广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(4):288～290
Vol. 25,No. 4 November 2009

基于SNMPv3协议的校园网防火墙与入侵检测联动系统构建*

The Interactive Analysis of Firewalls and Intrusion Detection System Campus Network Based on SNMPv3

骆参驹[1],杨 颖[2]
LUO Can-ju[1],YANG Ying[2]

(1.广西工商职业技术学院网络中心,广西南宁 530003;2.广西大学计算机与电子信息学院,广西南宁 530004)
(1. Network Center,Guangxi Vocational College of Technical and Business,Nanning,Guangxi,530003,China;2. School of Computer,Electronic and Information,Guangxi University,Nanning,Guangxi,530004,China)

摘要:围绕高校网络系统的安全问题,通过基于SNMPv3协议的网络管理平台使防火墙与入侵检测系统产生联动,构建一个动态、实时的,能够实现网络安全整体化、立体化需求的网络系统安全框架,为校园网络安全提供一种解决方案。

关键词:网络安全 防火墙 入侵检测系统 SNMPv3协议
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2009)04-0288-03

Abstract:Focusing on the network system security of colleges,the paper makes a linkage platform between firewall and intrusion detecting system on the SNMPv3-based network management. It also builds a dynamic and real-time network security framework to realize the intergraded and tridimensional demand,which offers a solution to the campus-wide web security.

Key words:network security,firewall,intrusion detection systems,SNMPv3

作为高校信息化建设重要的基础设施,校园网络担负着教学、科研、管理和对外交流的重任。校园网络的安全状况直接影响到学校教学活动的顺利进行。目前校园网络面临的攻击呈等比增加,数据信息被窃取和针对网络设备的攻击等潜伏着的安全威胁层出不穷。解决高校网络信息安全问题不容忽视。防火墙、入侵检测系统、漏洞扫描系统是保障校园网安全的3种常见措施。

防火墙是架设于两个信任程度不同的网络驳接处的软件与硬件设备的组合,它对两个网络之间的通信进行控制,通过强制实施统一的安全策略,采用白名单和黑名单过滤有害的数据报文,以达到保护系统安全的目的[1]。防火墙只能在网络层或应用层进行访问控制,无法监控通信的数据内容,无法控制内部网络行为。防火墙系统是一个静态的网络攻击防御,对网络环境下日新月异的攻击手段缺乏主动的响应,不能提供足够的安全保护。网络入侵检测系统能够实时收集网络通信信息并对其进行分析,从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象,并依据既定的策略采取相应的措施,最大限度保护网络系统安全[2]。入侵检测系统被公认为是防火墙之后的第二道安全闸门,从网络安全立体纵深、多层次防御的角度出发,对防范网络恶意攻击及误操作提供了主动的实时保护,从而能够在网络系统受到危害之前拦截和响应入侵。入侵检测技术

收稿日期:2009-10-10
作者简介:骆参驹(1978-),男,讲师,硕士研究生,主要从事计算机网络与并行分布式计算技术研究。
*广西自然科学基金项目(桂科青0731023)资助。

可以弥补单纯的防火墙技术暴露出明显的不足和弱点,为网络安全提供实时的入侵检测及采取相应的防护手段,与防火墙共同成为网络安全的核心设备。本文探讨防火墙与入侵检测系统之间联动的技术,并将之与网络管理系统相结合,构造一个基于SNMPv3协议联动的高校校园网络系统。

1 联动策略机制

在入侵检测系统与防火墙构成的联动安全体系中(图1),管理中心通过对防火墙/入侵检测系统的轮询或者预定义陷阱获得安全事件信息,然后,管理中心将安全事件与联动策略库中的各条策略进行匹配,一旦匹配成功,则根据策略所定义的响应对有关安全设备进行设置。策略处理模块完成以下功能:系统初始化阶段,由管理中心在各个安全设备的策略处理器中设置联动策略,然后,管理中心除了适当监视或者进行调整干涉外,可不再参与联动策略的执行过程。当某个设备发生安全事件(如入侵检测系统检测到入侵事件等)时,策略处理器事件监视模块将对事件进行策略匹配,一旦匹配的该事件符合某条策略,将执行该策略中指定的响应,如发送某个SNMP陷阱至另一台设备(如防火墙)。当目标设备收到策略陷阱后,交给它策略处理器中的解析模块,最后根据解释结果执行某个响应(如封锁这个网段的所有网络业务)。

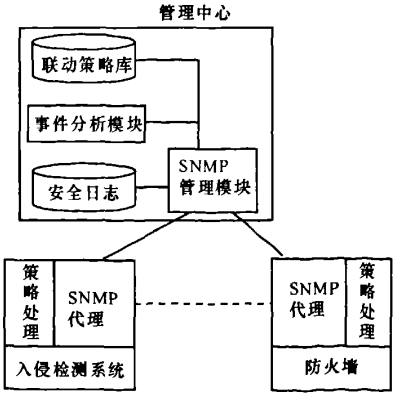

图1 联动系统框架

这种结构下,当发生安全事件时,网络上传输的仅仅是策略陷阱,并且在一般情况下不需要管理中心的直接参与,不仅可以摆脱对管理中心的过分依赖,而且可以在一定程度提高报警的准确率和减少误报率,减少安全组件间的通信流量,提高系统的性能,降低因为管理中心被侵入而对整个系统产生危害的风险。所以,这种模式非常适合对系统稳定性、可靠性要求较高的校园网环境。

2 联动的实现过程

如果系统中入侵检测探测到安全威胁事件发生就会发出报警信息。在SNMP代理的监控下,报警信息存放在管理信息库变量库里,管理工作站通过轮询获取管理信息库对象的值,了解在线入侵检测系统状态以及安全威胁事件。根据预先设置的trap表,安全威胁事件随时向管理模块发送错误报告,管理模块把实时收集的报警信息转换成统一格式发送到事件收集模块的事件数据库中,用于生成安全事件统计分析报告和图表。事件分析模块对转化成标准格式的事件信息根据知识库进行综合分析、推断和过滤,得到更有价值的数据,最终产生一个确定的安全警报到策略管理模块。策略管理模块对安全警报进行解析,通过对在策略库中的策略进行查询匹配,触发相应的联动策略,然后下达指令给防火墙的代理,使防火墙做出相应的SNMP应答和响应。对于更新和修改规则的请求,则由防火墙进行更新和修改后,通知控制台对防火墙规则的更新和修改是否成功,同时利用SNMP Trap向控制台报告异常行为。入侵检测系统与防火墙进行有效的互动后,以实现一个更为有效的网络安全防护体系,解决了传统信息安全技术的弊端,解决了原先防火墙的粗粒度防御和检测系统只发现难响应的问题。

如果在校园网内一个用户计算机系统感染上了某种病毒,这时具有安全设备联动机制的防护系统将产生如下动作:(1)入侵检测系统检测到了某台计算机被病毒感染;(2)入侵检测系统向安全管理中心发送一个协议数据包,报告病毒事件的详细信息;(3)网络管理中心根据这类事件的安全策略,向防火墙发送SNMP协议数据包;(4)防火墙收到消息立即封锁这个网段的所有网络业务,并以某种方式通知管理员。整个联动过程可以快速响应,第一时间阻止病毒传播,系统就可以把网络中不安全因素排除在外,从而避免更大的破坏。系统中联动策略机制起着关键的作用。

3 关键技术分析

3.1 SNMPv3消息的发送和接收

在联动控制台和代理进程之间,信息按照SNMPv3消息的格式进行发送和接收。SNMPv3的消息格式如图2所示。SNMP管理进程会先构建相应的PDU,在前面填充ContexName和

ContexEngineID，USM 会对加密部分进行对称加密，输出放到 PDU 域中。然后把 msgPrivacy-Parameters 的值设置为生成 IV（Initialization Vector）值，填入相应的参数。整个消息构建好之后 USM 执行认证算法，输出的认证码（MAC）放到 msgAuthentication Parameters 域中。这样一条含有认证消息的加密消息就可以从控制台的管理进程端发送到安全设备的代理进程端了。代理进程收到消息后，USM 先检测收到的 MAC 和它自己计算出来的 MAC 是否相符，如果相符，消息通过认证。然后 USM 通过 MsgAuthoritativeEngineBooks 和 MsgAuthoritativeEngineTime 参数检测消息是否在有效时间窗内，如果超时，则被认为认证未通过而被丢弃。最后如果 PDU 域被加密，则 USM 执行解密并返回明文。接着 VACM 模块会根据 PDU 域中的信息进行访问控制验证，看控制台是否有权对该防火墙/入侵检测系统的 MIB 变量做某种操作，如果访问控制验证通过，则把 PDU 中的信息送到 SNMP 应用模块进行处理，使得控制台对防火墙/入侵检测系统的管理信息库变量的操作能够最终安全实现。

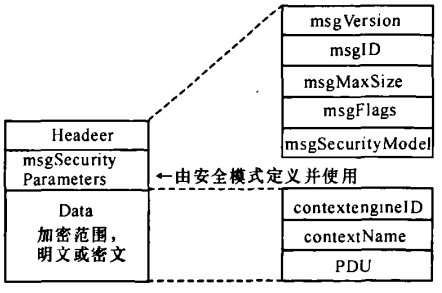

图 2 SNMPv3 消息格式

3.2 管理信息库的设计

管理信息库是管理信息的集合。SNMPv3 协议通过对管理信息进行相应的读写操作，对所管理的设备进行管理。

防火墙的管理信息库设计重点是针对防火墙静态包过滤规则进行的。通常防火墙的一条包过滤规则，包括：源 IP 地址、目的 IP 地址、目的端口、动作（通过还是丢弃）、作用时间等要素，所有这些要素都是建立管理信息库时需要考虑的对象。设计时可以把包过滤规则设计成一个专门的表，每一条规则对应表中的一行，这样可以通过 SNMP 协议规定的几种命令对这个表进行各种操作，从而达到控制防火墙包过滤规则的目的。

入侵检测系统的管理信息库不仅包括从事件分析器中获得的报警信息，而且包含了对入侵检测系统模块进行管理所必需的数据，它主要包括 5 张表：系统信息表、报警表、规则表、执行行为表，和日志表。系统信息表保存关于系统的总体信息，可以通过该表检索信息、有关事件收集的状态，定义一些全局配置的参数。报警表存储有关入侵检测系统发出的报警信息，其中包含 SNMP 的 Trap。规则表存储用来分析审计数据的规则。执行行为表存储对各检测事件所执行的行为动作。日志表存放收集来的审计数据，并依照 IDS RulesTable 中的指导作进一步的分析。

4 结束语

本文围绕高校网络系统的安全问题，将防火墙与入侵检测系统相结合，并通过基于 SNMPv3 协议的网络管理平台使两者产生联动，实现了网络安全整体化、立体化的需求，构建了一个动态、实时的网络系统安全框架，为校园网络安全提供一种解决方案。联动系统中 SNMPv3 协议本身的访问控制、身份验证和加密功能，同时为信息在网络设备间的安全传输提供了保证。如何对更多的安全产品与 SNMP 联动，以期不断地完善校园网络安全的整体防护，有待于在今后的工作中进一步的研究与分析。

参考文献：

[1] 周启明，李方敏. 防火墙与入侵检测系统的立体防御体系研究[J]. 网络安全技术与应用，2006(5)：22-24.

[2] 姚兰，王新梅. 防火墙与入侵检测系统的联动分析[J]. 信息安全与通信保密，2002(6)：29-31.

[3] WilliamStallings. SNMP 网络管理[M]. 胡成松，汪凯，译. 北京：中国电力出版社. 2001.

[4] 李连焕. 防火墙与入侵检测在校园网中的应用[J]. 计算机与信息技术，2007(15)：54.

（责任编辑：邓大玉）