

融合漏洞扫描的入侵检测系统模型的研究

段丹青^{1,2}, 陈松乔¹, 杨卫平^{1,2}

(1. 中南大学 信息科学与工程学院, 湖南 长沙 410083;

2. 湖南公安高等专科学校, 湖南 长沙 410006)

摘 要: 目前大部分入侵检测系统(IDS)采用基于模式匹配的入侵检测方法,该方法由于计算量大,因而在高速网络中检测效率较低。文章提出一种新的融合漏洞扫描功能的 IDS 模型,通过定期对系统进行漏洞扫描,及时修补系统安全漏洞,同时 IDS 根据漏洞扫描结果,对模式库进行动态更新,删除与得到修补的漏洞有关的攻击模式,缩减模式库的规模,提高检测效率。文章根据该模型提出一种基于多 Agent 的分布式 IDS 体系结构,提高了系统的可扩展性。

关键词: 入侵检测; 漏洞扫描; 模式匹配; 多 Agent

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2006)05-0131-03

An Intrusion Detection System Model Merged Vulnerability Scanner

DUAN Dan-qing^{1,2}, CHEN Song-qiao¹, YANG Wei-ping^{1,2}

(1. College of Information Science and Engineering, Central South University, Changsha 410083, China;

2. Hunan Public Security College, Changsha 410006, China)

Abstract: At present, most of intrusion detection systems employed a detection mechanism: the pattern matching, but due to giant computation of this mechanism, the IDS had low efficiency in high-speed network. The paper provides a new model of IDS merged vulnerability scanner. In this model, the system is scanned by the vulnerability scanner in regular time and patched the vulnerabilities in time, according to the results of the vulnerability scanner, the IDS will delete the attack patterns related with this patch in pattern library, it will decrease the size of pattern library, improve the efficiency of the IDS. Based on this model, the paper designs an IDS architecture based on multi-agent to improve the extensibility of the system.

Key words: intrusion detection; vulnerability scanner; pattern matching; multi-agent

0 引言

随着 Internet 的飞速发展,网络系统的安全性问题日益突出,计算机系统每天都遭受大量的安全威胁,要确保存在安全问题的信息系统免遭入侵是非常困难的。为了保证计算机系统安全性,各种网络安全方案相继产生,以期从不同角度、不同层次对网络实施保护^[1]。

入侵检测系统(IDS, Intrusion Detection System)通过对网络和系统记录的日志文件的分析来发现非法的入侵行为以及合法用户的滥用行为。入侵检测系统作为一种主动式的安全防御手段,已经成为网络安全技术的研究热点。

目前大部分 IDS 采用基于模式匹配的入侵检测方法,该方法是由 Kumar 在 1995 年提出的^[2],其原理是用一定的模式描述来提取攻击的主要特征,通过判别网络中搜集到的数据特征或从主机审计数据中提取的数据特征

是否在模式库中出现来检测入侵行为。模式匹配的特点是原理简单、扩展性好、检测效率高,可以实现实时检测,因而已经成为入侵领域中应用最为广泛的检测手段和机制之一。

然而,采用模式匹配的 IDS 存在以下问题:

(1)计算量大:采用模式匹配的 IDS 能否准确地识别出入侵行为,取决于能否对网络上的全部数据包进行监听和分析。IDS 中,截获网络的每一个数据包,并分析、匹配其中是否具有某种攻击的特征需要耗费大量的时间和系统资源,由于新的攻击方法层出不穷,新的漏洞不断被发现,模式库必将变得越来越庞大,模式匹配耗费的时间也就越多,因而不可避免地会降低检测效率。

(2)系统维护量大:采用模式匹配的 IDS 能否准确地识别出入侵行为,也依赖于模式库的完备性。完备模式库的建立是比较困难的,基于模式匹配方法的 IDS 要想检测到某一攻击的多种变形,必须将每一种变形的攻击模式都放入模式库,毫无疑问,这是不现实的。在目前 IDS 中,模式库的更新主要由系统管理员负责,采用手工进行,其更新速度较慢,难以满足入侵检测的需要。

可以看出,随着网络规模的不断扩大及攻击手段的不

收稿日期:2005-10-31

基金项目:湖南省教育厅青年项目(03B009)

作者简介:段丹青(1968-),女,江西永新人,博士研究生,研究方向为网络安全;陈松乔,教授,博士生导师,研究方向为软件工程。

断翻新,网络上传送的网络包数量不断增加,模式库不断膨胀,采用传统的模式匹配检测方法的 IDS,其性能将呈线性下降。为了解决上述问题,文中提出一种融合漏洞扫描的网络入侵检测模型。

漏洞扫描是自动检测远端或本地主机安全脆弱点的技术,它的主要作用是在发生网络攻击事件前,通过对整个网络范围扫描发现网络中存在的漏洞,及时给出修补方案,堵住安全漏洞,防止黑客利用该漏洞进行入侵活动,它是为了降低系统安全风险而发展起来的一种防患于未然的主动式安全防御技术^[3,4]。

将漏洞扫描技术与入侵检测技术相结合,实现漏洞扫描与网络入侵检测系统的联动,系统定期进行漏洞扫描,根据扫描结果对网络中的安全漏洞及时进行修补,然后将扫描结果传送给 IDS,IDS 将模式库中与已得到修补的安全漏洞相关的攻击模式删除,以缩简模式库规模,缩短模式匹配时间;同时,系统可以在对漏洞库更新的同时,检索模式库,对于新发现的安全漏洞,在模式库中动态增加其攻击模式,从而实现模式库的自动实时更新,达到提高 IDS 检测效率的目的。

1 嵌入漏洞扫描的网络入侵检测系统模型

图 1 给出了融合漏洞扫描的 IDS 模型。

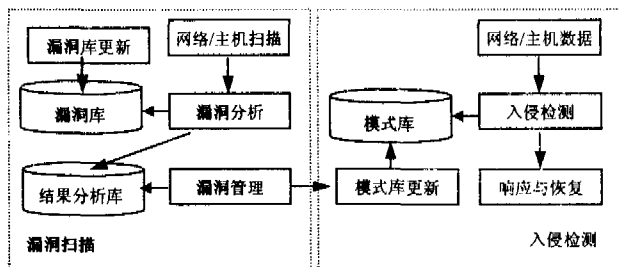


图 1 融合漏洞扫描的 IDS 模型

●在该模型中,漏洞扫描的工作过程如下:

(1)漏洞库更新:由于新的安全漏洞不断被发现,所以每次进行漏洞扫描之前,应先对漏洞库进行更新。同时将新发现的安全漏洞信息传送给 IDS 的模式库更新模块,便于 IDS 的模式库动态更新。

(2)收集信息:采用网络扫描/主机扫描方式,完成对网络主机信息的收集,这些信息包括主机提供的服务及软件版本、端口的分配,操作系统的版本类型及补丁版本、系统内核、文件属性设置、网络协议版本等。

(3)漏洞分析:将收集到的信息与漏洞库里的信息进行比对,并将分析结果存放于结果分析库。

(4)漏洞修补:漏洞管理模块从结果分析库中取出分析结果,生成相应的报表;针对发现的漏洞,提出需要采取的补救措施,对系统漏洞进行修补。

(5)结果传输:漏洞管理模块将扫描结果传送给 IDS 的模式库更新模块。

●与漏洞扫描实现联动的 IDS 工作过程如下:

(1)网络/主机数据采集:收集网络数据包和主机的系

统日志、审计记录等信息,并转换成相应的格式。

(2)入侵检测:采用基于协议分析的模式匹配方法,对采集到的数据进行检测,并将检测结果传送给响应与恢复模块。

(3)入侵响应:响应与恢复模块根据检测到的攻击类型,采取相应的响应或恢复措施。这些措施包括:报警、切断网络连接、关闭或重新启动机器,中断用户会话、入侵追踪等。

(4)模式库更新:模式库更新模块完成模式库的动态更新,包括两个方面内容:一方面,在每次漏洞检测完成后,模式库更新模块根据漏洞管理模块传送的扫描结果,将模式库中与已得到修补的漏洞相关的模式删除,同时对于漏洞库更新时新发现的安全漏洞,则在模式库增加相应的攻击模式;另一方面,对于不断出现的新的攻击手段,模式库更新模块定期对模式库进行升级维护。

2 基于多 Agent 的体系结构

由于 Agent 具有自治性、智能性、移动性和协作性等特征^[5],为分布式计算提供了一种更有效、更灵活的模式,将 Agent 技术引入 IDS,有利于提高大规模网络下 IDS 的可伸缩性、可维护性、效率和容错性。笔者根据图 1 模型,采用 Agent 技术,设计了基于 Agent 的分布式 IDS 体系结构,如图 2 所示。

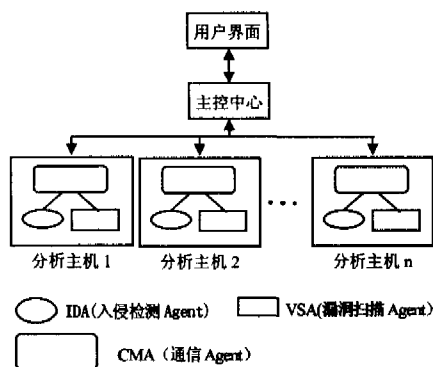


图 2 基于 Agent 的 IDS 结构

整个系统结构分为三层:

①用户界面:管理和监控系统的运行,并向用户报告入侵活动。

②主控制中心:协调控制整个网络系统的分析主机,向分析主机发送控制指令并接收主机的报告,同时控制中心可以通过分析多个分析主机的报告,采用信息融合技术,发现一些更为复杂的入侵行为。

③分析主机:每台分析主机负责一个逻辑网段的管理工作,它由通信 Agent(CMA)、入侵检测 Agent(IDA)、漏洞扫描 Agent(VSA)组成。IDA 是完成入侵检测功能的部件,VSA 是完成漏洞扫描的部件。CMA 完成本地 IDA、VSA 之间的通信,并将 IDA、VSA 的检测结果、扫描结果传送给控制中心,CMA 同时完成与其他宿主机上的 CMA 的通信功能。

在分布式环境下,每台分析主机都是独立的检测单元,监控一个网段,没有哪台分析主机处于控制核心地位。由于各分析主机可以独立完成检测功能,所以当某台分析主机出现故障时,只有与该分析主机相关的网段检测失效,不会造成整个系统的瘫痪。同时,当单台分析主机所收集的信息不足以判定可疑行为时,则多台分析主机可以相互协作来完成检测任务。

2.1 IDA(入侵检测 Agent)结构

IDA 主要完成对本地网络的监控,它将检测结果通过 CMA 传送给主控中心,并在必要时通过 CMA 传送给协作主机的 CMA,然后通过协作主机 CMA 传送给相应的 IDA;IDA 同时接收 VSA 传送的漏洞扫描结果,然后根据扫描结果对 IDA 的模式库进行动态更新。

IDA 的结构如图 3 所示。数据采集 Agent 截获网络数据包,将数据精简转化成统一格式后,将数据传送给检测 Agent,检测 Agent 采用基于协议分析的模式匹配方法,对数据进行检测,如发现入侵,则报告给入侵检测管理 Agent。检测 Agent 可以有多个,每个检测 Agent 完成对某一种特定网络应用的检测,如 FTP 检测 Agent、HTTP 检测 Agent 等。模式库更新 Agent 完成对模式库的动态更新,包括对模式库的升级维护和根据 VSA 传送的扫描结果完成对模式库中相应模式的检测标记。响应 Agent 则根据入侵方式采取相应的响应措施,包括:报警、切断网络连接、关闭或重新启动机器,中断用户会话、入侵追踪等。入侵检测管理 Agent 是 IDA 的控制中心,协调和管理本地 Agent 的工作状态,包括 Agent 的启动、停止、创建、删除、重置等。

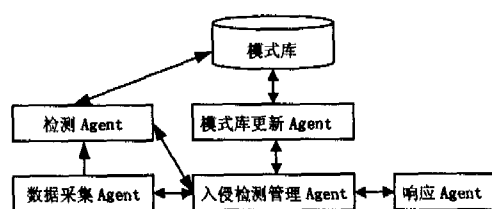


图 3 IDA 结构

2.2 VSA(漏洞扫描 Agent)结构

VSA 完成对本地网络的漏洞扫描,并将扫描结果通过 CMA 传送给本地 IDA。VSA 的结构如图 4 所示。

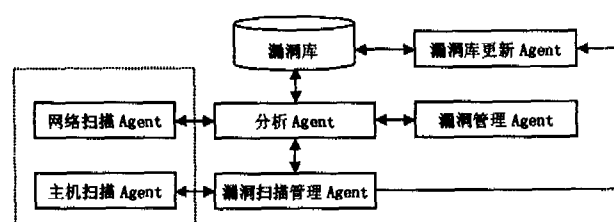


图 4 VSA 结构

漏洞扫描管理 Agent 协调和管理 VSA 中各 Agent 的工作状态,包括 Agent 的启动、停止、创建、删除等。网络扫描 Agent、主机扫描 Agent 分别完成对网络信息、主机信息的收集,并转化成统一格式后传送给分析 Agent,分析 Agent 将收集到的信息与漏洞库中的漏洞信息进行对比

分析。漏洞库中漏洞的命名采用 CVE 标准,有利于漏洞库的及时更新。分析 Agent 可以有多个,每个分析 Agent 完成某一种特定漏洞的扫描,如 CGI 脚本漏洞、finger 漏洞、FTP 漏洞、RPC 漏洞等。并将扫描结果传送给漏洞扫描管理 Agent;漏洞管理 Agent 根据分析结果,生成相应的报表;针对发现的漏洞,提出需要采取的补救措施,并调用漏洞库更新 Agent,完成对漏洞库的更新。VSA 的扫描结果通过 CMA 传送给 IDA。

2.3 CMA(通信 Agent)结构

CMA 是专门用于通信服务的 Agent,它是分析主机内 IDA 和 VSA 之间传送信息的桥梁,同时也是分析主机之间通信的桥梁。CMA 是数据传送的中介部件,它记录了本机 IDA 与 VSA 之间以及本机 IDA 与其它协作分析主机 IDA 之间的通信方式,可以为数据包提供路由服务,它的主要任务是数据包的接收和转发。Agent 之间可采用 KQML 作为通信语言,并使用 CIDE 框架定义的通用入侵规范语言 CIDL 描述的 GIDOs 作为 KQML 的内容语言,以实现 Agent 之间交换信息的标准化。由于各 Agent 之间要进行协作,各 Agent 间的通信是非常重要的。如果 Agent 之间的通信内容被截获,恶意用户就可很容易修改 Agent 的状态或破坏 Agent。所以,不同 Agent 之间以及 Agent 和主控中心之间在进行通信之前应该经过授权和认证,确认通讯双方的合法性;同时它们之间的通信应该进行加密,以保护通信信息的机密性和完整性。

3 模型的优点

通过与漏洞扫描的联动,使得该入侵检测模型具有以下优点:

(1)抗攻击性强:由于网络攻击大多是利用操作系统、Web 服务器、网络协议、网络服务等安全漏洞,本模型通过与漏洞扫描联动,定期扫描系统漏洞,并及时修补这些漏洞,使得与这些漏洞相关的攻击行为无法得逞,从而增强了系统的抗攻击性。

(2)检测效率高:由于大多数的攻击行为都是利用了网络和系统的脆弱性,系统及时对漏洞进行修补后,IDS 可以根据扫描结果将模式库中与该漏洞相关的攻击模式删除,从而极大地减少模式匹配的数量,提高检测速度。

(3)模式库动态更新:IDS 根据漏洞扫描结果,一方面可以动态删除与已得到修补的漏洞相关的入侵模式,避免了模式库的不断扩张;另一方面对于漏洞库进行更新时新发现的安全漏洞,模式库可以动态增加新的相关模式特征,从而实现模式库自动更新。

(4)稳定性好:系统采用基于 Agent 的分布式体系结构,每台分析主机独立地完成某一网段的入侵检测功能,避免了由于单点失效而造成整个系统瘫痪。

(5)可扩充性好:采用基于 Agent 技术,无论是在系统中增加分析主机还是增加检测 Agent 都很方便。

(下转第 142 页)

要增加或减少一台服务器, DNS 更新的速度相对较慢, 有时会花几小时甚至超过 24 小时来同步全球的 DNS 服务器。此外, 利用 DNS 解决负载均衡无法知晓各个服务器的工作情况, 不能知道各个服务器之间的差异, 可能会出现服务请求在某一台服务器上相对集中的情况^[4]。

利用 DNS 解决负载均衡除了可以利用在各种 B/S 系统上, 还可以应用在文件服务中, 用途比较广泛。

2.2 基于 NAT 的方法解决负载均衡

NAT 负载均衡是一种利用将 IP 地址转化为其它 IP 地址(一般是内网 IP 地址)的负载均衡技术, 它的性能较好。NAT 负载均衡可以使用软件或硬件完成。客户端访问的服务器是一台做 NAT 转换的服务器, 该服务器收到用户请求后, 会根据事先设置好的算法自动把请求数据包中的目的地址更改为服务器集群中的某个承担服务的 IP 地址, 从而分散请求^[5]。

在基于 Linux 的 B/S 系统下, 使用该方法可能会遇到问题: 在同一个会话(Session)过程中, 由于会话信息存放在服务器端的内存或硬盘中, 而客户端的每次连接可能将分布到不同的服务器中, 服务器之间无法确定用户的会话是否有效, 以及上次会话是由哪一台服务处理的, 所以这时用户的会话状态会丢失, 也就无法完整地为用户提供服务。

在应用中, 主要有 2 种方案可以解决以上问题:

(1) 使用数据库记录会话状态, 代替原有的使用内存或文件系统存储的方式。使用这种方式需要对源程序作改动。如果源程序抽象性非常强, 则只需更改少量代码实现此功能, 否则对程序将作大规模改动。在数据库负载高的应用中, 如果使用数据库记录会话状态, 会使数据库系统成为系统新的瓶颈。

(2) 使用共享文件系统, 如 NFS。首先把各类应用系统的会话存储设置为使用文件系统的形式, 然后把集群中的一台服务器作为会话共享服务器, 开启 NFS 共享, 其它服务器则把该共享目录使用 NFS 等手段远程挂上本地目录, 实现会话信息的全局共享。

基于 NAT 的负载均衡是一种比较完善的负载均衡方法, 其硬件实现方案也十分成熟。该类负载均衡方法所

有的数据交换必须通过 NAT 负载均衡服务器, 所以它适用于计算密度较高、对 CPU 或磁盘要求较高的应用场合, 不适合类似文件服务等对带宽要求很高的应用。

衡量一个负载均衡方法好坏的主要依据是轮询算法和消息反馈机制。以上几种方案都有相对成熟的轮询算法, 但没有消息反馈机制。一旦服务器集群中的某台服务器出现故障, 也无法知晓, 用户端的请求依然会被分配到出现故障的服务器上。

3 基于 Linux 的软件解决方案总结

综合以上 2 个问题及其解决方案, 可以给出基于 B/S 模型的 Web 服务器的优化解决方案, 其结构是:

(1) 使用多台服务器负载均衡, 选择 DNS 轮询作为负载均衡的手段。

(2) 每台服务器的 Web 服务器运行在非标准端口(如 81), 在 HTTP80 端口运行反向代理服务器。

(3) 在有条件的情况下分离 Web 服务器和反向代理, 以获得最佳性能。

以上结构特别适用于高并发、服务器群安放在异地的大型门户网站。通过以上结构, 可使系统的整体性能有质的飞跃。

参考文献:

- [1] Azar Y, Feder M, Lubetzky E, et al. The Multicast Bandwidth Advantage in Serving a Web Site[J]. Computer Science, 2003, 2233:180-188.
- [2] Oskar Pearson c/o Qualica Technologies (Pty) Ltd. Squid Documentation[EB/OL]. <http://www.squid-cache.org>, 2003.
- [3] Cardellini V, Colajanni M, Yu P S. DNS dispatching algorithms with state estimators for scalable Web-server clusters[J]. World Wide Web, 1999, 2:67-77.
- [4] 王木年, 曹先彬. 一种域分布合作 Web 缓存系统[J]. 计算机研究与发展, 2002, 39(3):275-279.
- [5] 周振. WWW 缓存技术的研究与实现[D]. 大连: 大连海事大学, 2004.

(上接第 133 页)

4 结束语

提出融合漏洞扫描功能的 IDS 系统模型, 通过漏洞扫描与 IDS 联动, 一方面增强了被监控主机的抗入侵能力; 另一方面提高了入侵检测系统的检测效率, 在网络入侵检测中是一种新的尝试。目前笔者根据该模型设计的网络入侵检测原型系统正在开发中, 系统开发平台采用 Windows 2000, 开发工具采用 Visual C++, 前台采用 JSP 技术实现基于 Web 的用户管理界面, 提供查询信息、控制和报警等功能。

参考文献:

- [1] 姚立红, 谢立. IPSEC 与防火墙协同工作设计与实现[J]. 小型微型计算机系统, 2004, 25(2):138-186.
- [2] Kumar G. Classification and detection of computer intrusion [D]. Indiana: Purdue University, 1995.
- [3] 徐漫江. 一种主机与网络相结合的漏洞扫描工具的设计与实现[J]. 雷达与对抗, 2002(2):65-68.
- [4] 杨英鹏, 马建峰. 一种基于代理的分布式抗攻击的入侵检测体系结构[J]. 计算机工程, 2003, 29(13):71-72.
- [5] 陈铁明, 蔡家楣, 蒋融融, 等. 基于插件的安全漏洞扫描系统设计[J]. 计算机工程与设计, 2004, 25(2):194-196.