面向ASP服务平台入侵检测技术研究

周旺基
(盐城工学院 电信学院,江苏 盐城 224051)

摘要:对ASP服务平台安全情况进行分析,提出面向ASP服务平台入侵检测技术,并详细描述了入侵检测检测系统工作流程、进行入侵检测检测系统功能分析等。通过实验验证了该面向ASP服务平台入侵检测技术的有效性。

关键词:ASP服务平台;入侵检测;网络安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1671-5322(2008)04-00014-04

ASP(Application Service Provider)应用服务系统平台是ASP厂商对企业提供在线业务应用服务和管理服务的基于Internet的应用软件系统平台,其应用软件系统安装在数据中心(IDC)或服务器集群上,通过网络将应用软件的功能提供给使用者的营运模式[1]。企业用户可以直接租用ASP的计算机及软件系统进行自己的业务管理,从而节省了用于IT产品技术购买和运行的资金,因此ASP成为中小企业信息化的首选模式。

作为一种典型的WEB应用,安全问题成为当前限制ASP发展的最重要方面,良好的安全策略能促进ASP的迅速发展及应用。尽管大多数ASP提供商采取了相关的安全措施,但是对ASP安全问题的研究局限在物理安全、网络安全、数据加密等表层,使ASP安全问题难以有突破性进展[2]。本文研究面向ASP的入侵检测系统这一网络安全机制,实时监测并分析ASP企业用户的活动,识别正在发起的攻击行为,对异常的网络活动进行分析,阻止不安全的网络活动,从而保障网络安全性。

1 ASP服务平台安全分析

在ASP模式中,用户与ASP通过Internet进行数据传输,数据被暴露在外面,任何用户、个人都可以通过Internet随意地访问ASP平台,非法客户可以通过网络截获用户数据。数据包含企业机密,企业的核心业务数据,不希望被企业以外的人看到,更不希望被竞争对手看到。另外使用同一个ASP的企业竞争对手的数据可能放在同一个数据库中,多个用户在使用同一个应用程序,通过同一个应用程序访问同一个数据库,所有这些,使得ASP安全问题比其他模式的安全问题更为敏感,更为重要。

ASP应用程序有用户、程序及对象三部分组成。与系统安全相比,描述三重关系的应用领域安全更为复杂。在系统安全领域,经常是有大量的用户和对象,但是只有几个操作,如读、写、执行文件操作等。这意味着只有一个应用操作的系统安全的复杂度较低。因此,安全系统得授权通常用二维关系来定义。而在应用安全领域,有众多的用户、大批量的对象以及大量的操作,因此应用领域是具有高度复杂的三维安全关系。

2 面向ASP服务平台的入侵检测模型

目前有多种入侵检测模型。面向ASP服务平台入侵检测是基于通用入侵检测构架CIDF(Common Intrusion Detection Framework)的一种模型(如图1所示)。它将一个入侵检测系统分为4个组件,并将需要分析的数据通称为事件,事件可以是基于网络的数据包也可以是基于主机的系统日志中的信息。

(1)事件产生器:事件产生器是入侵检测系统中负责原始数据采集的部分,它对数据流、日志文件等进行追踪,然后将搜集到的原始数据转换

收稿日期:2008-06-20
作者简介:周旺基(1968-),男,江苏射阳人,讲师,主要研究方向为计算机软件设计与应用。

万方数据

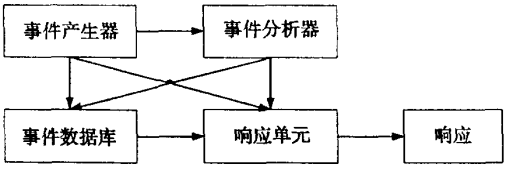

图 1　ASP 入侵检测系统模型

Fig. 1　The ASP Intrusion detection system model

为事件,并向系统的其他部分提供此事件。

(2)事件分析器:事件分析器接受事件信息,然后对它们进行分析,判断是否是入侵行为或异常现象,最后将判断的结果转换为警告信息。

(3)事件数据库:事件数据库是存放各种中间和最终数据的地方。它从事件产生器或事件分析器接收数据,一般会将数据进行较长时间的保存。它可以是复杂的数据库,也可以是简单的文本文件。

(4)响应单元:响应单元根据警告信息做出反应,它可以做出切断连接、改变文件属性等强烈反应,也可以只是简单地报警,它是入侵检测系统中地主动武器。

以上 4 个部分只是入侵检测系统的基本组成部分。从具体实现的角度看,入侵检测系统一般包括软件和硬件 2 个部分。硬件设备主要完成数据的采集和响应的设施,软件部分主要完成数据的处理、入侵的判断、响应的决策等功能。

2.1　入侵检测系统功能分析

入侵检测系统是通过实时监测信息源收集到的数据和信息进行关联筛选可疑行为,从中获得对检测入侵行为有价值的信息,然后对这些信息进行分析,从而检测出恶意入侵攻击行为并及时报警给网络管理者,以便迅速地采取相应措施阻止恶意的攻击,保障网络的安全[3]。入侵检测系统主要通过监控网络、系统、用户的状态和行为,来检测系统用户的超出边界行为和入侵的不轨企图等,能在入侵攻击对系统发生破坏前,检测并减少入侵攻击所造成的损失。

根据原始数据的信息源分类,入侵检测系统主要分为:基于主机的入侵检测系统和基于网络的入侵检测系统 2 类。基于主机的入侵检测系统。它用于保护网络中关键运行的服务器和主机,通过监视与分析主机的审计记录和日志文件来检测入侵,并迅速地启动相应的应急响应程序来断开攻击源的连接或进行反攻击。具有监控程度高、配置灵活、投资少等优点[4-5]。基于网络的入侵检测系统,它使用原始网络包作为数据源,通常利用运行在混合模式下网络设备来实时监测并分析通过网络的所有数据包。它的异常行为识别模块使用模式或表达式匹配、频率阀值、统计非常规现象等来识别攻击行为。若数据包与已知的攻击模式匹配,入侵检测系统将迅速报警或断开网络连接。

2.2　入侵检测系统体系结构

入侵检测系统的组成主要由数据采集模块、数据分析模块、数据管理模块、数据预处理模块、通信模块、数据存储模块、数据响应模块等组成。入侵检测系统的系统结构如下图所示:

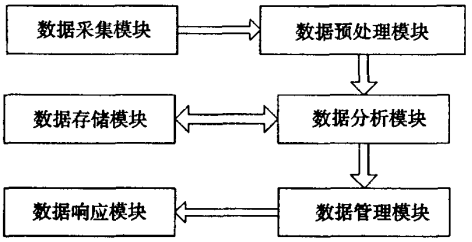

图 2　入侵检测系统的结构

Fig. 2　The structure of intrusion detection system

数据采集模块主要用来搜集数据,供分析模块分析;数据分析模块完成对数据的解析,并作出判断;数据管理模块通过图形界面,完成与用户的信息交互,提供检测结果,实现对其它模块的动态配置及管理,并及时作出决策;数据预处理模块完成对数据进行筛选、分类、合并和转换的任务;通信模块保证数据在各模块之间实时安全地通讯;数据存储模块将分析的结果和得出的新入侵行为模式保存入数据库;数据响应模块接收并执行管理模块作出的决策。

2.3　入侵检测系统工作流程

入侵检测系统各模块之间工作流程可用图 3 来表示。基于主机的信息源主要来自于系统日志和应用程序的事件日志。操作系统日志记录操作系统事件,由操作系统的系统程序产生的事件组成,这些事件包括组件失败事件、数据错误事件、应用程序瘫痪事件;安全日志中记录安全事件,例如有效或无效的注册和登录与退出,以及与系统资源相关的事件如创建、修改、删除系统文件等;事件日志记录应用文件,其记录的事件类型由具体的应用程序决定。基于网络的信息源一般都为

万方数据

网络数据包,在网络中传输的信息都是以网络数据包的形式存在的,故只要截获网络中的所有数据包,并加以分析,便能辨别出入侵网络包。通常使用包捕获工具可以获取网络数据包。例如网络监控程序 Tcpdump。Tcpdump 可以将通信网络中传输的数据包的包头完全截获以提供分析。它支持针对传输层、网络层、端口和协议的过滤。

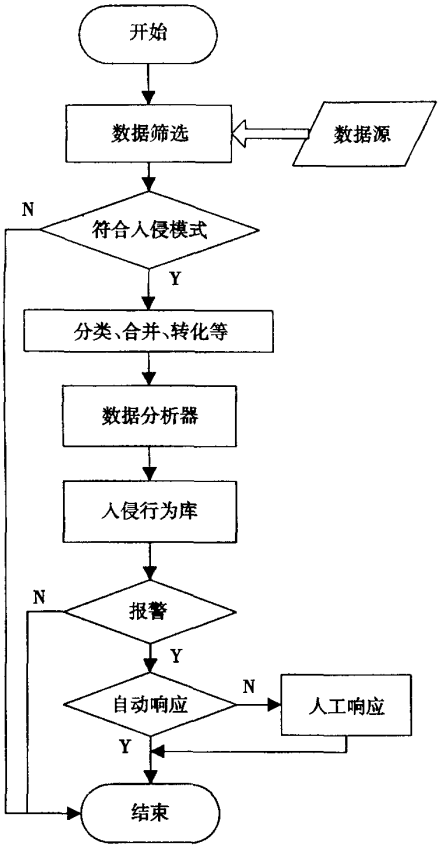

图3 入侵检测系统各模块工作流程

Fig.3 The working process of intrusion detection system

数据分析模块是入侵检测系统的核心部分,通过采用各种统计分析、特征匹配、数据挖掘、协议分析、自适应学习等技术完成具体的事件分析任务,确定该事件是否为入侵行为并决定是否送给管理模块进行决策响应。目前常用的分析检测方法有异常检测方法和特征检测方法以及两者结合的互补应用。异常检测是对系统的正常行为的建模,通过建立系统和用户的正常行为模型,监测用户的行为是否符合正常行为模型,从而做出决策判断。这种方法是指正常行为库中没有描述的行为被认为是不符合正常行为的,判断为入侵。它的难点是建立正常行为数据库,优点是能检测出未知的入侵手段,缺点是误报率高。特征检测是对已知的入侵手段和系统缺陷进行检测,是对不正常行为的建模。

数据响应模块接收并执行管理模块作出的决策,根据管理模块的命令在主机或网络上实施相应的响应措施,如发送 TCP 的 RESET 数据包,断开指定连接,或自动报警给管理员,由管理员综合考虑入侵行为将造成的后果采取具体措施。

2.4 入侵检测系统相关代码

入侵行为检测消息交换格式采用 XML 进行编码报警数据,具体如下:

```
//入侵检测到的黑客来源
<Address ident
="c2b5e1s3 -002" category ="ipv4 -net -mask" >
<Address >
172.16.2.112
</Address >
//入侵检测到的入侵 IP 地址
<netmask >
202.16.45.108
</netmask >
//入侵检测到的入侵网络掩码
</Address > //结束标识符
</Node >
</Source >
</Alert >
</IDMEF -Message >//结束标识符
```

3 入侵检测实验

通过网络数据包捕获工具 Tcpdump 捕获采集大量网络数据,同时使用系统日志文件、安全日志文件和应用程序日志文件中的主机数据进行训练,利用神经网络算法和数据挖掘技术得到网络正常行为和异常行为的模式,建立了入侵行为检测模型,并进行特征检测和异常检测。在特征检测实验中,从不正常数据中不断挖掘和自适应学习获得特征模式,构造入侵行为特征。

实验中,我们将网络攻击分为 IP 攻击、ARP/RARP 攻击、ICMP/IGMP 攻击、TCP 攻击、FTP 攻击、TELNET 攻击等,根据这些入侵手段,通过自

万方数据

适应学习和数据挖掘技术构造了基于网络连接失败的统计特征和内容特征、基于端口登陆尝试次数值的统计特征的入侵行为检测模型,分别用于检测相似或相关联的入侵行为。实验结果验证了模型的可行性并能有效地检测中获得的类似入侵模式。

4　结束语

面向ASP服务平台的入侵检测与防火墙技术相比,本技术可以通过数据挖掘技术等自适应学习算法学习攻击者的入侵行为特征和模式,并通过数据管理模块做出决策后及时地通知数据响应模块采取措施,以保护网络的安全运行。入侵检测技术是一种基于主动捕获的网络安全保障技术,对网络的内部攻击、外部攻击都提供了实时监测防护,能有效避免ASP服务平台中的重要资源受到攻击。

参考文献:

[1] 谢庆生.我国制造业ASP发展的模式与策略[J].中国制造业信息化,2003(1):66-70.
[2] 李少波,谢庆生.基于ASP的动态联盟制造资源管理框架研究[J].中国机械工程,2005,16(6):502-507.
[3] 饶元,冯博琴.基于状态的入侵检测系统研究,信息技术[J].2003,27(12):50-53.
[4] 周明全,吕林涛,李军怀.网络信息安全技术[M].西安:西安电子科技大学出版社,2003.
[5] 周世杰,秦志光.基于多Agent的入侵快速响应系统[J].电子科技大学学报,2004,33(4):419-422.

Research on ASP - Oriented Intrusion Detection Technology

ZHOU Wang-ji
(School of Electronics, Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)

Abstract: With the complication of the Internet and the development of the service provided by the ASP - platform, the problem of internet security is becoming more and more important, and network attacks happen occasionally. After analyzing the security circumference of the ASP - platform, a ASP - oriented intrusion detection technology has been put forward, and the process of the intrusion detection system and function analysis discussed in detail. Finally, a case has been employed to demonstrate the practicality of applying ASP - oriented intrusion detection technology.

Keywords: ASP service platform; intrusion detection; network security

(责任编校:张英健;校对:沈建新)

万方数据