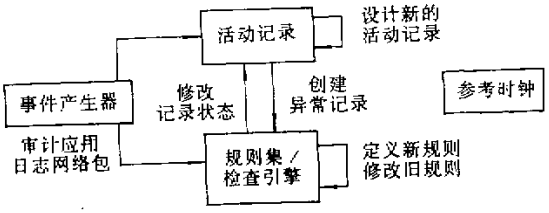

图1 通用攻击检测模型

Fig.1 General intrusion detection model

从攻击检测的定义不难看出,其功能模型包括四个方面:观测(Observe),定位(Orient),决策(Decide)和响应(Act),这四个方面构成了一个OODA环[2],环中的前一级输出成为了后一级的输入。图2为简化的IDS功能模型示意图。

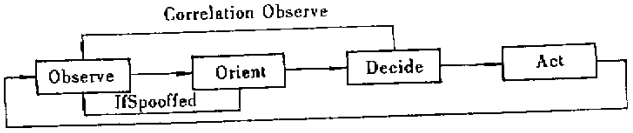

图2 IDS功能模型/OODA环

Fig.2 IDS function model/OODA loop

1.2 IDS的优点

IDS的最大优点就是减轻了网络安全管理人员的压力。通过集中的、标准化的信息搜集和过滤,实时或定期地生成网络和系统遭受攻击的报告。管理员们就可以从手工分析海量系统日志中解脱出来。同时攻击检测提供了自动检测和响应机制,使安全专家们摆脱了手工分析和反应的不利局面。

此外,IDS可以有效地弥补防火墙的缺陷,发现并阻断一些已经进入防火墙的攻击行为,同时还可以有效地发现或制止源自网络内部的攻击行为。因此IDS可以成为防火墙的一种延伸[2],与其他安全策略一起构建成一个真正实现纵深防御的网络安全系统。

1.3 传统IDS存在的问题

虽然IDS的功能日益全面,但它还并不是解决网络安全问题的"一揽子"方案,像其它所有安全产品一样,目前的IDS普遍存在一些有待克服的问题。

首先,大部分IDS系统进行攻击检测的主要依据是攻击特征[5],然而每天都有新的攻击技术和攻击方法出现;IDS检测出未知攻击方法的概率几乎为零,而目前几乎所有的IDS都缺乏有效的攻击特征快速更新策略。

其次,IDS要对大部分网段内部和进出网段的数据包进行过滤分析,当网络通信流量较大时,检测的实时性和有效性就要大打折扣。

此外,目前IDS系统的检测分析机制比较简单,基本不具备关联性分析和趋势分析能力,因此对时空跨度加大的攻击方式(如DDOS等)的检测效果不很理想。

2 DIDS对于传统IDS的改进

为了解决IDS所存在的问题,我们提出分布式IDS系统(Distributed IDS)的思想。DIDS综合了基于主机和基于网络的IDS的功能。DIDS的分布式表现在两个方面:首先数据包过滤的工作由分布在各网络设备(包括联网主机)上的探测代理完成;其次,探测代理认为可疑的数据包将根据其类型交给专

用的分析层设备处理。各探测代理不仅实现信息过滤,同时对所在系统进行监视;而分析层和管理层则可对全局的信息进行关联性分析。这样对网络信息进行分流,既可以提高检测速度,解决检测效率低的问题,又增强了DIDS本身抗击拒绝服务攻击的能力。具体而言,与IDS相比,DIDS中采取了如下的改进措施:

(1) 增加了专门的特征库检索、验证和更新引擎,用来实现攻击特征库的实时更新。

(2) 采用分布式设计,由多个独立工作相互协调的模块分担网络数据包的过滤与分析。

(3) 设计网络信息的关联性描述模型,用统计学方法分析用户的行为特征,形成用户网络行为的趋势估计,从而全面提高DIDS检测DDOS等攻击的能力。

(4) 采用一些特定的网络攻击方法,对检出的网络攻击行为实施有效的反攻,使攻击者暂时或较长时间丧失进一步攻击的能力,从而提高攻击响应的主动性。

目前,已有的IDS系统种类繁多。下表列举了目前的一些主流IDS系统的主要性能指标以及DIDS在这些方面的设计目标。

附表

项目 \ 产品	CyberCop	NetProwler	NetRanger	RealSecure	我们的DIDS
基础系统	WinNT	Win32	SUNOS	WinNT	Linux FreeBSD
信息源	系统日志	网络数据包	网络数据包	网络数据包	网络数据包、日志
处理速度	定时	1 000P/s	5 000P/s	3 000P/s	各层分担
检测方法	知识库	知识库	知识库	知识库	知识库/统计预测
响应策略	主动/被动	主动/被动	主动/被动	主动/被动	主动/被动/反攻击性
系统拓扑	集中式	分布式	分布式	分布式	多级分布式
代理数量	几十	几百	几百	几百	几千
用户设置	可以	较好	可以	可以	好
自身安全	差	较好	好	较好	较好
互操作性	差	较好	好	较好	差
可扩展性	差	差	差	较好	较好

从上表可以看出,DIDS在预测方法上加入了统计预测,可以获取更高的检测概率;多级分布式的拓扑结构和分层处理数据的机制使得它可以达到更快的处理速度,从而保证响应的快速和及时;另外,DIDS能有效地协调更多的探测代理,支持用户对规则集的修改,采取了保障通信的措施,还具有良好的可扩展性。不过,由于DIDS现在还不是标准的产品,它的互操作性较差。

3 DIDS的设计

3.1 DIDS的功能模块设计

DIDS的总体设计原则是分布式检测分析,集中式管理维护。按逻辑层次划分为管理层、分析层和检测层。其结构如图3所示。

管理层包含唯一的管理控制中心(CONSOLE),用来维护全局数据库,对分析层和检测层模块实施控制与管理,并进行网络行为的关联性分析。在企业网络中,DIDS管理中心服务器应该和内部数据库服务器等设备得到同等的保

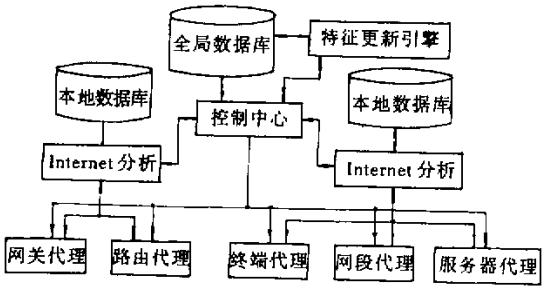

图3 DIDS逻辑模块

Fig.3 DIDS construction model

护。

分析层按网络结构分为 Internet 信息包分析模块和 Intranet 信息包分析模块,在各分析模块中按不同的通信协议划分子模块;分析层接收各下属检测层模块的输入,对确认的攻击行为按照设定的响应策略采取相应的措施;分析层拥有本地数据库,该库的维护由管理层完成。分析层与代理层是松散的附属关系,其间的关系可以由图 4 说明。

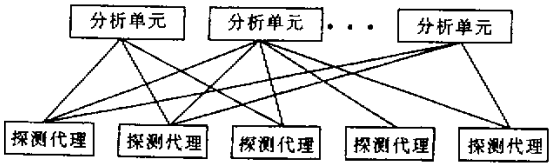

图 4 分析单元与探测代理之间的关系

Fig.4 Analyse unit and detection proxy unit

检测层实现各种类型的信息过滤和探测功能,称为探测代理,图 5 是探测代理的一个通用模型。探测代理对系统和网络中的信息进行初步检测分析,对于确认的合法通信不予干涉,而对于未知的通信和信息则递交给相应的分析层模块作进一步处理。各探测代理之间不存在直接的信息交互,相应的攻击行为将由管理中心负责实施。探测代理不仅完成网络信息的过滤分析,同时对所在系统的日志、审计文件和文件系统进行分析,以便发现系统的滥用或其它恶意行为。各探测代理有各自相应的规则库,规则库的维护由管理中心负责。

探测代理分布在网络的各个关键服务器、主机或其它网络设备上,目前设计中的代理都是以应用程序方式运行在目标系统上的,因此对目标操作系统的类型有一定的要求。

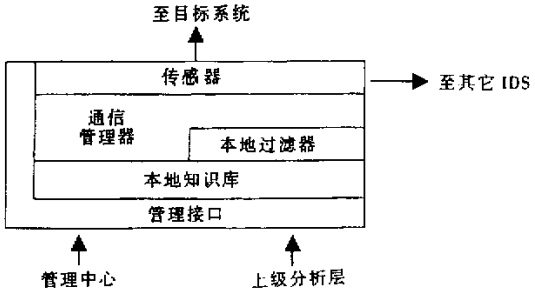

图 5 探测代理

Fig.5 Detection proxy unit

3.2 攻击特征的在线获取、测试与实时更新

攻击特征库的实时更新是 DIDS 的关键技术之一,它关系到 IDS 能否有效检测最新出现的攻击方法。更新引擎的数据来源是攻击方法库。通过检索互联网上的攻击信息网站,管理员将得到的漏洞等信息整理后输入攻击方法库。更新引擎时首先将所有攻击行为的特征信息输入特征库,然后对新产生的方法在本地网段进行模拟验证。若为有效的攻击方法,则对该漏洞进行 patch;若 patch 失败,则通知管理员,管理员通过管理中心对各分析层的本地数据库进行维护。

管理人员的维护工作包括几个方面:(1) 攻击信息的在线获取;(2) 攻击信息的分类整理和特征归纳;(3) 失效 patch 的手工补救。

目前,IDS 实现自动的特征更新还不太现实,但是在设计中可以预留自动更新的接口模块,以适应技术发展的需求。

3.3 提高攻击行为的检测与反应速度

作为一个 IDS 系统而言,对攻击行为的检测与反应速度是非常关键的指标。例如 RealSecure 可以在 0.5ms 内检测到 WINNT 的 CGI 漏洞的攻击并且做出反应。即使一个 IDS 系统可以检测到所有的网络入侵,但是如果反应速度很慢,系统已经造成了损失,这时 IDS 也就丧失了它存在的意义。

通过不同的分析模块分担数据包的分析工作是提高 DIDS 反应速度的关键,这里设计的重点是要对信息进行合理的划分。内部网络和外部网络的信息由不同的分析中心处理是最粗放的划分处理方

式,进一步地,可以针对不同的网络通信协议设计相应的分析子模块。

在检测代理部分实现初步的信息过滤和分检工作是提高速度的又一有效方法。检测代理根据其本地知识库,筛选出一些明显的合法和非法通信,其它信息再交给上层模块处理。此外,精确简练的行为特征描述也可以较大幅度地提高DIDS的反应速度。从现有IDS系统的兼容性出发,可以考虑在N-Code的基础上设计扩展宏作为特征描述语言。

3.4 攻击行为的关联性分析

目前分布式攻击逐渐成为网络攻击的主流之一,2000年Yahoo、Amason等就遭到来自全球50多个主机的DDOS攻击。分布式攻击的特点是攻击的发起者利用分布于世界各地的主机,在某时间段内在较大的空间跨度上对特定系统实施攻击;攻击的源头具有较强的隐蔽性,同时由于各单独主机对系统的行为基本不能构成有效的攻击,所以攻击的责任者也很难确定。目前几乎所有安全手段对分布式攻击都难以奏效,因此分布式攻击被称为网络安全的一个肿瘤。

克服分布式攻击的一种有效策略是利用分布式检测,并同时进行关联性分析。分布式检测一方面可以提高检测和反应速度,另一方面还有助于发现来自可疑主机的非正常行为;而关联性分析是为了发现各独立网络行为之间的相关性,从而找到攻击的证据,并且借助于趋势分析,在系统遭到最终攻击之前及早做好保护。

关联性分析的最大优势在于可以对用户网络行为进行趋势分析。通过对用户的网络行为进行统计分析以了解用户的行为偏好,当用户的网络行为突然背离其趋势预计时,系统可以采取相应的措施实施保护,如进一步检测数据包的源地址以防止用户会话被劫持、要求用户再次进行身份确认、给相应用户发送邮件以确认用户账号未被盗用等。可见,趋势分析可以非常有效地防止内部网络的恶意行为。

关联性分析研究的关键是建立恰当的统计学模型,从网络的特性出发,我们初步估计可以建立一个多元高阶的马尔科夫模型。另外,进行关联性分析的时间窗口长度也是非常重要的;若该窗口太大,则需要消耗大量的系统资源,太小则无法检测出一些"深谋远虑"的攻击行为。因此传统的矩形窗是难以满足需求的,我们认为窗口应该具有样条冲击响应曲线的有关特性,并且每个事件按不同的类型赋予多个权重系数,系数随时间的推移逐渐减小,不同事件之间的相关性由各事件的权重系数决定。

3.5 更加主动的反应策略

目前IDS的响应主要包括:记录、发email给管理员、寻呼管理员、终止会话、阻断用户等[4],这些方法虽然可以在一定程度上保护系统,但是相对攻击者而言仍然处于被动地位。如果IDS对那些确认的恶意攻击者实施有效的反攻,则可以在很大程度上遏制攻击者的入侵欲望,有助于形成一个和平的网络环境。

反攻技术研究的关键是如何使攻击模块和分析模块协调运作,此外有效攻击技术的研究也是一个关键。一般来说,可以考虑采取DOS攻击,因为攻击者所利用的带宽往往很小(常见的是Modem),DOS比较易于实现。当然,采取攻击行为必须非常谨慎,只有在获得了足够的证据时才可以实施。

4 结束语

随着信息技术的飞速发展,信息的安全日益成为全社会关注的热点。在网络安全领域,IDS的技术有着广阔的发展和应用前景。DIDS是我们提出的一种对经典IDS的改进,我们将在后续工作中将其进一步完善。

参考文献:

[1] Kossakowski, Peter, et al. *Responding to Intrusions* [A]. (CMU/SEI-SIM-006). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998.

[2] Porras, Phillip A. Neumann, Peter G. SRI International [A]. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances.

[3] Stephen. 网络入侵检测分析员手册 [M]. 余青霓等译. 北京:人民邮电出版社,2000.

[4] 林和东等. 防范黑客不求人[M]. 北京:人民邮电出版社,2001.