网络安全事件集中管理系统的设计与实现

The Design and Implementation of Network Security Event Centralized Management System

黄家林　甘妙金　程 暄　张征帆　（中南大学信息科学与工程学院 湖南长沙 410083）

摘要：针对网络上的各种攻击，本文论述了一种基于网络日志等报警信息的网络安全事件集中管理系统。本文首先提出了其系统模型，然后详细阐述了系统实现的方法，最后论述了该系统的一些特点。本系统综合分析了的网络安全事件的报警信息，有效的降低了误报率，提高防御响应的准确性。

关键词：日志 报警信息 安全事件 集中管理

1 引言

由于互联网具有开放性、互连性、共享性的特点，使其遭受入侵的风险越来越严重。计算机网络安全问题日益突出[1,2]。

目前针对网络上的各种攻击，已经出现了各种各样的安全防御产品。尽管安全技术越来越复杂，但因特网还是很容易受到攻击[3]。在实际运行中发现每个单一的安全产品都有其特有的功能和作用范围，但普遍存在漏报、误报和重复报警（广义上说也属于误报）的现象，并且这些来自不同层次、不同安全设备的信息也难以反映系统整体的安全状态，相互之间无法协调工作。使得安全管理人员淹没在大量的报警信息之中而无法对安全事件做出及时、有效的响应，也难以应对有步骤、有组织的复杂攻击[4]。

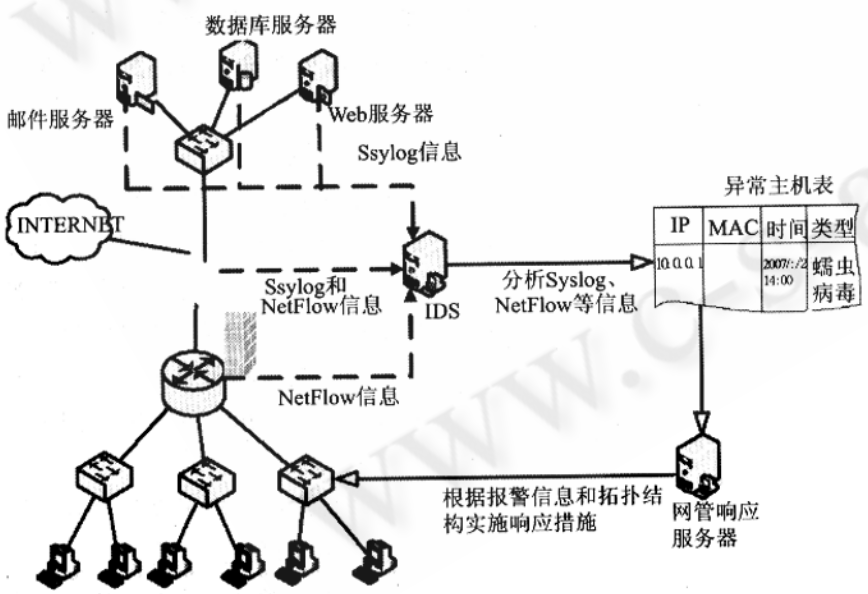

图 1　系统整体框架

针对上述问题，我们应该将网络安全事件统一进行管理。目前比较好的网络安全事件集中管理系统的相关产品有 Intrusion Vision 公司的可视化数据管理工具，Intellitactics 公司的 Intellitactics Security Manager，SecurityFocus 公司开发的 Aris 系统，Cisco 公司的 MARS 系统，Juniper 公司的安全准入系统。

以上提到的这些产品大多价格很高，另外对其它一些公司的网络设备，尤其是国产网络设备的支持不足，使得其兼容性不好。针对这些问题我们设计了本系统，系统综合分析了网络安全事件的报警信息，以期降低误报率，提高防御响应的准确性。

2 系统整体框架和模型

本文设计的系统的整体框架如图 1 所示。在该模型中，一次安全事件的完整响应过

程包括三个阶段:网络安全报警信息的收集、分析和对分析的结果进行自动响应。

首先,对网络中需要监控的路由器、交换机、防火墙、服务器、主机等设备进行配置,将其 Netflow、Syslog 等日志信息收集到入侵检测系统(IDS)中。入侵检测系统接收从网络设备发来的各种信息,并将其保存在数据库中。定期对数据进行综合分析,完成分析后将异常主机的信息保存在另外的一个表中,我们称之为异常主机表。然后,异常主机表被发送到网管服务器中,网管服务器根据表中的 IP、MAC 等信息对威胁进行定位,并最终确定威胁产生机器的网络接入点。在完成以上各步后,网管服务器根据威胁的类型和安全策略确定响应方式,并与接入点的网络设备联动,最终关闭所在接入点设备上的转发端口,将威胁彻底从网络中消除。

本系统的系统模型如图 2 所示,主要包括四个层次:安全事件预处理层,报警事件处理层,管理层和响应层。其中的安全事件预处理层和报警事件处理层的主要任务就是对安全事件进行分析,管理层和响应层的任务是对分析的结果进行响应。

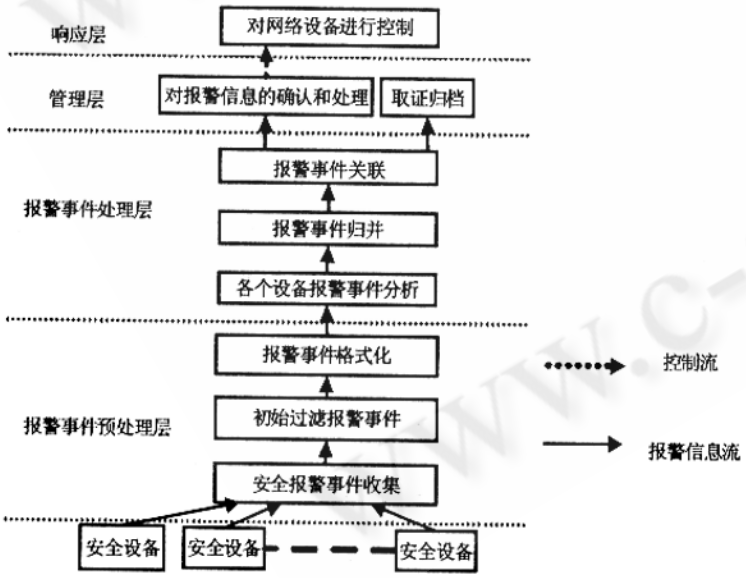

图 2　系统模型

3　系统实现

本文实现的系统是在 RedHat AS4 平台上用 Java 开发的;数据库使用的是 mysql5.0。各层的功能实现如下。

3.1　报警事件预处理层

同一网络安全事件在不同设备的日志信息中都有反映,但由于日志信息格式没有统一的规范,使得各个安全设备对同一事件的反映在格式等方面有些差异。这样在各个安全设备之间产生了大量的重复报警信息。有用的报警信息被淹没在海量的报警信息中。这就要求我们对这些信息进行有效的分析和处理。本层首先经过初始过滤将一些明显是误报或冗余的报警信息删除,之后经过报警事件格式化将不同设备产生的报警信息用统一的格式表示出来。如果一条报警信息包含的内容为{安全设备编号,源地址/端口,目的地址/端口,报警产生时间,报警结束时间,消息类型标志,响应优先级别,攻击类别,附加数据},那么假设攻击事件用 E 表示,则这条报警事件可以对应表示为

E = (Dev_ID, SrcIP, SrcPort, DestIP, DestPort, Begin_Time, End_Time, MessageClassID, ResponsePriority, Classification, AdditionalData)

其中,消息类型标志 MessageClassID = 0 时,表示 E 为报警信息;报警 E 对应的可能响应优先级别 ResponsePriority 的取值范围为二进制的 000 到 111,对应的优先级别由低到高;Classification 表示攻击类别,分别采用 CVE 编号和 EventType 两个属性来描述,AdditionalData 为安全设备的原始报警详细信息。

3.2　报警事件处理层

本层的功能主要是处理经过报警事件预处理层处理的数据,归并这些报警事件,将存在冗余关系的报警事件归并成一条新的报警事件,关联报警日志,消除重复报警,减少报警信息量。系统主要是利用聚类和分类的方法来消除重复报警。利用时间戳将不同设备的安全事件关联起来。

报警事件处理层中日志报警信息经过了如图 3 的分析步骤得到分析结果。

本系统首先对 Syslog 和 NetFlow 的日志信息进行处理、分析。对海量的数据信息进行挖掘,从中提取网络行为特征(威胁定性),找出攻击源(威胁定位)。对于防火墙的 Syslog 和 NetFlow 信息首先对同一地址的连接数进行分析,这样可以减少很多的误报事件,本系统根据经验确定连接数的阀值,得出可能有威胁存在的机器,然后根据地

址、端口、协议和数据包大小等分类，确定威胁机器并分析出入侵行为。对于主机 Syslog 信息进行 Mac 冲突分析、ssh 登录分析、拓扑环路分析和连接数分析等多种技术来确定威胁的机器。

上述步骤分析的是单个安全设备的日志事件。之后本系统对这些处理后的日志信息进行归并。主要方法如下。

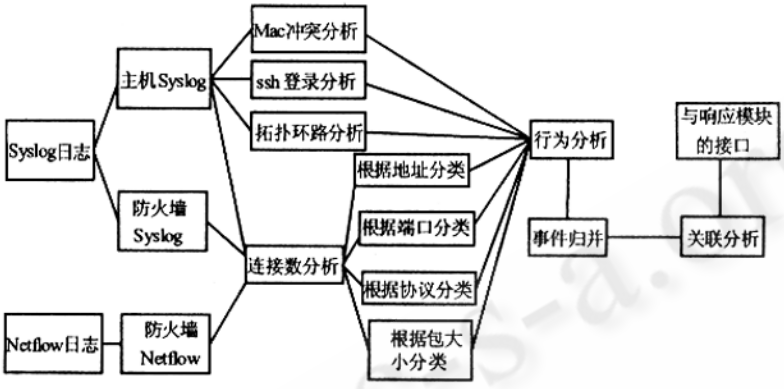

图 3　日志的分析流图

IP地址	MAC地址	接入端口	处理端口	vlan号	被封时间	解封时间	被封原因	建议方法	修改	解封	被封依据
192.168.64.6	00e0.4cf7.3ca3	6509;G3/4	6509;G3/4	64	07-05-18 14：40		UDP连接过多	安装系统补丁，清除计算机病毒，如果本机是代理服务器，则需要对其所代理的每台计算机安装系统补丁，清除计算机病毒才能解决问题。	修改	解封	查看
IP地址为192.158.64.6的计算机共1条被封锁历史记录											

图 4　管理当前被屏蔽用户

假设有两个报警事件，第一个事件用上述表示方法表示为：A1（Dev_ID1，SrcIP1，SrcPort1，DestIP1，DestPort1，Begin_Time1，End_Time1，MessageClassID1，ResponsePriority1，Classification1，AdditionalData1）。第二个事件用上述表示方法表示为：A2（Dev_ID2，SrcIP2，SrcPort2，DestIP2，DestPort2，Begin _ Time2，End _ Time2，MessageClassID2，ResponsePriority2，Classification2，AdditionalData2）

（1）若只有 Begin_Time，End_Time 和 AdditionalData 不同，并且时间之差小于设定的阈值，则满足重复关系；

（2）若只有 Dev_ID，Begin_Time，End_Time 和 AdditionalData 不同，并且时间之差小于设定的阈值，则满足并发关系。

冗余归并后的报警信息如下：A（SrcIP1，SrcPort1，DestIP1，DestPort1，Min（Begin_Time，End_Time），Max（Begin_Time，End_Time），MessageClassID1，ResponsePriority1，Classification1，AdditionalData1）。这样就消除了大量的重复报警事件。

经过归并处理后的报警信息再经过关联分析，再分析确认入侵机器和入侵行为。最后根据网络安全威胁程度，响应优先级别和攻击类别等，分别采取通知系统管理员或直接提交到主动防御响应模块进行处理。

3.3　管理层

管理层主要负责把经过处理而得到的报警信息提供给系统管理员或用户，此时呈现在系统管理员面前的报警信息简练、清晰，方便系统管理员根据当前状态作出响应，采取相应的防范措施。另外，本层还归档管理的依据。当定位到有威胁的机器后，将相关的报警信息和原始数据包整理进行归档，并对这些证据进行管理以作为处理的依据。

比如我们要封锁 IP 地址为 192.168.64.6 的计算机，其管理界面截图如图 4 所示。

3.4　响应层

经过处理后得到的报警信息以可视化的方式提供给管理员后，可以根据实际情况，对相应的设备进行手动或自动处理。如：出现针对某一个 IP 地址的报警，管理员想封锁这个 IP 地址，则只要在管理界面上或通过程序自动进行操作就可达到目的。

要自动的对设备进行控制，就必须利用一种或几种技术准确的定位有威胁的机器。在系统设计中利用数据链路层拓扑发现技术，对威胁进行自动搜索和准确定位。

当准确的定位到攻击源后，还必须对攻击源进行处理。根据威胁的种类和预先定义的安全策略，采用合理的方式对其响应，从而达到减缓、限制威胁或者消除攻击源的目的。其中采用的方式可以是屏蔽用户及

通知用户等。

4 系统的特点

本系统其特点如下：

(1) 有效地减少重复报警信息。本系统通过层层过滤的方法减少重复报警。首先安全事件预处理层经过初始过滤将一些明显是误报的报警信息过滤，然后在报警事件处理层利用各种分析技术进一步减少重复报警信息。

(2) 处理后的报警信息简洁。经过处理后的报警信息提供给网络管理员和用户，可以有效的减轻网络管理员的负担。

(3) 与现有设备兼容。本系统各个环节的处理使用的是标准协议，所以其可以与现有不同公司的网络设备兼容。

(4) 可扩展性好。本系统目前只收集了来自防火墙和主机服务器的 Syslog 日志信息以及防火墙的 NetFlow 信息。事实上，本系统是基于模块化的设计，系统还可以通过增加模块收集来自其它网络安全设备的信息而不需要改变系统的其他任何一部分的设计。应该说收集的报警信息来源越多，分析的结果就越精确，威胁定位的也就越准确。

5 结束语

本文针对现有网络安全防御方面的缺点以及现有相关产品的存在的问题提出了网络安全事件集中管理系统。首先提出了该系统的模型，对该系统进行了总体的描述；然后介绍了系统各层功能的实现；最后介绍了系统的一些特点。本系统在实际工作过程中运行良好。

参考文献

1 Richardson R. 2003 CSI/FBI Computer Crime a - nd Security Survey [R/OL]. http:// www. gocs - i. com/aeareness/fbi. jhtml. 2003.

2 张宏，网络安全基础(第一版) [M]，北京：机械工业出版社，2004 年，131.

3 匿名等著，王东霞、李蔚红等译，最高安全机密(第四版) [M]，机械工业出版社，2004 -3.

4 佟奎强、邓兆云、李维东，安全事件集中管理系统的开发与应用[J]，电网技术，2006 -8，30(5).

5 李辉，多层次入侵事件检测和关联方法研究[D]，西安：西安交通大学，2003.

6 Intellitactics. Solving Challenging Problems [EB/OL]. http://www. intellitactics. com/blue. asp? PageID = 21.

7 Cisco. Cisco Security Monitoring, Analysis and Response System [EB/OL]. http://www. cisco. c - om/en/US/products/ps6241/products _ data _ sheet0900aecd80272e64. html. 2006.