入侵检测系统综述

任恒妮^{1,2}

(1、西安电子科技大学,陕西 西安 710071 2、陕西国际商贸学院,陕西 咸阳 712046)

摘要:对于任何一个国家、企业或者个人来说,随着计算机及网络的发展,网络安全问题是一个无法回避且重要的问题呈现在面前,很多非法分子或者合法用户的不当使用都会对网络系统造成破坏,针对这些行为要采用相应的技术进行制止或者预防,入侵检测技术成为解决该问题的最好方法之一。文章主要综述了入侵检测系统的基本检测方法。

关键词:入侵检测;入侵检测系统;误用检测;异常检测

1 入侵检测系统概述

随着计算机技术及网络技术的不断发展,计算机及数据的安全问题随之出现,传统的防火墙技术虽然可以进行有效的防御,但是由于其存在很多弊端,例如很多外部访问不经过防火墙,来自计算机数据库内部的威胁等,防火墙就无能为力了,它并不能对已经进入计算机系统或者来自计算机数据库内部威胁进行检测,访问控制系统可以根据权限来防止越权行为,但是很难保证具有高级权限的用户对系统所做的破坏行为,也无法阻止低权限用户非法活动高级权限对系统所进行的破坏,漏洞扫描系统是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查,然后根据扫描结果向用户提供系统的安全性分析报告,以使用户采取相应措施来提高网络安全。它虽然可以发现系统和网络漏洞,但无法对系统进行实时扫描,入侵检测系统可以进行实时扫描。

发现入侵行为就是入侵检测。它通过从计算机网络或系统的核心点收集信息并对其进行分析,然后从其中看网络或系统中是否有违反安全策略的动作和被攻击的迹象。入侵检测目的是保证系统资源的可用性、机密性和完整性,要达到这个目的就要对系统的运行状态进行监视,以便发现各种攻击操作、攻击结果或者攻击动态。进行入侵检测的硬件与软件的组合构成了入侵检测系统,它能执行所有的入侵检测任务和功能,监视或阻止入侵或者企图控制系统或者网络资源的行为,它可以实时检测入侵者和入侵信息,并进行相应处理,最大化的保证系统安全。通过对系统各个环节来收集和分析信息,发现入侵活动的特征,对检测到的行为自动作出响应、记录并报告检测过程及结果是入侵检测系统的基本原理的四个部分。

入侵检测系统从系统结构看,至少包括信息源、分析引擎和响应三个功能模块。信息源的功能是分析引擎提供原始数据,入侵分析,信息源的正确性和可靠性直接影响入侵检测的效果,要使检测系统软件具有完整性,必须使IDS软件自己有很强的坚固性,分析引擎的功能是执行入侵或者异常行为检测,分析引擎的结果提交给响应模块后,响应模块采取必要和适当的措施,阻止入侵行为或回复受损害的系统。分析引擎包括完整性分析、模式匹配和统计分析。响应可分为主动响应和被动响应。主动响应就是系统自动或者以用户设置的方式阻断攻击过程或以其他方式来阻断攻击过程,被动响应是系统只报告和记录发生的事件。响应包括简单报警、切断连接、封锁用户、改变文件属性,最大的反应就是回击攻击者。

入侵检测系统性能主要的参数是误报和漏报。所谓误报就是把正常事件的识别看做是攻击,所谓漏报是指本来是攻击事件却没被IDS检测。根据入侵检测技术系统采用的技术的不同,将IDS分为异常检测系统和特征检测系统。异常检测把入侵活动异常于正常主体活动作为假设,建立一个“活动简档”作为正常活动文档,对系统运行进行实时监控,若发现当前主体的活动与其统计规律发生冲突时,便进行报警。异常入侵检测技术与系统相对无关,通用性较强,甚至有可能检测出以前未出现的攻击行为,但误检率高,面临受恶意训练攻击的可能。

特征检测系统是把入侵者的活动用一种模式表示出来作为假设,对系统运行进行实时观察,比较观察到的对象与这些模式是否一致或者相符,一旦发生了相符情况,便进行报警。检测准确度高是其最大的优点,但是受已知知识的局限,另外对目标系统依赖性太强,不但移植性不好,维护工作量大,对于内部人员的入侵行为无能为力。

2 常见的入侵检测方法

2.1 在异常入侵检测系统中常常采用以下几种检测方法:

2.1.1 基于贝叶斯推理检测法:是通过在任何给定的时刻,测量变量值,推理判断系统是否发生入侵事件。

2.1.2 基于特征选择检测法:指从一组度量中挑选出能检测入

侵的度量,用它来对入侵行为进行预测或分类。

2.1.3 基于贝叶斯网络检测法:用图形方式表示随机变量之间的关系。通过指定的与邻接节点相关一个小的概率集来计算随机变量的联接概率分布。按给定全部节点组合,所有根节点的先验概率和非根节点概率构成这个集。贝叶斯网络是一个有向图,弧表示父、子节点之间的依赖关系。当随机变量的值变为已知时,就允许将它吸收为证据,为其他的剩余随机变量条件值判断提供计算框架。

2.1.4 基于模式预测的检测法:事件序列不是随机发生的而是遵循某种可辨别的模式是基于模式预测的异常检测法的假设条件,其特点是事件序列及相互联系被考虑到了,只关心少数相关安全事件是该检测法的最大优点。

2.1.5 基于统计的异常检测法:是根据用户对象的活动为每个用户都建立一个特征轮廓表,通过对当前特征与以前已经建立的特征进行比较,来判断当前行为的异常性。用户特征轮廓表要根据审计记录情况不断更新,其保护去多衡量指标,这些指标值要根据经验值或一段时间内的统计而得到。

2.1.6 基于机器学习检测法:是根据离散数据临时序列学习获得网络、系统和个体的行为特征,并提出了一个实例学习法IBL,IBL是基于相似度,该方法通过新的序列相似度计算将原始数据(如离散事件流和无序的记录)转化成可度量的空间。然后,应用IBL学习技术和一种新的基于序列的分类方法,发现异常类型事件,从而检测入侵行为。其中,成员分类的概率由阈值的选取来决定。

2.1.7 数据挖掘检测法:数据挖掘的目的是要从海量的数据中提取出有用的数据信息。网络中会有大量的审计记录存在,审计记录大多都是以文件形式存放的,如果靠手工方法来发现记录中的异常现象是远远不够的,所以将数据挖掘技术应用于入侵检测中,可以从审计数据中提取有用的知识,然后用这些知识区检测异常入侵和已知的入侵。目前的方法有KDD算法,其优点是善于处理大量数据的能力与数据关联分析的能力,但是实时性较差。

2.1.8 基于应用模式的异常检测法:该方法是根据服务请求类型、服务请求长度、服务请求包大小分布计算网络服务的异常值。通过实时计算的异常值和所训练的阈值比较,从而发现异常行为。

2.1.9 基于文本分类的异常检测法:该方法是系统产生的进程调用集合转换为“文档”。利用K最近邻聚类文本分类算法,计算文档的相似性。

2.2 误用入侵检测系统中常用的检测方法有:

2.2.1 模式匹配法:是常常被用于入侵检测技术中。它是通过把收集到的信息与网络入侵和系统误用模式数据库中的已知信息进行比较,从而对违背安全策略的行为进行发现。模式匹配法可以显著地减少系统负担,有较高的检测率和准确率。

2.2.2 专家系统法:这个方法的思想是把安全专家的知识表示成规则知识库,再用推理算法检测入侵。主要是针对有特征的入侵行为。

2.2.3 基于状态转移分析的检测法:该方法的基本思想是将攻击看成是一个连续的、分步骤的并且各个步骤之间有一定的关联的过程。在网络中发生入侵时及时阻断入侵行为,防止可能还会进一步发生的类似攻击行为。在状态转移分析方法中,一个渗透过程可以看作是由攻击者做出的一系列的行为而导致系统从某个初始状态变为最终某个被危害的状态。

参考文献

- [1]李剑.入侵检测技术[M].北京:高等教育出版社,2008.
- [2]薛静锋.入侵检测技术[M].北京:机械工业出版社,2004.
- [3]吴庆涛,邵志清.入侵检测研究综述[J].计算机应用研究,2005,12.