Windows 平台下 Snort 系统的架构与实现

马占飞[1],尹传卓[2]
(1. 内蒙古科技大学 包头师范学院,内蒙古 包头 014030;
2. 内蒙古科技大学 信息工程学院,内蒙古 包头 014010)

摘 要:通过对入侵检测系统的深入研究,在此基础上,架构了一个在 Windows 平台下的基于 Snort 的分布式网络入侵检测系统。该系统模型融合了层次模型和分布式协作模型的优点,采用三级分层体系结构,并融合了改进的 BM 模式匹配算法(IBM 算法)。实验结果表明,该系统能够对缓冲区溢出、端口扫描等攻击进行很好地探测,相比传统的 Snort 系统,在检测效率和性能上均有大幅度提高。同时该系统还提供了更加人性化的操作界面,方便了用户的操作和使用。

关键词:网络安全;入侵检测系统;Snort;BM 算法;ACID
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2013)01-0154-03
doi:10.3969/j.issn.1673-629X.2013.01.038

Architecture and Implementation of Snort System under Windows Platform

MA Zhan-fei[1], YIN Chuan-zhuo[2]
(1. Baotou Teachers College, Inner Mongolia University of Science and Technology, Baotou 014030, China;
2. School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China)

Abstract: Through studying and analyzing the current intrusion detection system (IDS), a novel and visual distributed intrusion detection system (DIDS) based on the Snort under the Windows platform is proposed. The system model combines the advantages of the hierarchical model and the distributed collaboration model, using three-layer architecture, and integrated into the improved BM pattern matching algorithm (IBM algorithm). The experimental results show that the Snort system is able to detect buffer overflows, port scans and other attacks. Compared with the traditional Snort system, the system can improve greatly the detection efficiency and performance, and possesses better universalness and expansibility. The system also provides a more humane operation interface, and be convenient for the user's operation and use.

Key words: network security; intrusion detection system; Snort; BM algorithm; ACID

0 引 言

随着网络技术的迅猛发展和 Internet 的广泛应用,网络已经深入到社会的各个领域,网络在给人们的工作、生活和学习带来了极大便利的同时,也带来了诸多安全问题[1,2]。为了保障计算机系统、网络系统和信息的安全,各 IT 厂商推出了许多安全技术和产品,对网络系统的各个环节提供安全保护[3,4]。防火墙作为保护互联网络的首选安全产品,在市场上得到了广泛的认可和应用。防火墙(Firewall)是一个软硬件的结合体,是内部可信网络与外部不可信网络之间的一道安全防护屏障[5~7],一般被安置于 Internet 与被保护的内网之间。然而防火墙是一种被动的访问控制技术,它依据事先设计好的规则对在两个或者多个网络之间传输的数据包进行检查,从而保护内部网络不受攻击。由于互联网的开放性,防火墙也存在着对实时的攻击或异常的行为不能做出及时响应,无法防范病毒或感染了病毒的软件或文件,也不能防范内部攻击等诸多潜在的威胁。在这样的背景下,入侵检测系统(Intrusion Detection System, IDS)就应运而生了[8,9]。IDS 是

收稿日期:2012-05-18;**修回日期**:2012-08-24
基金项目:国家自然科学基金资助项目(61163025);内蒙古自治区自然科学基金项目(2010BS0904);内蒙古自治区高等学校科学研究基金项目(重点项目)(NJ10162);内蒙古自治区高等学校科学研究项目基金项目(NJZY07116)
作者简介:马占飞(1973-),男,内蒙古包头人,教授,博士,CCF 高级会员,主要研究领域为计算机网络技术与信息安全、人工智能;尹传卓(1986-),男,山东人,硕士研究生,主要研究领域为计算机网络技术与信息安全。

一种能够保护自己免受攻击的新型网络安全技术,它通过监视网络资源(网络数据包、系统日志、文件和用户活动的状态行为),主动寻找分析入侵行为的迹象,从而给网络系统提供对外部攻击、内部攻击和误操作的安全保护[10]。

鉴于此,文中在 Windows Server 2003 平台下架构了 Snort 系统,将前期研究的改进 BM(Boyer-Moore)模式匹配算法(IBM 算法)应用到了该 Snort 检测引擎中[11],并对 Snort 规则进行了改进和优化,旨在增强系统的检测分析能力,提高入侵检测效率,以及对入侵者的意图进行跟踪与预测等。

1　Snort 系统概述

Snort 是一个轻量级的网络入侵检测系统(Network Intrusion Detection System,NIDS)。所谓轻量级是指在检测时对网络正常运行所产生的影响尽可能低。Snort 作为轻量级网络入侵检测系统的典范,具备跨系统平台操作、对系统性能影响较小等特征,用户可以根据自己的需要在短时间内调整检测策略[12,13]。

Snort 的工作模式有三种:嗅探器模式、数据包记录器模式、网络入侵检测模式[14]。嗅探器模式是 Snort 使用 Libpcap 包捕获库,即 TCP DUMP 使用的库,从网络接口的混杂模式读取并解析共享信道中的网络数据包,作为连续不断的流显示在终端上。数据包记录器模式是 Snort 使用 Packet Logger 模式,把数据包记录到硬盘上,并指定到一个目录中。网络入侵检测模式是用户最常用到的模式,并且需要载入规则库才能工作。这种模式融合了嗅探器和数据包记录器两种模式,操作相对复杂,但是它是可配置的,用户可以让 Snort 系统按照自定义的一些规则来匹配分析网络数据包,并根据检测结果采取一定的响应策略,文中正是基于这一模式进行设计和分析的。

2　Windows 平台下 Snort 系统架构与实现

2.1　Snort 系统架构

文中在前期研究成果基础上,架构了一种基于 Windows Server 2003 平台的分布式 Snort 入侵检测系统模型。该模型融合了层次模型和分布式协作模型的优点[15],采用三级分层体系结构,主要包括 Snort 监视器层、数据分析层和决策管理层[11]。Snort 系统的体系结构如图 1 所示。

在该系统模型中,Snort 监视器是一个本地的 IDS,负责监视各自管辖的网段。对于一些已知的入侵行为,如果监视器能够进行独立判断,则按照预先的配置做出相应的响应;对于一些可疑行为或复杂的攻击行为,Snort 监视器负责将这些数据包进行预处理(包括

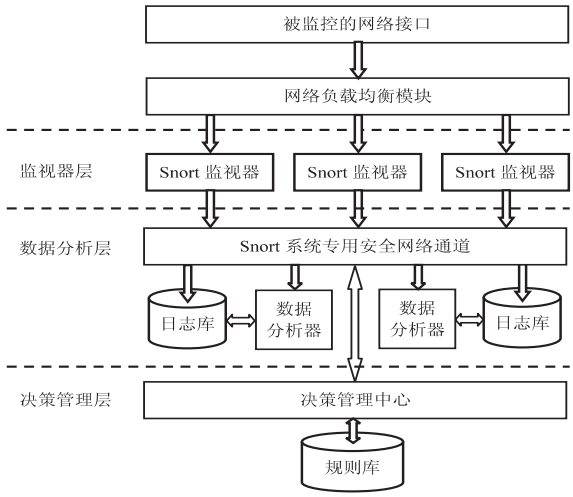

图 1　Snort 系统的体系结构

数据的格式化和提取),并将日志文件和经预处理的数据包通过专用安全通道一并提交数据分析层,由数据分析器做进一步分析处理。为了避免系统的单一失效点,数据分析层设有多个数据分析器,每一个分析器都设有自己的优先级。优先级主要根据该数据分析器所在主机的数据处理能力而定,处理能力越强,则优先级越高。在该层只有优先级最高的数据分析器处于活动状态,其它的均处于就绪状态,这样可以有效地节约系统资源。一旦活动的数据分析器失效,那么在就绪的数据分析器中立即选举出一个,使其成为活动的数据分析器。决策管理层主要用来管理和控制各 Snort 监视器与数据分析器,并根据监视器和分析器反馈的检测结果,更新和维护全局规则数据库。另外,决策管理中心还为系统管理员提供了一个可视化的、友好的人机交互界面,让管理员可以更方便地管理整个系统。

2.2　Snort 系统的实现

文中设计的基于 Windows 平台的分布式 Snort 入侵检测系统的工作原理:通过抓包工具 WinPcap 来获取网络上的数据包,然后送到 Snort 检测引擎,由 Snort 检测引擎负责将数据包与规则库进行匹配,判断其是否为入侵行为或者违反策略的访问,如果成功匹配了规则库中的任意一条规则,系统就会进行报警或者以日志的方式记录下来,并保存到日志数据库中。系统分析控制台 ACID(Analysis Console for Intrusion Database)的作用是为系统提供更加人性化的操作界面,它

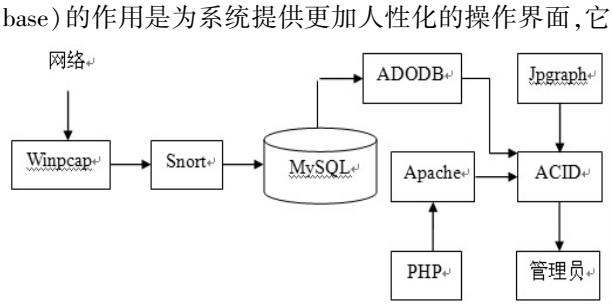

图 2　Snort 系统的工作原理

通过 Web 网页形式为管理员提供报警和日志信息,以供管理员进行分析并做出决策。其工作原理如图 2 所示。

依据 Snort 系统的工作原理,进行了系统实现与配置。Snort 系统实现所需的软件如表 1 所示。

表 1 Windows 平台下 Snort 系统所需的软件

软件名称	主要功能
Apache-2.2	Windows 版本的 Apache Web 服务器
Php-5.2	Windows 版本的 Php 脚本环境支持
WinPcap-4.1.2	Windows 版本的 Pcap,网络数据包截取驱动程序
Snort-2.9	Snort 系统安装包,入侵检测系统的核心
MySql-5.0	用于存储 Snort 的日志、报警等信息
Adodb-5.14	为 Php 提供统一的数据库连接函数
Acid-0.9.6	基于 Php 的入侵检测数据库分析控制台
JpGraph-3.5	Php 所用的图形库

Snort 系统的实现步骤如下:

1)首先安装 Apache 与 Php,假定 Apache 的安装目录为 D:\Snort\Apache,用 IE 浏览器验证:http://localhost 或 http://127.0.0.1,测试 Apache 是否安装成功;然后 PHP 按照指定目录 D:\Snort\php 安装即可。

2)按照提示安装 WinPcap 抓包工具,Snort 检测引擎的安装目录设置为 D:\Snort\Snort,完成安装后用“D:\Snort\Snort \bin> snort.exe -W”(W 为大写)测试其是否正常工作。

3)MySql 数据库的安装与配置,指定 MySql 安装目录为 D:\Snort\MySql。将 D:\Snort\Snort \schemas 目录下的 create_mysql 脚本文件复制到 D:\Snort\MySql\bin 目录下,在 MySql 数据库中建立 snort 库和 snort_archive 库,并为 Snort 与 ACID 设置密码及用户权限,使 IDS Center 或 acid 能够正常访问 MySql 中与 Snort 相关的数据文件。同时启用 Php 对 MySQL 的支持。

4)把 Adodb-5.14.zip 解压缩到 D:\Snort\php\adodb 目录下,把系统用到的图形库 Jpgraph-3.5 安装在 D:\Snort\php\jpgraph 目录下,把系统分析控制台源文件 Acid-0.9.6b23.tar.tar 解压缩到 D:\Snort\Apache \htdocs\acid 目录下。

3 系统测试与分析

文中将前期研究的改进 BM 模式匹配算法(IBM 算法)融入到 Snort 检测引擎中,并对 Snort 规则进行了改进和优化,通过一系列实验对该系统的有效性进行了测试和分析[16]。从数据包的类型来看,该系统不仅能够检测出所使用的协议、攻击方式、检测器的数量、名称和位置等,还能够通过 ACID 平台来统计报警的数量、源/目的 IP 地址、源/目的端口的种类和数量。此外,该系统还能对一段时间内检测到的相关攻击行为特征信息进行统计分析,以便找出其内在的一些规律。图 3 所示为某一周时间内该系统检测到攻击次数的分布情况。

通过对 Windows Server 2003 平台下的 Snort 系统整体测试运行结果来看,该系统能够对缓冲区溢出、端口扫描等常用攻击软件所发起的攻击进行很好地探测,系统的检测结果相比传统的 Snort 系统,在检测效率和性能上均有了大幅度提高。

4 结束语

文中在 Windows 平台上架构了基于 Snort 的分布式网络入侵检测系统,该系统通过融入改进的 BM 模式匹配算法(IBM 算法),以及对 Snort 规则库设计和优化,能够有效地提高 Snort 系统的整体检测性能。特别是采用 ACID 提供的图形化显示界面,简化了系统配置和使用难度,符合轻量级、简单使用的原则。通过一系列测试,证实了该系统的设计是成功的。然而由于 Snort 系统的入侵检测模式具有一定的局限性,系统的检测性能和效率还有待进一步提升。

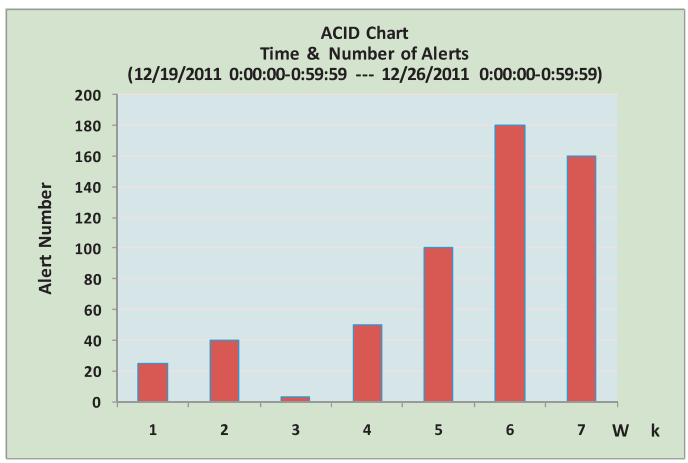

图 3 告警次数分布图

参考文献:

[1] Aguirre I, Alonso S. Improving the automation of security information management: a collaborative approach[J]. Security & Privacy, 2012, 10(1): 55-59.

[2] Shiravi A, Shiravi H, Tavallaee M, et al. Toward developing a systematic approach to generate benchmark datasets for intrusion detection[J]. Computers and Security, 2012, 31(3): 357-374.

[3] Hulitt E, Vaughn R B. Information system security compliance to FISMA standard: a quantitative measure[J]. Telecommunication Systems, 2010, 45(2-3): 139-152.

[4] Werlinger R, Muldner K, Hawkey K, et al. Preparation, detection and analysis: the diagnostic work of IT security incident

(下转第 176 页)

2.2.3 报表及数据导出管理

为了将现有的管理信息系统和之前的人工管理系统对接,本管理信息系统提供了丰富的数据导出功能,可将数据库中的数据导出到 PDF 文档、Excel 文档、Word 文档中,同时也可将数据直接以报表形式打印输出。其中报表对象是本系统中设计的一个重点,为了与现有工作流审批时的纸质文档相符,设计报表时尽量做到格式规范,界面美观。本系统使用的报表控件是. NET 平台下的水晶报表控件,该控件中提供的 ReportDocument 对象模型可以方便地设计报表的结构布局以及绑定其数据源到 ADO. NET 数据集[12],使数据库中的数据其以规定的格式显示在用户界面。

3 结束语

通过建立高校学科竞赛管理系统,在传统的手工管理方式上,融入数据库和网络业务流程管理,使学科竞赛管理走向规范化、标准化、高效化。本系统目前已投入试运行,系统运行状况良好,能较全面地反映学科竞赛的实际流程,符合竞赛管理的实际需求,界面友好,操作简便,基本能满足竞赛管理上的各方面要求。当然,系统在使用中也存在若干问题,某些方面做得还不够成熟,还有待进一步改进。

参考文献:

[1] 夏百战,吕 燚. 学科竞赛对独立学院教学工作的重要意义[J]. 中国现代教育装备,2009(17):167-169.

[2] 瞿绍军. 以学科竞赛为载体,培养大学生创新能力-以大学生程序设计竞赛为例[J]. 电脑知识与技术,2010,15(6):3980-3981.

[3] 赵瑞军,温晓娣,李红球. 基于学科竞赛平台构建的创新人才培养[J]. 金华职业技术学院学报,2010,10(3):13-15.

[4] 唐玉芳,张永胜. 基于. NET 的学生信息管理系统的设计与实现[J]. 计算机技术与发展,2010,20(4):242-245.

[5] MacDonald M. ASP. NET 3.5 从入门到精通(C#2008 版)[M]. 施宏斌,马 煜译. 北京:清华大学出版社,2010.

[6] 丁士锋,朱 毅,杨明羽. 精通 C#3.0 与 NET 3.5 高级编程:LINQ、WCF、WPF、WF[M]. 北京:清华大学出版社,2009.

[7] Crampton J, Loizou G. Administrative scope: A foundation for role-based administrative models[J]. ACM Transactions on Information System Security, 2003, 6(2): 201-203.

[8] 刘金晓. Web 应用系统中权限控制的研究与实现[J]. 计算机工程与设计,2008,29(10):2550-2553.

[9] Bukovics B. WF 高级程序设计[M]. 柴晓伟译. 北京:人民邮电出版社,2009.

[10] 缪 永,周 健,陶 亮. 基于工作流的企业协同 OA 系统关键技术实现[J]. 计算机技术与发展,2011,21(3):90-93.

[11] Nuu C J. The evolution towards flexible workflow systems[J]. Distributed Systems Engineering, 2006, 3(4): 276-294.

[12] Kurt W, Scott H, Robert S. Building systems form commercial components[M]. [s. l.]: Addison-Wesley, 2003.

(上接第 156 页)

response[J]. Information Management & Computer Security, 2010, 18(1): 26-42.

[5] Yoon M, Chen Shigang, Zhang Zhan. Minimizing the maximum firewall rule set in a network with multiple firewalls[J]. IEEE Transactions on Computers, 2010, 59(2): 218-230.

[6] Chao C S, Yang S J H. A novel three-tiered visualization approach for firewall rule validation[J]. Journal of Visual Languages & Computing, 2011, 22(6): 401-414.

[7] Rovniagin D, Wool A. The geometric efficient matching algorithm for firewalls[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(1): 147-159.

[8] Shahrestani S A. Employing artificial immunology and approximate reasoning models for enhanced network intrusion detection[J]. WSEAS Transactions on Information Science and Applications, 2009, 6(2): 190-200.

[9] Aydin M A, Zaim A H, Ceylan K G A. Hybrid intrusion detection system design for computer network security[J]. Computers and Electrical Engineering, 2009, 35(3): 517-526.

[10] Papadogiannakis A, Vasiliadis G, Antoniades D, et al. Improving the performance of passive network monitoring applications with memory locality enhancements[J]. Computer Communications, 2012, 35(1): 129-140.

[11] 尹传卓. 基于 Snort 的分布式入侵检测系统的研究与实现[D]. 包头:内蒙古科技大学,2012.

[12] Kurundkar G D, Naik N A, Khamitkar S D. Network Intrusion Detection Using SNORT[J]. International Journal of Engineering Research and Applications, 2012, 2(2): 1288-1296.

[13] 宋连涛,庄卫华. 基于异常的入侵检测技术在 Snort 系统中的应用[J]. 计算机技术与发展,2006,16(6):136-138.

[14] Wang Baoyi, Yang Haipeng, Zhang Shaomin. Research on application of interaction firewall with IDS in distribution automation system[J]. Lecture Notes in Electrical Engineering, 2012, 139: 527-532.

[15] Gómez C J, Padilla G N, Baños R, et al. Design of a Snort-based hybrid intrusion detection system[J]. Lecture Notes in Computer Science, 2009, 5518: 515-522.

[16] Salah K, Kahtani A. Performance evaluation comparison of Snort NIDS under Linux and Windows server[J]. Journal of Network and Computer Applications, 2010, 33(1): 6-15.

Windows 平台下 Snort 系统的架构与实现

作者： 马占飞， 尹传卓
作者单位： 马占飞(内蒙古科技大学 包头师范学院,内蒙古 包头 014030)， 尹传卓(内蒙古科技大学信息工程学院,内蒙古 包头 014010)

刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(1)